# Cisco SD-WAN (Viptela) vManage Help for Cisco IOS XE SD-WAN Release 16.10.x and Cisco SD-WAN Release 18.4.x

# Administration

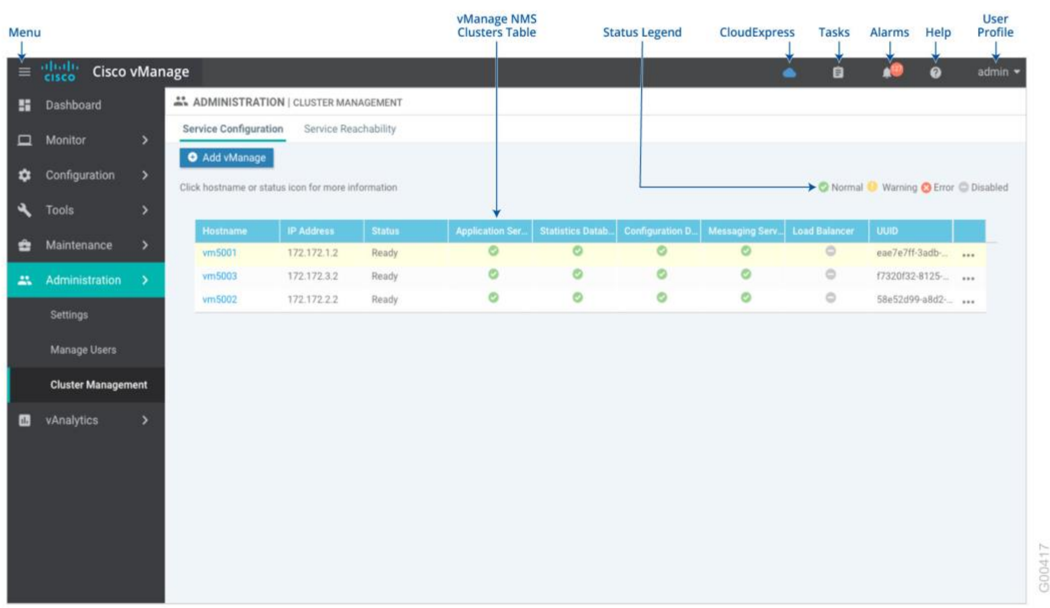
## Cluster Management

Use the Cluster Management screen to create a vManage NMS cluster. In a vManage NMS cluster, all the cluster members communicate and work cooperatively to manage all the vBond orchestrators, vEdge routers, and vSmart controllers in the overlay network. Each vManage server can manage up to about 2,000 vEdge routers in the overlay network.

It is strongly recommended that all members of a vManage NMS cluster be located in the same data center.

## Screen Elements

- Top bar—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.
- Title bar—Includes the title of the screen, Cluster Management.
- Service Configuration bar—Includes tabs for Service Configuration and Service Reachability.
  - Service Configuration tab—Display the configured vManage NMSs and cluster services configured on each vManage NMS. When you first open the Cluster Management screen, the Service Configuration tab is selected.
    - Add vManage button—Add a new vManage NMS to a cluster.
  - Service Reachability tab—Display the reachable cluster services reachable on the vManage NMSs in the cluster.
    - Current vManage—Display the IP address of the vManage NMS you are currently logged into.
- Status legend—Includes colored icons for Normal, Warning, Error, and Disabled.
- Table of vManage NMS cluster members—Click a green check mark in the table to display which cluster members are reporting the status. To re-arrange the columns, drag the column title to the desired position.



# Change the IP Address of the Current vManage NMS

It is recommended that you configure the IP address of the vManage server statically, in its configuration file. Configure this IP address on a non-tunnel interface in VPN 0. It is also recommended that you do not configure DHCP in VPN 512.

When you start a vManage NMS for the first time, the default IP address of the vManage server is shown as "localhost". Before you can add a new vManage NMS to a cluster, you must change "localhost" to an IP address:

1. In the Service Configuration tab, click the Add vManage button. The Edit vManage screen opens.
2. From the vManage IP Address drop-down list, select an IP address to assign to the vManage server.
3. Specify a username and password for the vManage server.
4. Click Update.

The vManage server automatically reboots and displays the Cluster Management screen.

# Add a vManage NMS

To add a new vManage NMS to the cluster:

1. In the Service Configuration tab, click the Add vManage button. The Add vManage screen opens.
2. Enter the IP address of the vManage NMS you are adding to the cluster.

Note: It is strongly recommended that the IP addresses of all members of the vManage cluster be in the same subnet.

3. Specify the username and password for the new vManage server.
4. Select the services to run on the vManage server. You can select from the services listed below.
   Note that the Application Server field is not editable. The vManage Application Server is the local vManage HTTP web server.

- Statistics Database—Stores all real-time statistics from all Viptela devices in the network.
- Configuration Database—Stores all the device and feature templates and configurations for all Viptela devices in the network.
- Messaging Server—Distributes messages and shares state among all vManage NMS cluster members.

5. Click Add. The vManage NMS that you just added then reboots before joining the cluster.

In a cluster, it is recommended that you run at least three instances of each service.

Note: The members of a vManage cluster rely on timestamps to synchronize data and to track device uptime. For this time-dependent data to remain accurate, you cannot change the clock time on any one of the vManage servers of the cluster after you create the cluster.

# Configure the Statistics Database

To configure the statistics database, which stores all real-time statistics from the local vManage NMS:

1. In the Service Configuration tab, click the Statistics Database Configuration button. The Statistics Database Configuration screen opens. The top of the screen specifies the maximum space available for the database.
2. For each Statistics Type field, assign an the amount of storage to allocate, in gigabytes (GB). The total value of all fields cannot exceed the maximum available space.
3. Click Update.

vManage NMS updates the storage allocations you have assigned once a day, at midnight.

## View Statistics Database Space Usage

To view the amount of space available and utilized for the statistics database on the local vManage NMS, in the Service Configuration tab, click the Statistics Database Configuration button. The Statistics Database Configuration screen opens. The top of the screen shows the maximum space available for the database and the total amount of space currently being utilized. The table on this screen shows, for each statistics type, the disk space currently being utilized.

## View vManage Service Details

To view detailed information about the services running on a vManage NMS:

1. In the Service Configuration tab, click on the hostname of the vManage server. The IP Address screen opens, with the vManage Details tab selected. This screen displays the process IDs of all the vManage services that are enabled on the vManage NMS.
2. Click Cluster Management in the breadcrumb in the title bar to return to the Cluster Management screen.

## View Devices Connected to a vManage NMS

To view a list of devices connected to a vManage NMS:

1. In the Service Configuration tab, click on the hostname of the vManage server. The IP Address screen opens with the vManage Details tab selected.
2. Click the Connected Device tab to view a detailed list of all devices connected to the vManage NMS.

Alternatively:

1. In the Service Configuration tab, for a vManage NMS, click the More Actions icon to the right of its row.
2. Click Device Connected.

## Edit a vManage NMS

1. In the Service Configuration tab, for a vManage NMS, click the More Actions icon to the right of its row and click Edit. The Edit vManage screen opens.
2. In the vManage IP Address box, select the IP address to edit.
3. Enter the username and password, and edit the cluster services provided by that vManage NMS.
4. Click Update.

## Remove a vManage NMS from the Cluster

1. In the Service Configuration tab, for a vManage NMS, click the More Actions icon to the right of its row and click Remove. The Remove vManage dialog box opens.
2. Enter the username and password to confirm removal of the device from the network.
3. Click Remove.

The vManage NMS is removed from the cluster, the device is invalidated, and the certificates for that device are deleted. The remaining members in the cluster re-balance the NMS services.

## View Available Cluster Services

To view the services that are available and reachable on all members in the vManage NMS cluster, click the Service Reachability tab.

## Additional Information

Create a vManage Cluster

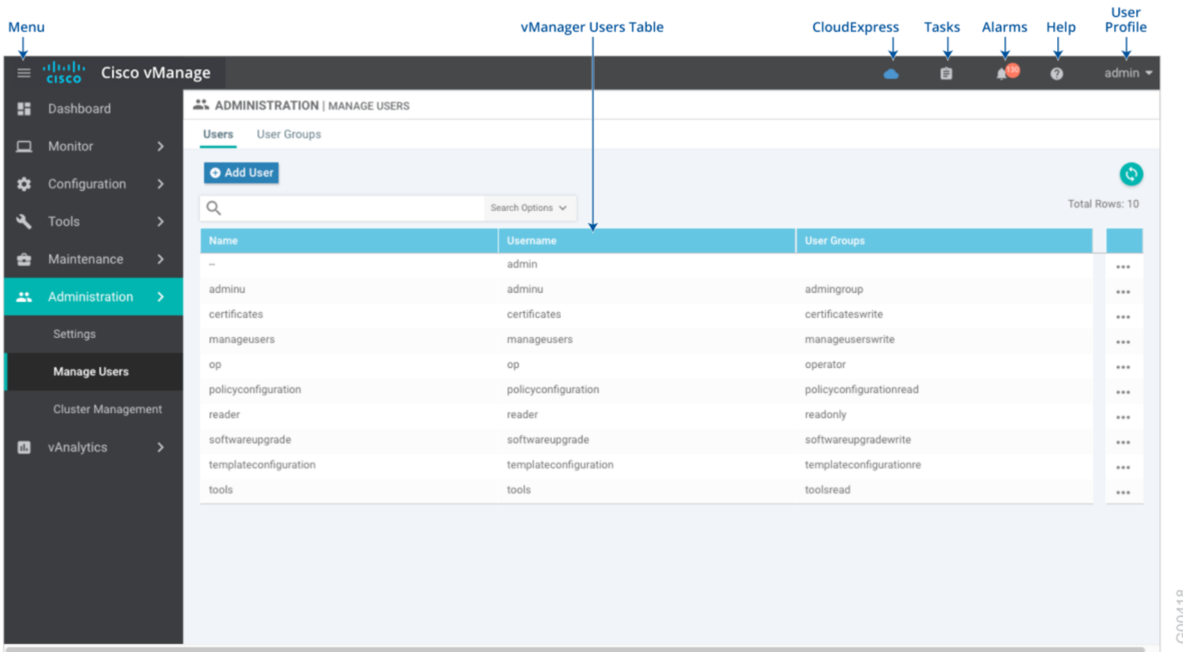
## Manage Users

Use the Manage Users screen to add, edit, or delete users and user groups from the vManage NMS.

Only a user logged in as the **admin** user or a user who has Manage Users write permission can add, edit, or delete users and user groups from the vManage NMS.

## Screen Elements

- Top bar—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.
- Title bar—Includes the title of the screen, Manage Users.
- Users tab—Add, edit, or delete users who are allowed to perform operations on the vManage NMS.
    - Add User: Add a new user.
    - Search box: Includes the Search Options drop-down, for a Contains or Match string.
    - Refresh icon: Click to refresh data in the device table with the most current data.
    - Table with list of users: To re-arrange the columns, drag the column title to the desired position.
- User Groups tab—Add, edit, or delete user groups.
    - Add User Group: Add a user group.
    - Group Name: Search for a user group. The list of user groups are displayed directly beneath Group Name in the left pane.
    - Edit: Edit the privilege levels for the selected user group.
    - Privilege level table: Displays privilege levels for the user group selected in the Group Name field.




## Add a User

To perform operations on a Viptela device, you configure usernames and passwords for users who are allowed to access the Viptela device. The Viptela software provides one standard username, **admin** , and you can also create custom usernames, as needed.

To add a user:

1. In the Users tab, click Add User.
2. In the Add User popup window, enter the full name, username, and password for the user. Note that uppercase characters are not allowed in usernames.
3. From the User Groups drop-down list, select the groups that the user will be a member of.
4. Click Add. The user is then listed in the user table.

## Delete a User

1. In the Users tab, select the user you wish to delete.
2. Click the More Actions icon to the right of the column and click Delete.
3. Click OK to confirm deletion of the user.

## Edit User Details

1. In the Users tab, select the user whose details you wish to edit.
2. Click the More Actions icon to the right of the column and click Edit.
3. Edit login details, and add or remove the user from user groups.

4. Click Update.

## Change User Password

1. In the Users tab, select the user whose password you wish to change.
2. Click the More Actions icon to the right of the column and click Change Password.
3. Enter, and then confirm, the new password. Note that the user, if logged in, is logged out.
4. Click Done.

## Add a User Group

Users are placed in groups, which define the specific configuration and operational commands that the users are authorized to view and modify. A single user can be in one or more groups. The Viptela software provides three standard user groups, and you can also create custom user groups, as needed:

- basic—Includes users who have permission to view interface and system information.
- netadmin—Includes the admin user, by default, who can perform all operations on the vManage NMS. You can add other users to this group.
- operator—Includes users who have permission only to view information.

To add a user group:

1. In the User Groups tab, click Add User Group.
2. In the Add User Group popup window, enter the user group name and select the desired read and write permissions for each feature. Note that uppercase characters are not allowed in user group names.
3. Click OK. The user group is then listed in the left pane.

Each user group can have read or write permission for the features listed below. Write permission includes read permission.

Note: All user groups, regardless of the read or write permissions selected, can view the information displayed in the vManage Dashboard screen.

| Feature | Read Permission | Write Permission |
|---|---|---|
| Alarms | Set alarm filters and view alarms generated on Viptela devices on the Monitor ▶ Alarms screen. | No additional permissions. |
| Audit Log | Set audit log filters and view a log of all activities on Viptela devices on the Monitor ▶ Audit Log screen. | No additional permissions. |
| Certificates | View a list of vEdge routers in the overlay network on the Configuration ▶ Certificates ▶ vEdge List screen.<br><br>View a CSR and certificate on the Configuration ▶ Certificates ▶ Controllers screen. | Validate and invalidate a vEdge router, stage a vEdge router, and send the serial number of valid controller devices to the vBond orchestrator on the Configuration ▶ Certificates ▶ vEdge List screen.<br><br>Generate a CSR, install a signed certificate, reset the RSA key pair, and invalidate a controller device on the Configuration ▶ Certificates ▶ Controllers screen. |

| | | |
|---|---|---|
| Cluster | View information about services running on a vManage NMS, a list of devices connected to a vManage NMS, and the services that are available and running on all the vManage NMSs in the cluster on the Administration ► Cluster Management screen. | Change the IP address of the current vManage NMS, add a vManage NMS to the cluster, configure the statistics database, edit a vManage NMS, and remove a vManage NMS from the cluster on the Administration ► Cluster Management screen. |
| Device Inventory | View a vEdge router's running and local configuration, a log of template activities, and the status of attaching configuration templates to vEdge routers on the Configuration ► Devices ► vEdge List screen.<br><br>View the running and local configuration of a controller device, a log of template activities, and the status of attaching configuration templates to controller devices on the Configuration ► Devices ► Controllers screen. | Upload the vEdge router authorized serial number file to the vManage NMS, toggle a vEdge router from vManage configuration mode to CLI mode, copy a vEdge router's configuration, and delete a vEdge router from the network on the Configuration ► Devices ► vEdge List screen.<br><br>Add and delete controller devices from the overlay network, and edit the IP address and login credentials of a controller device on the Configuration ► Devices ► Controllers screen. |
| Device Monitoring | View the geographic location of Viptela devices on the Monitor ► Geography screen.<br><br>View events that have occurred on Viptela devices on the Monitor ► Events screen.<br><br>View a list of Viptela devices in the network, device status summary, DPI flow information, TLOC loss, latency, and jitter information, control and tunnel connections, system status, and events on the Monitor ► Network screen (only if System is selected). | Ping a device, run a traceroute, and analyze the traffic path for an IP packet on the Monitor ► Network ► Troubleshooting screen (only if System is selected). |
| Device Reboot | View a list of devices on which the reboot operation can be performed on the Maintenance ► Device Reboot screen. | Reboot one or more Viptela device on the Maintenance ► Device Reboot screen. |
| Interface | View information about interfaces on a device on the Monitor ► Network ► Interface screen (only is Device Monitoring is selected). | Edit Chart Options to select the type of data to display, and edit the time period for which to display data on the Monitor ► Network ► Interface screen (only if Device Monitoring is selected). |
| Manage Users | View users and user groups on the Administration ► Manage Users screen. | Add, edit, and delete users and user groups from the vManage NMS, and edit user group privileges on the Administration ► Manage Users screen. |
| Policy | View common policies for all vSmart controllers or vEdge routers in the network on the Configuration ► Policy screen (only if Policy Configuration and Policy Deploy are selected). | Create, edit, and delete common policies for all vSmart controllers or vEdge routers in the network on the Configuration ► Policy screen (only if Policy Configuration and Policy Deploy are selected). |
| Policy Configuration | View list of policies created and details about them on the Configuration ► Policy screen (only if Policy is selected). | Create, edit, and delete common policies for all vSmart controllers and vEdge routers in the network on the Configuration ► Policy screen (only if Policy is selected). |
| Policy Deploy | View the current status of the vSmart controllers to which a policy is being applied on the Configuration ► Policy screen (only if Policy is selected). | Activate and deactivate common policies for all vSmart controllers in the network on the Configuration ► Policy screen (only if Policy is selected). |
| Routing | View real-time routing information for a device on the Monitor ► Network ► Real-Time screen (only if Device Monitoring is selected). | Add command filters to speed up the display of information on the Monitor ► Network ► Real-Time screen (only if Device Monitoring is selected). |

| | | |
|---|---|---|
| Settings | View the organization name, vBond DNS/IP address, certificate authorization settings, software version enforced on a vEdge router, custom banner on the vManage login screen, and the current settings for collecting statistics on the Administration ▶ Settings screen. | Edit the organization name, vBond DNS/IP address, certificate authorization settings, software version enforced on a vEdge router, custom banner on the vManage login screen, current settings for collecting statistics, generate a Certificate Signing Request (CSR) for a web server certificate, and install a certificate on the Administration ▶ Settings screen. |
| Software Upgrade | View a list of Viptela devices on which software upgrade can be performed and the current software version running on a device on the Maintenance ▶ Software Upgrade screen. | Upload new software images on Viptela devices, upgrade, activate, and delete a software image on a device, and set a software image to be the default image on a Viptela device on the Maintenance ▶ Software Upgrade screen. |
| System | View system-wide parameters configured using vManage templates on the Configuration ▶ Templates ▶ System screen (only if Device Monitoring is selected). | Configure system-wide parameters using vManage templates on the Configuration ▶ Templates ▶ System screen (only if Device Monitoring is selected). |
| Template Configuration | View feature and device templates on the Configuration ▶ Templates screen. | Create, edit, delete, and copy a feature or device template on the Configuration ▶ Templates screen. |
| Template Deploy | View devices attached to a device template on the Configuration ▶ Templates screen. | Attach a device to a device template on the Configuration ▶ Templates screen. |
| Tools | Use the Admin Tech command to collect system status information for a device on the Tools ▶ Operational Commands screen. | Use the Admin Tech command to collect system status information for a device, and use the Interface Reset command to shut down and then restart an interface on a device in a single operation on the Tools ▶ Operational Commands screen.<br><br>Rediscover the network to locate new devices and synchronize them with the vManage NMS on the Tools ▶ Rediscover Network screen.<br><br>Establish an SSH session to a Viptela device and issue CLI commands on the Tools ▶ SSH Terminal screen. |

## Delete a User Group

1. In the User Groups tab, click the name of the user group you wish to delete. Note that you cannot delete any of the three standard user groups—basic, netadmin, and operator.
2. Click the Trash icon.
3. Click OK to confirm deletion of the user group.

## Edit User Group Privileges

1. In the User Groups tab, select the name of the user group whose privileges you wish to edit. Note that you cannot edit privileges for the three standard user groups—basic, netadmin, and operator.
2. Click the Edit button located directly above the privilege level table, and edit privileges as needed.
3. Click Save.

If an **admin** user changes the privileges of a user by changing their group, and if that user is currently logged in to the device, the user is logged out and must log back in again.

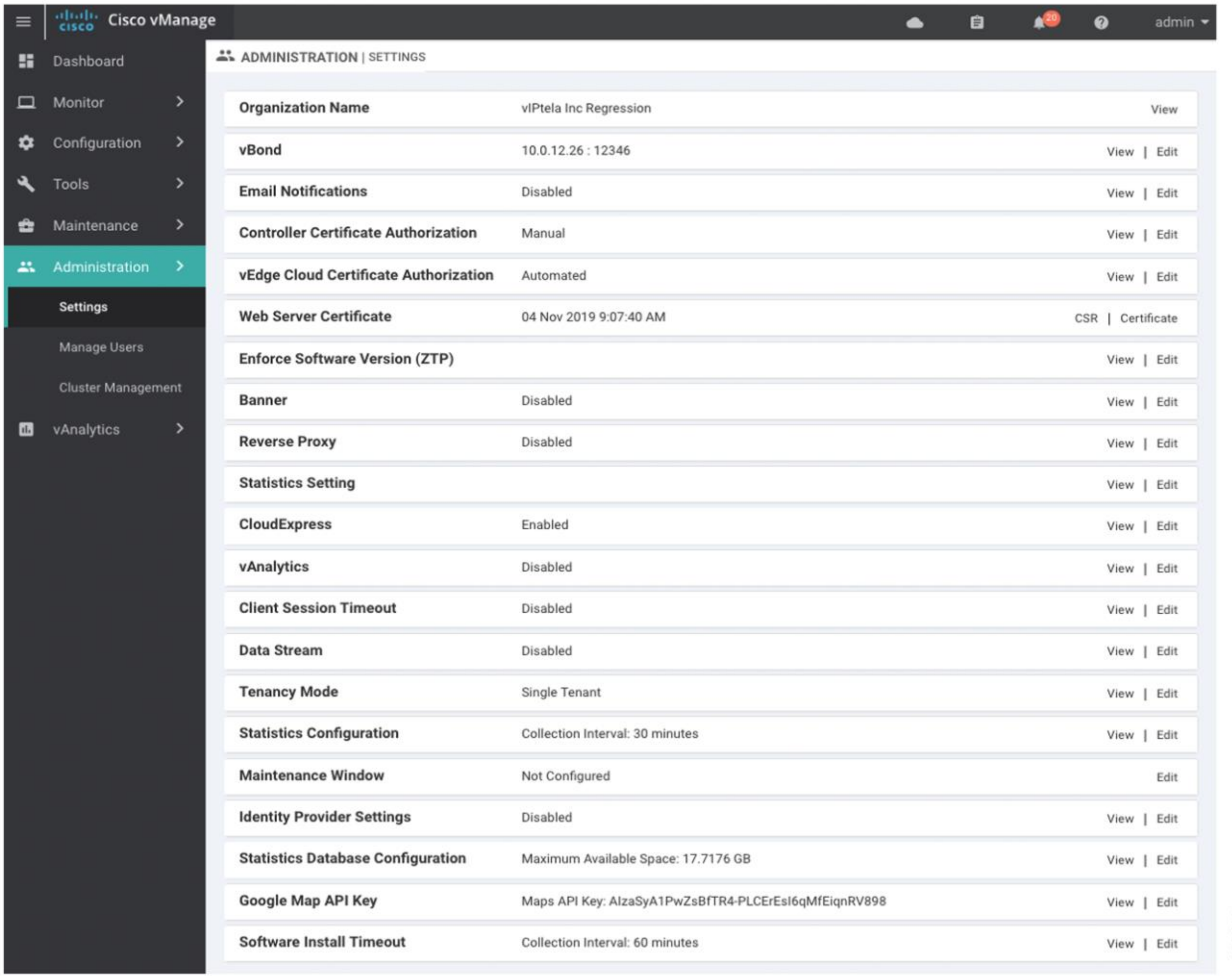
## Settings

Use the Settings screen to view the current settings and configure the setting for vManage NMS 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.

## Screen Elements

- Top bar—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.
- Title bar—Includes the title of the screen, Settings.
- Organization Name bar—Click View to view the organization name or Edit to edit the name.
- vBond bar—Click View to view the vBond DNS/IP address or Edit to enter new values.
- Email Notifications bar—Click View to view the settings for email notifications from the vManage server.
- Controller Certificate Authorization bar—Click View to view the certificate authorization settings or Edit to edit the settings.
- vEdge Cloud Certificate Authorization bar—Click View to view the vEdge Cloud certification authorization setting or Edit to edit the setting.
- Web Server Certificate bar—Click CSR to generate a Certificate Signing Request (CSR) for a web server certificate or Certificate to install the certificate.
- Enforce Software Version (ZTP) bar—Click View to view the software version enforced on a vEdge router or Edit to enforce a software version on the router.
- Banner bar—Click View to view the custom banner on the vManage login screen or Edit to edit or create a custom banner.
- Reverse Proxy bar—Click View to view the current settings for reverse proxy or Edit to edit the settings.
- Statistics Setting bar—Click View to view the current settings for collecting device statistics or Edit to edit the settings.
- Cloud onRamp bar—Click View to view the current settings for Cloud onRamp service or Edit to edit the setting.
- vAnalytics bar—Click View to view the current settings for the vAnalytics platform or Edit to edit the setting.
- Client Session Timeout bar—Click View to view the current vManage client session timeout setting or Edit to edit the setting.
- Identity Provider Settings—Click View to view the current vManage identity provider setting or Edit to edit the setting.
- Data Stream bar—Click View to view the current data streaming setting or Edit to edit the setting.
- Tenancy Mode bar—Click View to view the current tenancy setting or Edit to edit the setting.
- Statistics Configuration bar—Click View to view the current time interval for collecting device statistics or Edit to edit the setting.
- Maintenance Window bar—Click Edit to configure a maintenance time window notification.
- Statistics Database Configuration bar—Click View to view the current the vManage statistics database setting or Edit to edit the settings.




## Configure Organization Name

Before you can generate a CSR, you must configure the name of your organization. The organization name is included in the CSR.

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 not editable.

## Configure 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 vBond orchestrator and the port number to use to connect to it.
3. Click Save.

## Enable Email Notifications

You can configure the vManage NMS to send email notifications when alarms occur on devices in the overlay network. First configure the SMTP and email recipient parameters on this screen:

1. Click the Edit button to the right of the Email Notifications bar.
2. In the Enable Email Notifications field, click Enabled.
3. Select the security level for sending the email notifications. The security level can be none, SSL, or TLS.
4. In the SMTP Server field, enter the name or IP address of the SMTP server to receive the email notifications.
5. In the SMTP port field, enter the SMTP port number. For no security, the default port is 25; for SSL it is 465; and for TLS it is 587.
6. In the From Address field, enter the full email address to include as the sender in email notifications.
7. In the Reply To address, enter the full email address to include in the Reply-To field of the email. This address can be a noreply address, such as noreply@cisco.com.
8. To enable SMTP authentication to the SMTP server, click Use SMTP Authentication. Enter the username and password to use for SMTP authentication. The default user email suffix is appended to the username. The password that you type is hidden.
9. Click Save.

Then configure the alarms that trigger emails by clicking the Email Notifications button on the Monitor ► Alarms screen.

## 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 vManage NMS that you generate these certificates and install them on the controller devices—vBond orchestrators, vManage NMSs, and 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 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 the Certificate Retrieve Interval field, specify how often the 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:
   • Country: United States
   • State: California
   • City: San Jose
   • Organizational unit: vIPtela Inc Regression
   • Organization: vIPtela Inc
   • Domain name: viptela.com
   • Email: support@viptela.com
   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:
   vSmart# **show certificate signing-request decoded**
   ...
   Subject: C=US, ST=California, L=San Jose, OU=vIPtela Inc Regression, O=vIPtela Inc, CN=vsmart- *uuid* .viptela.com/emailAddress=support@viptela.com
   ...
   vSmart#

   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.

## Configure vEdge Cloud Certificate Authorization Settings

Certificates are used to authenticate vEdge Cloud routers in the overlay network. Once authentication is complete, vEdge Cloud routers can establish secure sessions with other devices in the overlay network.

By default, vEdge Cloud certification authorization is automated. This is the recommended setting.

If you use third-party certificate authorization, configure certificate authorization to be manual:

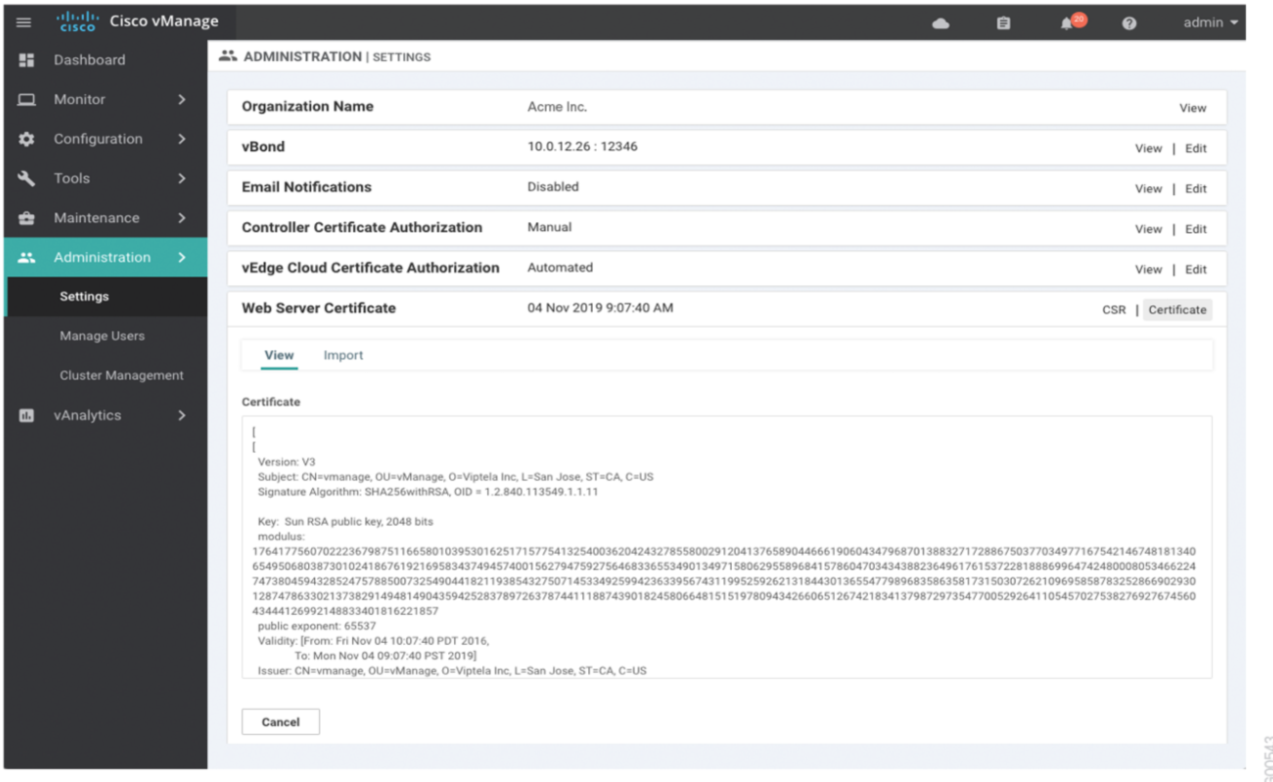
1. Click the Edit button to the right of the vEdge Cloud Certificate Authorization bar.
2. In the vEdge Cloud field, click Manual (Enterprise CA).
3. Click Save.

## Generate Web Server Certificate

To establish a secure connection between your web browser and the vManage server using authentication certificates, generate a CSR to create a certificate, have it signed by a root CA, and then install it. To do so:

1. Click the CSR button to the right of the Web Server Certificate bar.
2. In the Common Name field, enter the domain name or IP address of the vManage server. For example, the fully-qualified domain name of vManage could be vmanage.org.local.
3. In the Organizational Unit field, enter the unit name within your organization, for example, Network Engineering.
4. In the Organization field, enter the exact name of your organization as specified by your root CA, for example, Viptela Inc.
5. In the City field, enter the name of the city where your organization is located, for example, San Jose.
6. In the State field, enter the state in which your city is located, for example, California.
7. In the 2-Letter Country Code field, enter the two-letter code for the country in which your state is located. For example, the two-letter country code for the United States of America is US.
8. From the Validity drop-down, select the validity period for the certificate.
9. Click Generate to generate the CSR.
10. Send the CSR to Symantec or a root CA for signing.
11. When you receive the signed certificate, click the Certificate button to the right of the Web Server Certificate bar to install the new certificate. The View box displays the current certificate on the vManage server.
12. Copy and paste the new certificate in the box. Or click the Import button, click Select a File to download the new certificate file, and click Import.
13. Once the certificate is installed, reboot the vManage server.

Below is an example of a certificate generated with the above configuration. Note that the certificate is truncated in this example.




## View Web Server Certificate Expiration Date

When you establish a secure connection between your web browser and the vManage server using authentication certificates, you configure the time period for which the certification is valid (in Step 8 in the previous section). At the end of this time period, the certificate expires. The Web Server Certificate bar shows the expiration date and time.

Starting 60 days before the certificate expires, the vManage Dashboard displays a notification indicating that the certificate is about to expire. This notification is then redisplayed 30, 15, and 7 days before the expiration date, and then daily.

## Enforce Software Version on vEdge Routers

If you are using the Viptela ZTP hosted service, you can enforce a version of the Viptela software to run on a vEdge router when it first joins the overlay network. To do so:

1. Ensure that the software image for the desired vEdge router software version is present in the vManage software image repository:

    a. In vManage NMS, select the Maintenance ► Software Upgrade screen.

    b. In the Device List drop-down, click 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.

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

    d. Select the location from which to download the software images, either vManage or Remote Server.

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

    f. Click Upload or 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 Software Version drop-down, select the version of the software to enforce on vEdge routers when they join the network.

5. Click Save.

If you enable this feature on the vManage NMS, any vEdge router joining the network is configured with the version of the software specified in the Enforce Software Version field regardless of whether the router was running a higher or lower version of Viptela software.

## Create a Custom Banner

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

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.

## Enable Reverse Proxy

To enable reverse proxy services in the overlay network:

1. Click the Edit button to the right of the Reverse Proxy bar.

2. Click Enabled.

3. Click Save.

To configure reverse proxy on individual vManage NMS and vSmart controller devices, in vManage NMS select Configuration ► Devices and then click the Controllers tab. For the desired device, click the More Actions icon to the right of the row, and click Add Reverse Proxy. Then configure the private and proxy IP addresses and ports for the device.

For more information, see Enable Reverse Proxy .

## 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 Viptela 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.

## Enable Cloud onRamp Service

1. Click the Edit button to the right of the Cloud onRamp bar.
2. In the Enable Cloud onRamp field, click Enabled.
3. Click Save.

## Enable vAnalytics Platform

1. Click the Edit button to the right of the vAnalytics bar.
2. In the Enable vAnalytics field, click Enabled.
3. Click Save.

## Enable vManage Client Session Timeout

By default, a user's session to a vManage client remains established indefinitely and never times out. To set how long a vManage client session is inactive before a user is logged out:

1. Click the Edit button to the right of the Client Session Timeout bar.
2. In the Session Timeout field, click Enabled.
3. In the Timeout field, enter the timeout value, in minutes. This value can be from 10 to 180 minutes.
4. Click Save.

The client session timeout value applies to all vManage servers in a vManage cluster.

## Enable Single Sign-On

To enable single sign-on (SSO) for the vManage NMS to allow users to be authenticated using an external identity provider:

1. Ensure that you have enabled NTP on the vManage NMS.
2. Click the Edit button to the right of the Identity Provider Settings bar.
3. In the Enable Identity Provider field, click Enabled,
4. Copy and paste the identity provider metadata in the Upload Identity Provider Metadata box. Or click Select a File to upload the identity provider metadata file.
5. Click Save.

## Enable Data Stream Collection

By default, collecting streams of data from a network device is not enabled. To use the Packet Capture, Speed Test, and Debug Logs troubleshooting tools, you must enable the collection of data streams.

To collect data streams:

1. Click the Edit button to the right of the Data Stream bar.
2. In the Data Stream field, click Enabled.
3. In the Hostname field, enter the name of the host to which to send the collected data. Enter just the hostname (such as "test") with no domain name. It is recommended that this host be one that is used for out-of-band management and that is located in the management VPN.
4. In the VPN field, enter the number of the VPN in which the host is located. It is recommended that this be the management VPN, which is typically VPN 512.
5. Click Save.

## Set the Tenancy Mode

By default, the vManage server is in single-tenant mode, which enables it to manage a single overlay network. In single-tenant mode, the vManage server can manage up to 10,000 devices.

To place the vManage server in multitenant mode so that you can manage the overlay networks of multiple tenants:

1. Click the Edit button to the right of the Tenancy Mode bar.
2. In the Tenancy field, click Multitenant.
3. In the Domain field, enter the domain name for the service provider (for example, viptela.com).
4. Click Save. The vManage server reboots and comes back up in multitenant mode.

Note: After you place a vManage server into multitenant mode, you cannot convert it back to single-tenant mode.

In multitenant mode, you can configure up to 500 tenants and up to a total of 10,000 devices.

To configure tenants, go to the Administration ► Tenant Management screen.

## Set Interval to Collect Device Statistics

To set the time interval at which vManage NMS should collect statistics for devices in the overlay network:

1. Click the Edit button to the right of the Statistics Configuration bar. By default, statistics is collected for all Viptela devices every 30 minutes.
2. Click the up or down arrow in the Collection Interval drop-down to change the frequency at which to collect device statistics. The minimum time you can specify is 5 minutes and the maximum is 180 minutes.
3. Click Save.

## Configure a Maintenance Window

To configure a maintenance window for the vManage server:

1. Click the Edit button to the right of the Maintenance Window bar.
2. Click the Start date and time drop-down, and select the date and time when the maintenance window will start.
3. Click the End date and time drop-down, and select the date and time when the maintenance window will end.
4. 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.

To cancel a maintenance window for the vManage server:

1. Click the Edit button to the right of the Maintenance Window bar.
2. Click Cancel maintenance window.

## Configure the vManage Statistics Database

To configure the vManage statistics database, which stores all real-time statistics from the local vManage NMS:

1. Click the Edit button to the right of the Statistics Database Configuration bar. The Statistics Database Configuration screen opens. The Statistics Database Configuration bar shows the maximum space available for the database.
2. For each Statistics Type row, enter the maximum size of the statistics file, in gigabytes (GB). The total value of all fields cannot exceed the maximum available space.
3. Click Save.

vManage NMS updates the storage allocations you have assigned once a day, at midnight.

To view the actual and maximum size of statistics database on the vManage server:

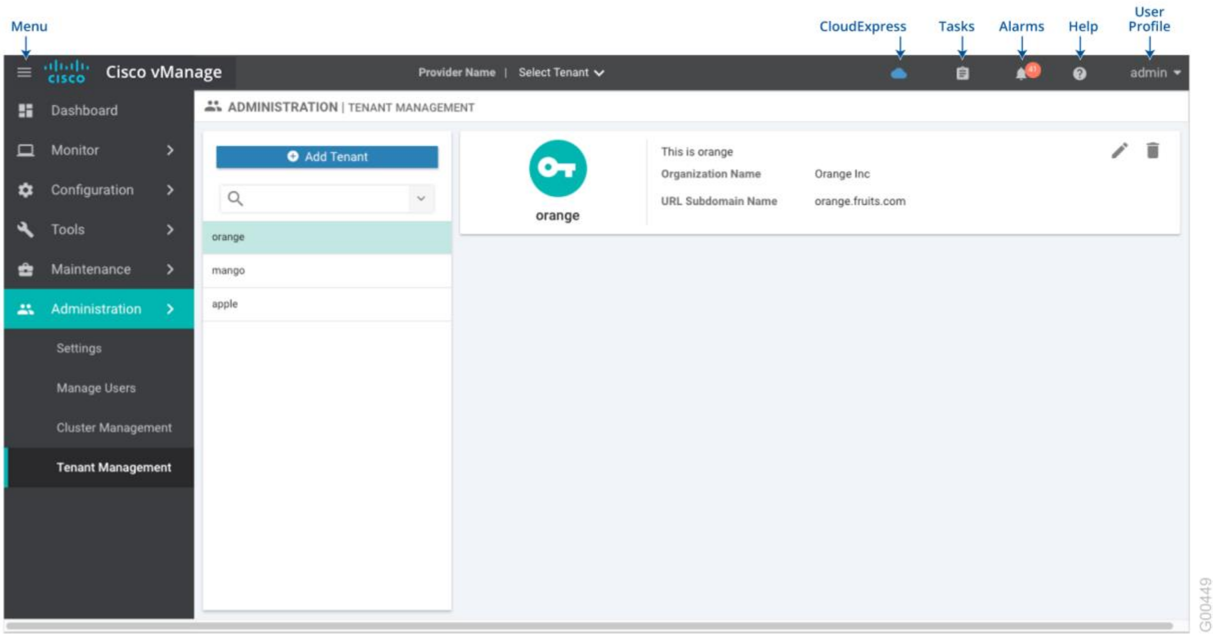
1. Click the Edit button to the right of the Statistics Database Configuration bar. The Statistics Database Configuration screen opens. The table on this screen shows, for each statistics type, the disk space currently being utilized.
2. Click Close.

## Tenant Management

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

## Screen Elements

- Top bar—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. In the middle is the name of the provider and the Select Tenant drop-down. On the right are a number of icons and the user profile drop-down.
- Title bar—Includes the title of the screen, Tenant Management.
- Add Tenant button—Add a new tenant to the provider's domain.
- Search box—Includes the Search Options drop-down, for a Contains or Match string.
- All tenants—The left pane lists all the tenants.
- Tenant—The right pane shows information for the tenant selected in the left pane.




## 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 Viptela 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. For example, for the provider viptela.com, a valid domain name might be plum.viptela.com. 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 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 vManage password and click Save.

## Additional Information

Multitenant Dashboard
Use a Multitenant vManage NMS

# Configuration

## Certificates

Use the Certificates screen to manage certificates and authenticate WAN edge and controller devices in the overlay network.

Two components of the Viptela solution provide device authentication:

- 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 vManage NMS that you generate these certificates and install them on the controller devices—vManage NMSs, vBond orchestrators, and vSmart controllers.
- WAN edge authorized serial number file contains the serial numbers of all valid vEdge and WAN routers in your network. You receive this file from Viptela, mark each router as valid or invalid, and then from the vManage NMS, send the file to the controller devices in the network.

You must install the certificates and the WAN edge authorized serial number file on the controller devices to allow the Viptela overlay network components to validate and authenticate each other and thus to allow the overlay network to become operational.

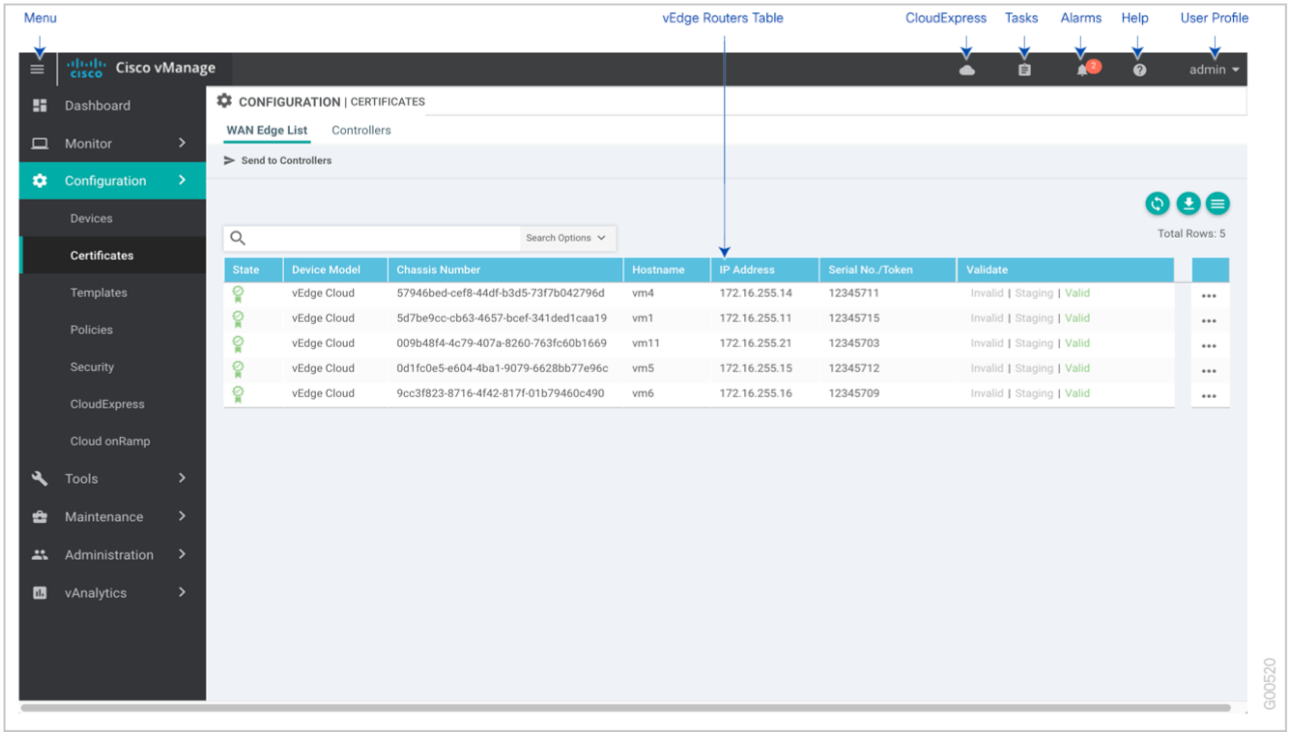
Note: For purposes of certificate management, the term *controller* is used to collectively refer to the vManage NMS, the vSmart controller, and the vBond orchestrator.

## Screen Elements

- Top bar—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.
- Title bar—Includes the title of the screen, Certificates.
- WAN Edge List tab—Install the router authorized serial number file on the controllers in the overlay network and manage the serial numbers in the file. When you first open the Certificates screen, the WAN Edge List tab is selected.
  - Send to Controllers—Send the WAN edge router chassis and serial numbers to the controllers in the network.
  - Table of WAN edge routers in the overlay network—To re-arrange the columns, drag the column title to the desired position.
- Controllers tab—Install certificates and download the device serial numbers to the vBond orchestrator.
  - Send to vBond—Send the controller serial numbers to the vBond orchestrator.
  - Install Certificate—Install the signed certificates on the controller devices. This button is available only if you select Manual in Administration ► Settings ► Certificate Signing by Symantec.
  - Export Root Certificate—Display a copy of the root certificate for the controller devices that you can download to a file.
  - Table of controller devices in the overlay network—To re-arrange the columns, drag the column title to the desired position.
  - Certificate status bar—Located at the bottom of the screen, this bar is available only if you select Server Automated in Administration ► Settings ► Certificate Authorization. It displays the states of the certificate installation process:
    - Device Added
    - Generate CSR
    - Waiting for Certificate
    - Send to Controllers

A green check mark indicates that the step has been completed. A grey check mark indicates that the step has not yet been performed.

- Search box—Includes the Search Options drop-down, for a Contains or Match string.
- Refresh icon—Click to refresh data in the device table with the most current data.
- Export icon—Click to download all data to a file, in CSV format.
- Show Table Fields icon—Click the icon to display or hide columns from the device table. By default, all columns are displayed.




## Check the WAN Edge Router Certificate Status

In the WAN Edge List tab, check the Validate column. The status can be one of the following:

- Valid (shown in green)—The router's certificate is valid.
- Staging (shown in yellow)—The router is in the staging state.
- Invalid (shown in red)—The router's certificate is not valid.

## Validate a WAN Edge Router

When you add vEdge and WAN routers to the network using the Configuration ▶ Devices screen, you can automatically validate the routers and send their chassis and serial numbers to the controller devices by clicking the checkbox Validate the uploaded WAN Edge List and send to controllers. If you do not select this option, you must individually validate each router and send their chassis and serial numbers to the controller devices. To do so:

1. In the WAN Edge List tab, select the router to validate.
2. In the Validate column, click Valid.
3. Click OK to confirm the move to the valid state.
4. Repeat Steps 1 to 3 for each router you wish to validate.

5. Click the Send to Controllers button in the upper left corner of the screen to send the chassis and serial numbers of the validated routers to the controller devices in the network. vManage NMS displays the Push WAN Edge List screen showing the status of the push operation.

## Stage a WAN Edge Router

When you initially bring up and configure a WAN Edge router, you can place it in staging state using the vManage NMS. When the router is in this state, you can configure the router, and you can test that the router is able to establish operational connections with the vSmart controller and the vManage NMS.

After you physically place the router at its production site, you change the router's state from staging to valid. It is only at this point that the router joins the actual production network. To stage a router:

1. In the WAN Edge List tab, select the router to stage.
2. In the Validate column, click Staging.
3. Click OK to confirm the move to the staging state.
4. Click Send to Controllers in the upper left corner of the screen to sync the WAN edge authorized serial number file with the controllers. vManage NMS displays the Push WAN Edge List screen showing the status of the push operation.

## Invalidate a WAN Edge Router

1. In the WAN Edge List tab, select the router to invalidate.
2. In the Validate column, click Invalid.
3. Click OK to confirm the move to the invalid state.
4. Repeat Steps 1 to 3 for each router you wish to invalidate.
5. Click the Send to Controllers button in the upper left corner of the screen to send the chassis and serial numbers of the validated routers to the controller devices in the network. vManage NMS displays the Push WAN Edge List screen showing the status of the push operation.

## Send the Controller Serial Numbers to vBond Orchestrator

To determine which controllers in the overlay network are valid, the vBond orchestrator keeps a list of the controller serial numbers. The vManage NMS learns these serial numbers during the certificate-generation process.

To send the controller serial numbers to the vBond orchestrator:

1. In the Controllers tab, check the certificate status bar at the bottom of the screen. If the Send to Controllers check mark is green, all serial numbers have already been sent to the vBond orchestrator. If it is grey, you can send one or more serial numbers to the vBond orchestrator.
2. Click the Send to vBond button in the Controllers tab.
   A controller's serial number is sent only once to the vBond orchestrator. If all serial numbers have been sent, when you click the Send to vBond button, an error message is displayed. To resend a controller's serial number, you must first select the device and then select Invalid in the Validity column.

After the serial numbers have been sent, click the Tasks icon in the vManage toolbar to display a log of the file download and other recent activities.

## Install Signed Certificate

If in Administration ► Settings ► Certificate Signing by Symantec, you selected the Manual option for the certificate-generation process, use the Install Certificate button to manually install certificates on the controller devices.

After Symantec or your enterprise root CA has signed the certificates, they return the files containing the individual signed certificates. Place them on a server in your local network. Then install them on each controller:

1. In the Controllers tab, click the Install Certificate button.
2. In the Install Certificate window, select a file, or copy and paste the certificate text.
3. Click Install to install the certificate on the device.
   The certificate contains information that identifies the controller, so you do not need to select the device on which to install the certificate.
4. Repeat Steps 1 to 3 to install additional certificates.

## Export Root Certificate

1. In the Controllers tab, click the Export Root Certificate button.
2. In the Export Root Certificate window, click Download to export the root certificate to a file.
3. Click Close.

## View the CSR

1. In the WAN Edge List or Controllers tab, select a device.
2. Click the More Actions icon to the right of the row, and click View CSR to view the certificate signing request (CSR).

## View the Certificate

1. In the Controllers tab, select a device.
2. Click the More Actions icon to the right of the row and click View Certificate.

## Generate the CSR

1. In the Controllers tab, select a device.
2. Click the More Actions icon to the right of the row and click Generate CSR.
3. In the Generate CSR window, click Download to download the file to your local PC (that is, to the PC you are using to connect to the vManage NMS).
4. Repeat Steps 1 to 4 for each controller for which you are generating a CSR.

## Reset the RSA Key Pair

1. In the Controllers tab, select a device.
2. Click the More Actions icon to the right of the row and click Reset RSA.

3. Click OK to confirm resetting of the device's RSA key and to generate a new CSR with new public/private keys.

## Invalidate a Device

1. In the Controllers tab, select a device.
2. Click the More Actions icon to the right of the row and click Invalidate.
3. Click OK to confirm invalidation of the device.

## View Log of Certificate Activities

To view the status of certificate-related activities:

1. Click the Tasks icon located in the vManage toolbar. vManage NMS displays a list of all running tasks along with the total number of successes and failures.
2. Click a row to see details of a task. vManage NMS opens a status window displaying the status of the task and details of the device on which the task was performed.

## Network Hub

Use the CloudDock screen to configure a CloudDock cluster and service groups to use with the cluster.

The CloudDock solutions securely connects enterprise applications that are hosted in an enterprise data center, in either a public, private or hybrid cloud, to the enterprise's employees, devices, customers, and partners.

## Screen Elements

- Top bar—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.
- Title bar—Includes the title of the screen, CloudDock.
- Cluster and Service Group tabs—When you first open the CloudDock screen, the Cluster tab is selected.
  - Cluster tab—Click to create a CloudDock cluster.
  - Service Group tab—Click to create a CloudDock service group.
- Cluster or Service Group table—If you have created at least one cluster or service group, these are listed in the table at the lower portion of the screen. If you have not created any CloudDock clusters or service groups, the lower portion of the screen displays either the Create CloudDock Cluster button or the Create Service Group button.

## Configure CloudDock

To configure CloudDock, you create a cluster and you create service groups. Order of configuration doesn't matter. In future, provider can create cluster and, for multiple tenants, each tenant can create their own service groups.

Three steps: 1. create cluster, 2. create service groups, 3. connect the clusters and service groups.

## Create a CloudDock Cluster

ADD INTRO

1. In vManage NMS, select the Configure ► CloudDock screen.
2. Select Cluster in the top bar.
3. If no cluster have yet been configured, click the Create CloudDock Cluster button.
   If at least one cluster has been configured, click the Configure & Provision Cluster button.
   The lower portion of the screen displays a graphical representation of the default cluster, which consists of two switches each connected to two Cisco Cloud Services Platforms (CSPs).
4. In the Cluster Name field, enter a name for the cluster. The name can be up to 128 characters and can contain only alphanumeric characters.
5. In the Description field, enter a description of the cluster. The description can be up to 2048 characters and can contain only alphanumeric characters.
6. In the Site ID field, enter the overlay network site identifier. This can be a value from 1 through 4294967295 ($2^{32} – 1$).
7. In the Location field, type the location of the cluster. The location can be up to 128 characters and can contain only alphanumeric characters.
8. Name each switch in the cluster:
   a. In the Switch box, click the switch icon. The Edit Switch dialog box is displayed on the right side of the screen.
   b. In the Name field, enter a name for the switch. The name can be up to 128 characters and can contain only alphanumeric characters.
   c. In the Serial Number drop-down, select the serial number of the switch.
   d. Click Save.
9. Name each CSP in the cluster:
   a. In the CSP box, click the CSP icon. The Edit Switch dialog box is displayed on the right side of the screen.
   b. In the Name field, enter a name for the CSP. The name can be up to 128 characters and can contain only alphanumeric characters.
   c. In the Serial Number drop-down, select the serial number of the CSP.
   d. Click Save.
10. Add a CSP to the cluster:
    a. In the CSP and Cluster Settings tab bar, click CSP. The Edit Switch dialog box is displayed on the right side of the screen.
    b. In the Name field, enter a name for the CSP. The name can be up to 128 characters and can contain only alphanumeric characters.
    c. In the Serial Number drop-down, select the serial number of the CSP.
    d. Click Save.
11. Configure login credentials for the cluster:
    a. In the Cluster Settings box, click Credentials. The Credentials dialog box is displayed to the right of the screen.
    b. In the Template Name field, enter a name for the cluster credentials template. The name can be up to 128 characters and can contain only alphanumeric characters.

c. In theDescription field, enter a description of the credentials. The description can be up to 2048 characters and can contain only alphanumeric characters.

d. Click New User.

i. In the Name field, enter the user's name.

ii. In the Password field, enter the user's password.

iii. In the Role field, enter the TBD.

iv. Click Add.

v. Click Save. The Credentials box background changes from white to purple.

12. Configure the IP address pool for the cluster:

a. In the Cluster Settings box, click IP Pool. The IP Pool dialog box is displayed to the right of the screen.

b. In the Name field, enter a name for the IP address pool. The name can be up to 128 characters and can contain only alphanumeric characters.

c. In the Description field, enter a description of the IP address pool. The description can be up to 2048 characters and can contain only alphanumeric characters.

d. Click New User.

i. In the Name field, enter the user's name.

ii. In the Password field, enter the user's password.

iii. In the Service Chain VLAN Pool field, enter the numbers of the VLAN to use for service chains. To enter multiple numbers, separate them by commas. To enter a numeric range, separate the numbers with a hyphen (for example, 20-30). WHAT ARE THESE? VLAN range for bringing up VNFs, so each circuit has VLAN configured when it comes up

iv. In the VNF Management IP Pool field, enter the IP addresses to use for the virtualized network function (VNF). o enter multiple IP addresses, separate them by commas. To enter a range, separate the IP addresses with a hyphen (for example, 20-30). WHAT ARE THESE? IPs for secure interfaces; will be renamed

v. In the VNF Network Data Pool field, enter the IP addresses to use for VNF network and data traffic TBD. To enter multiple IP addresses, separate them by commas. To enter a range, separate the IP addresses with a hyphen (for example, 20-30). WHAT ARE THESE?

vi. In the Management Gateway field, enter the IP address of the gateway to the management network. for DNS to exit the cluster

vii. In the System IP Pool field, enter the IP addresses to use for system IP addresses. To enter multiple IP addresses, separate them by commas. To enter a range, separate the IP addresses with a hyphen (for example, 20-30). WHAT ARE THESE? IP pool to use for tunnel

viii. Click Add.

ix. Click Save. The Credentials box background changes from white to purple.

13. Optionally, configure NTP servers for the cluster:

a. In the Cluster Settings drop-down, select NTP. The NTP template configuration box is displayed to the right of the screen.

b. In the Template Name field, enter a name for the NTP template. The name can be up to 128 characters and can contain only alphanumeric characters.

c. In the Description field, enter a description of the NTP template. The description can be up to 2048 characters and can contain only alphanumeric characters.

d. In the Preferred server field, enter the IP address of the primary NTP server.

e. In the Backup server field, enter the IP address of the secondary NTP server.

f. Click Save. A purple NTP field is added to the Cluster Settings box.

14. Optionally, configure syslog parameters for the cluster:

    a. In the Cluster Settings drop-down, select System Log. The System Log template configuration box is displayed to the right of the screen.

    b. In the Template Name field, enter a name for the System Log template. The name can be up to 128 characters and can contain only alphanumeric characters.

    c. In the Description field, enter a description of the System Log template. The description can be up to 2048 characters and can contain only alphanumeric characters.

    d. In the Severity drop-down, select the severity of syslog messages to log.

    e. To configure s syslog server:

        i. Click New Server.

        ii. Type the IP address of a syslog server

    f. Click Save. A purple Syslog field is added to the Cluster Settings box.

15. Optionally, configure SNMP parameters for the cluster:

    a. In the Cluster Settings drop-down, select SNMP. The SNMP template configuration box is displayed to the right of the screen.

    b. In the Template Name field, enter a name for the SNMP template. The name can be up to 128 characters and can contain only alphanumeric characters.

    c. In the Description field, enter a description of the SNMP template. The description can be up to 2048 characters and can contain only alphanumeric characters.

    d. In the Shutdown field, TBD.

    e. In the Name of Device for SNMP field, enter a name for the SNMP server. The name can be up to 128 characters and can contain only alphanumeric characters.

    f. In the Contact Person field, enter a contact person's name. The name can be up to 128 characters and can contain only alphanumeric characters.

    g. In the Location of Device field, enter information the SNMP server's location. The text can be up to 128 characters and can contain only alphanumeric characters.

    h. To use SNMPv2, click V2:

        i. Configure one or more SNMP views, communities, trap groups and trap target servers.

        ii. Cck Save. A purple SNMP field is added to the Cluster Settings box.

    i. To use SNMPv3, click V3:

        i. Configure one or more SNMP users and groups, and configure trap information.

        ii. Cick Save. A purple SNMP field is added to the Cluster Settings box.

16. Click Save Cluster. The new cluster is listed in a table on the Cluster tab.

## Create a Service Group

ADD INTRO: for configuring VNF. Each service group consists of a service chain

1. In vManage NMS, select the Configure ► CloudDock screen.
2. Select Service Group in the top bar.
3. If no service groups have yet been configured, click the Create Service Group button.
   If at least one service group has been configured, click the TBD button.
   The Service Group configuration screen is displayed.
4. In the Service Name field, enter a name for the service. The name can be up to 128 characters and can contain only alphanumeric characters.
5. In the Description field, enter a description of the service. The description can be up to 2048 characters and can contain only alphanumeric characters.
6. Click Add Service Chain. The Add Service Chain dialog box is displayed to the right of the screen.
   a. In the Name field, enter a name for the IP address pool. The name can be up to 128 characters and can contain only alphanumeric characters.
   b. In the Description field, enter a description of the IP address pool. The description can be up to 2048 characters and can contain only alphanumeric characters.
   c. In the Bandwidth field, enter TBD.
   d. In the Input Handoff VLAN field, enter TBD.
   e. In the Output Handoff VLAN field, enter TBD.
   f. In the Service Chain drop-down, select the type of service chain device. The device chain can be a Firewall-Router, and Router-Firewall-Router chain, or a Firewall. You can also create a custom service.
   g. Click Add. A graphical representation of the service chain is display on the screen, showing all the configured service chains within each virtual network function (VNF).
7. Click a service chain device in the VNF to configure it. The Configure dialog box for that service chain is displayed to the right of the screen.
   a. For a Firewall, configure TBD. (Image Package; click Fetch VNF Properties. Click Configure when done. The Router icon background changes from white to purple.)
   b. For a Router, configure TBD. (Image Package; click Fetch VNF Properties. Click Configure when done. The Router icon background changes from white to turquoise.)
8. To add a router on either side of the service chain, click the Router Icon in the left bar, and drag the icon to its proper location. The Configure Router dialog box is displayed to the right of the screen:
   a. In the Serial Number drop-down, select the serial number for the router.
   b. In the Router Image Package drop-down, select the software image to load onto the router.
   c. In the Name field, enter the router's name.
   d. In the Password field, enter the administrative password for the router.
   e. In the CPU field, TBD

f. In the Memory field, enter the amount of memory to allocate for memory on the router, in megabytes (MB).

g. In the Disk field, enter the amount of memory to allocate for storage on the router, in gigabytes (GB).

h. WHAT ARE FIELD1 and FIELD2?

i. Click Enable HA to enable high availability on the router. WHAT DOES THIS DO?

j. Click Mark as First VNF to configure this router as the default service chain. WHY?

k. WHAT IS Share VNF to?

l. Click Save. The Router icon background changes from white to turquoise.

9. To add a firewall device on either side of the service chain, click the Firewall Icon in the left bar, and drag the icon to its proper location. The Configure Firewall dialog box is displayed to the right of the screen: [Now called Configure VNF]

   a. In the Image Package drop-down, select the software image to load onto the firewall device.

   b. In the Serial Number drop-down, select the serial number for the firewall device.

   c. In the Name field, enter the router's name.

   d. In the Password field, enter the administrative password for the router.

   e. In the CPU field, TBD this is a dropdown

   f. In the Memory field, enter the amount of memory to allocate for memory on the router, in megabytes (MB). this is a dropdown

   g. In the Disk field, enter the amount of memory to allocate for storage on the router, in gigabytes (GB).

   h. Click Transparent or Router. WHAT DO THESE MEAN

   i. Click Enable HA to enable high availability on the router. WHAT DOES THIS DO?

   j. Click Save. The Router icon background changes from white to purple.

10. Click Save. The new service group is listed in a table on the Service Group tab.

## Attach Service Groups to a Cluster

First step is to Activate

To complete the CloudDock configuration, you attach service groups to a cluster:

1. In vManage NMS, select the Configure ► CloudDock screen.
2. In the Cluster/Service Group bar, select Cluster. The table on the lower portion of the screen lists the configured clusters.
3. Click the More Actions icon to the right of the row, and click Attach Service Groups. The Attach Service Groups dialog box is displayed.
4. In the Available Service Groups box, on the left, click the desired service groups.
5. Click the arrow to move the service groups to the Selected Service Groups box.
6. Click Attach.

# Perform Cluster Operations

## View Cluster Information

1. In the Cluster/Service Group bar, select Cluster.
2. Select the cluster row from the table.
3. Click the More Actions icon to the right of the row, and click View.

The Cluster window opens, displaying the switches and CSPs in the cluster and showing which cluster settings have been configured.

## Edit a Cluster

1. In the Cluster/Service Group bar, select Cluster.
2. Select the cluster row from the table.
3. Click the More Actions icon to the right of the row, and click Edit. The Cluster window opens, displaying the switches and CSPs in the cluster and showing which cluster settings have been configured.
4. Edit the desired cluster elements.
5. Click Save Cluster.

## Attach Service Groups to a Cluster

TBD: See above?

## Detach Service Groups from a Cluster

TBD

## Activate a Cluster

Activating a cluster does TBD:

1. In the Cluster/Service Group bar, select Cluster.
2. Select the cluster row from the table.
3. Click the More Actions icon to the right of the row, and click Activate.
4. TBD

## Delete a Cluster

WHAT ARE THE AFFECTS OF DELETING A CLUSTER?

1. In the Cluster/Service Group bar, select Cluster.
2. Select the cluster row from the table.
3. Click the More Actions icon to the right of the row, and click Delete.
4. Click OK to confirm you want to delete the cluster.

## Perform Service Group Operations

### View a Service Group

TBD

## Additional Information

How To Configure CloudDock
Software Repository

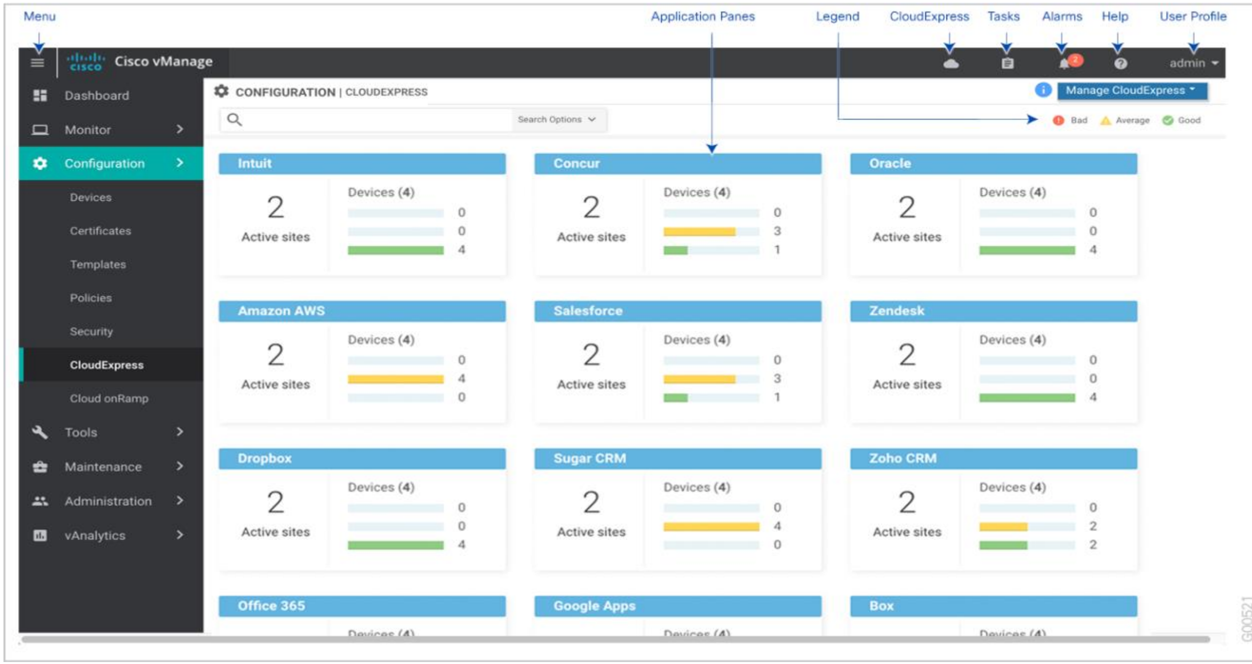
## Cloud onRamp

Use the Cloud onRamp dashboard to configure the Cloud onRamp for SaaS service and to view the performance of cloud applications for which you have enabled Cloud onRamp service.

Cloud onRamp service calculates a value called the Viptela Quality of Experience (vQoE). The vQoE value weighs loss and latency using a formula customized for each application. For example, email applications tolerate latency better than video applications do, and video applications tolerate loss better than email does. The vQoE value ranges from zero to ten, with zero being the worst quality and ten being the best. Cloud onRamp service computes vQoE values for applications and paths, then assigns applications to the paths that best match their vQoE value. Cloud onRamp service periodically recalculates vQoE values for paths to ensure ongoing optimal application performance.

## Screen Elements

- Top bar—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.
- Title bar—Includes the title of the screen, Cloud onRamp.
- Search box—Includes the Search Options drop-down, for a Contains or Match string.
- Application panes—Display performance of individual applications.
- Legend—Indicates quality of experience levels for cloud applications.
- Manage Cloud onRamp—Manage Cloud onRamp applications, client sites, gateways, and Direct Internet Access (DIA) sites.



## View Application Performance

Each pane in the Cloud onRamp dashboard displays the performance of a cloud application.

Each application pane displays the number of vEdge routers accessing the application and the quality of the connection:

- The bottom status bar displays green for devices experiencing good quality.
- The middle status bar displays yellow for devices experiencing average quality.
- The top status bar displays red for devices experiencing bad quality.

The number to the right of each status bar indicates how many devices are experiencing that quality of connection.

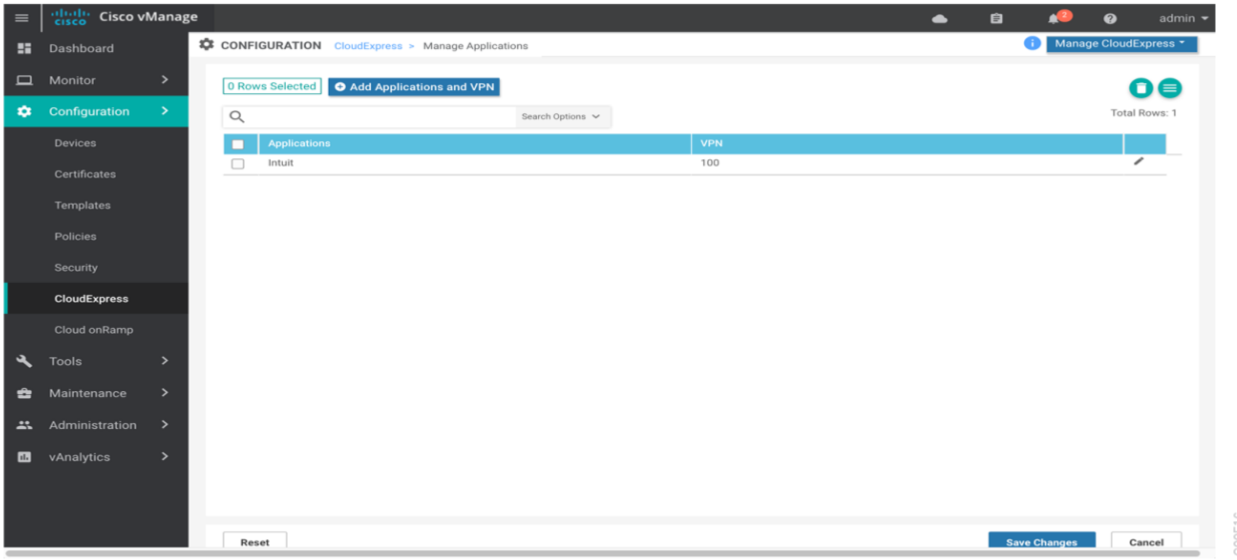
## View Details about an Application

1. Click in an application's pane. vManage NMS displays a list of sites accessing the application.
2. Click a graph icon in the vQoE Score column to display vQoE history for that site.
   - Click the time duration links to adjust the data the chart displays.
   - Hover over a point on the chart to display vQoE details for that point in time.

## Manage Cloud onRamp Applications

Select Manage Cloud onRamp ► Applications. The screen changes and displays the following elements:

- Add Applications and VPN—Add applications to Cloud onRamp service.
- Applications table—Display applications and VPNs configured for Cloud onRamp service.




To edit the VPN configured for an application, click the Edit icon for that application, then enter the new VPN. You can enter any VPN other than 0, which is the transport VPN, or 512, which is the management VPN.

To add applications to Cloud onRamp service:

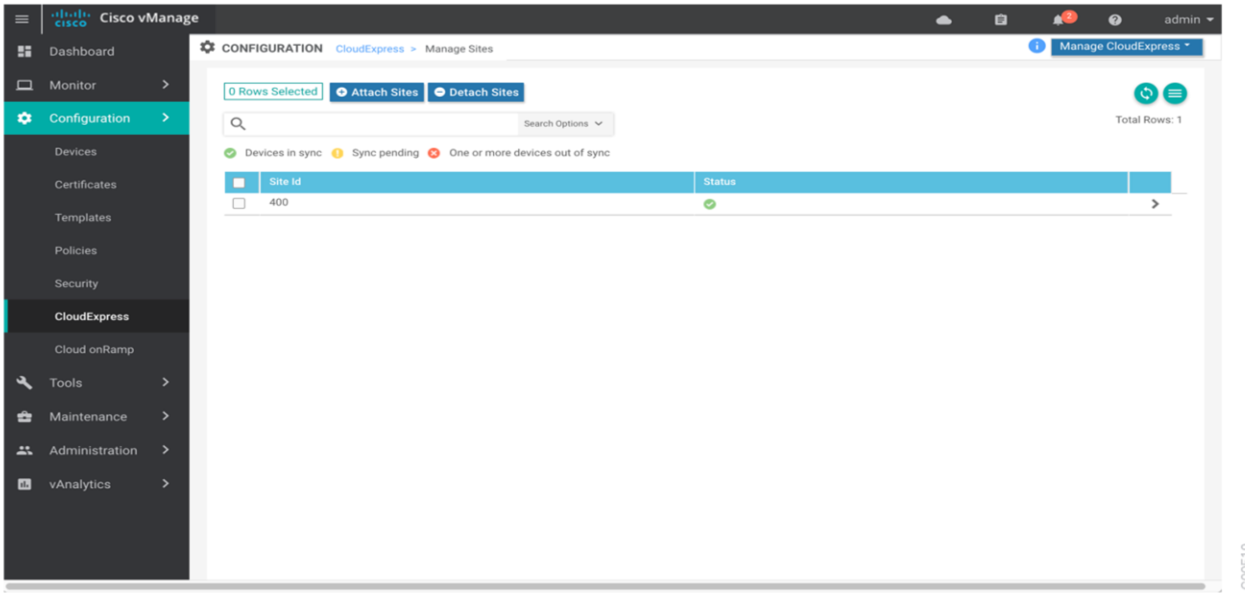
1. From the Manage Cloud onRamp drop-down, located to the right of the title bar, select Applications.
2. Click the Add Applications and VPN button. The Add Applications & VPN popup window displays.
3. In the Applications field, select an application.
4. In the VPN field, enter the service VPN in which that application runs. You can enter any VPN other than 0 and 512.
5. Click Add.
6. Repeat Steps 2 through 4 for each application you want to add.
7. Click Save Changes.

## Manage Cloud onRamp Client Sites

Client sites in Cloud onRamp service choose the best gateway site for each application to use for accessing the internet.

In the title bar, select Manage Cloud onRamp ▶ Client Sites. The screen changes and displays the following elements:

- Attach Sites—Add client sites to Cloud onRamp service.
- Detach Sites—Remove client sites from Cloud onRamp service.
- Client sites table—Display client sites configured for Cloud onRamp service.




To display details about a client site, select the site from the Client Sites Table and click the forward arrow located to the right of the row.

To detach a client site, select the site from the Client Sites Table and click Detach Sites.

To add client sites to Cloud onRamp service:

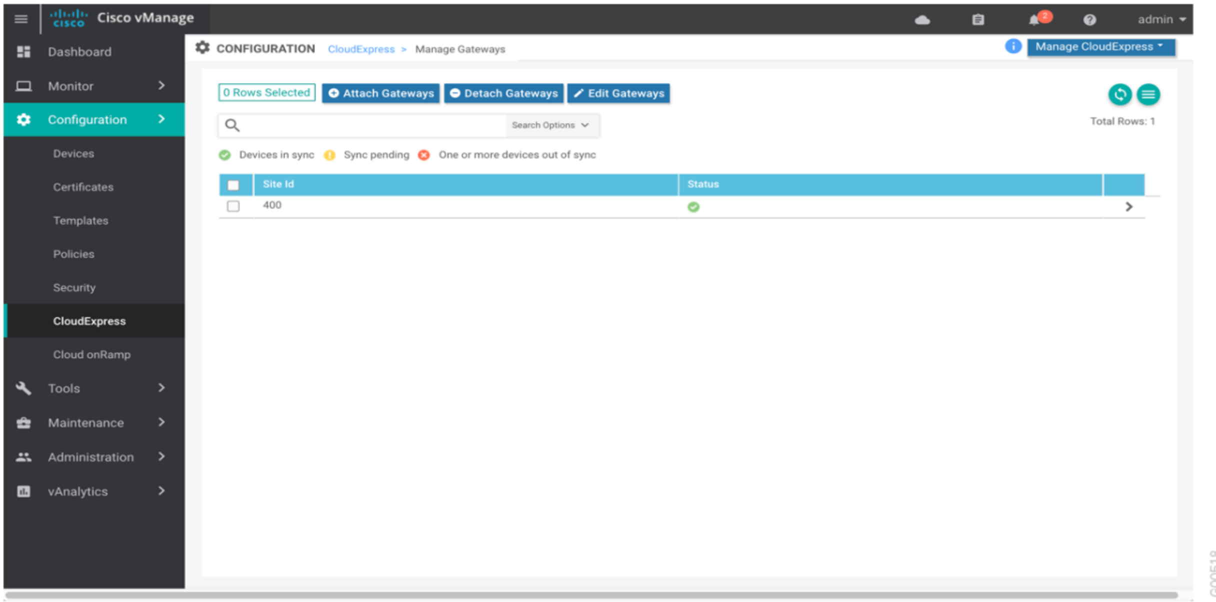
1. Click Attach Sites. The Attach Sites popup window displays all sites in your overlay network, with available sites highlighted. For a site to be available, all devices at that site must be running in vManage mode.
2. In the Available Sites pane, select a site to attach and click the right arrow. If you wish to remove a site from the Selected Sites pane, select the site and click the left arrow.
3. Click Attach to push the new template to the vEdge routers.

## Manage Cloud onRamp Gateways

Gateway sites in Cloud onRamp service choose the best network path for application traffic that originates at client sites.

In the title bar, select Manage Cloud onRamp ► Gateways. The screen changes and displays the following elements:

- Attach Gateways—Attach gateway sites.
- Detach Sites—Remove gateway sites from Cloud onRamp service.
- Edit Sites—Edit interfaces on gateway sites.
- Gateways table—Display gateway sites configured for Cloud onRamp service.




To display details about a gateway site, select the site from the Gateways Table and click the forward arrow located to the right of the row.

To detach a gateway site, select the site from the Gateways Table and click Detach Gateways.

To attach gateways:

1. Click Attach Gateways. The Attach Gateways screen displays. The Site List shows all available sites in your overlay network. For a site to be available, all devices at that site must be running in vManage mode.
2. In the Available Gateways pane, select a site to attach and click the right arrow. If you wish to remove a site from the Selected Sites pane, select the site and click the left arrow.
3. If you would like to specify GRE interfaces for Cloud onRamp service to use:
   a. Click Add Interfaces to Selected Sites.
   b. In the Interfaces drop-downs, add GRE interfaces.

If you do not specify interfaces for Cloud onRamp service to use, the system will select a NAT-enabled physical interface from VPN 0.

4. Click Attach to push the new template to the vEdge routers.

To edit Cloud onRamp interfaces on gateway sites:

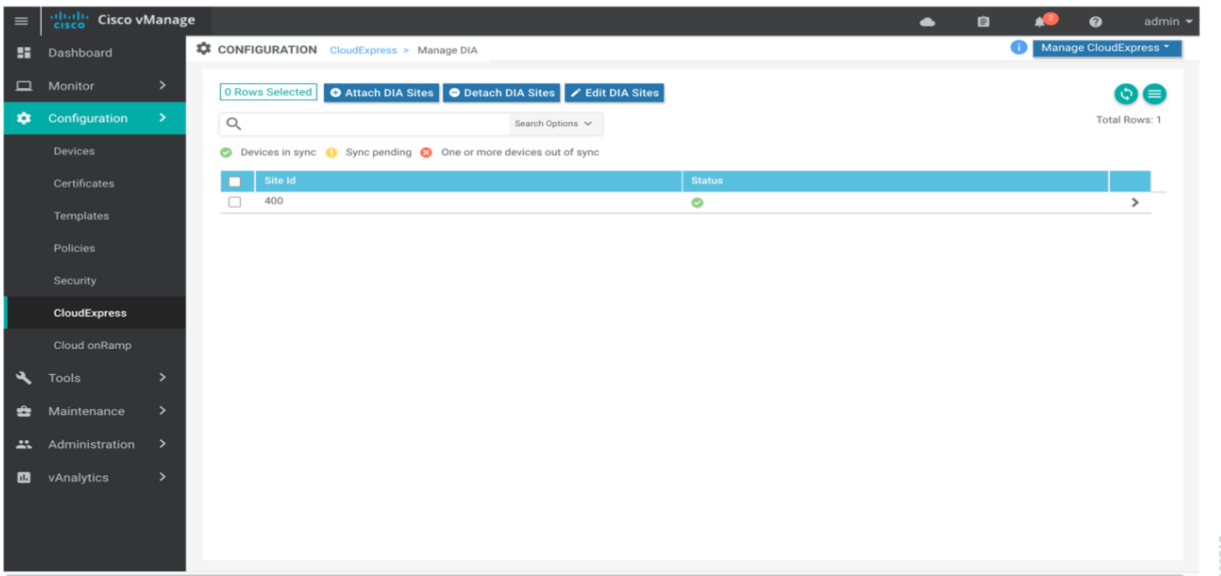
1. Select the sites you want to edit and click Edit Gateways.
2. In the Edit Interfaces of Selected Sites screen, select a site to edit.
   – To add interfaces, click the Interfaces field to select available interfaces.
   – To remove an interface, click the X beside its name.
3. Click Save Changes to push the new template to the vEdge routers.

# Manage Cloud onRamp DIA Sites

In Cloud onRamp service, DIA sites choose the best internet path for the application to use. They also consider paths that exit to the internet through gateway sites.

In the title bar, select Manage Cloud onRamp ▶ DIA. The screen changes and displays the following elements:

- Attach DIA Sites—Attach DIA sites.
- Detach DIA Sites—Remove DIA sites.
- Edit DIA Sites—Edit interfaces on DIA sites.
- Sites table—Display sites configured for Cloud onRamp service.




To display details about a site, select the site from the Sites Table and click the forward arrow located to the right of the row.

To detach a DIA site, select the site from the Sites Table and click Detach DIA Sites.

To attach DIA sites:

1. Click Attach DIA Sites. The Attach DIA Sites screen displays. The Site List shows all sites in your overlay network, with available sites highlighted. For a site to be available, all devices at that site must be running in vManage mode.
2. In the Available Sites pane, select a site to attach and click the right arrow. If you wish to remove a site from the Selected Sites pane, select the site and click the left arrow.
3. If you would like to specify GRE interfaces for Cloud onRamp service to use:
    a. Click Add Interfaces to Selected Sites.
    b. In the Interfaces drop-downs, add GRE interfaces.

If you do not specify interfaces for Cloud onRamp service to use, the system will select a NAT-enabled physical interface from VPN 0.

4. Click Save Changes to push the new template to the vEdge routers.

To edit Cloud onRamp interfaces on DIA sites:

1. Select the sites you want to edit and click Edit DIA Sites.

2. In the Edit Interfaces of Selected Sites screen, select a site to edit.
   - To add interfaces, click the Interfaces field to select available interfaces.
   - To remove an interface, click the X beside its name.
3. Click Save Changes to push the new template to the vEdge routers.

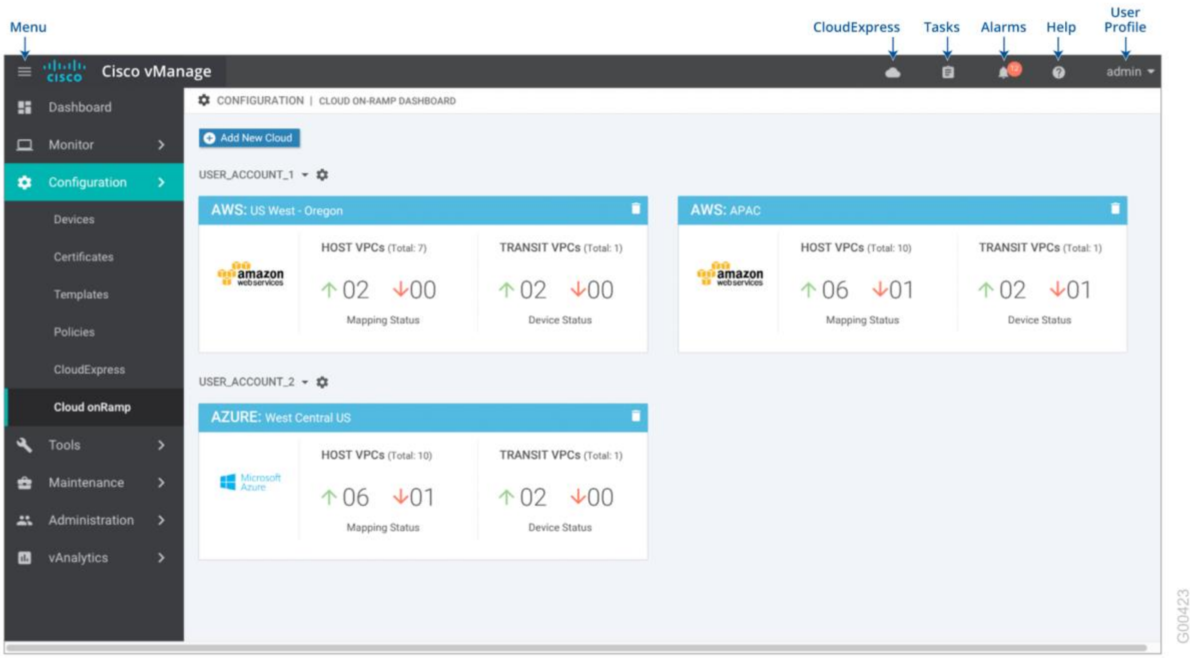
## Cloud OnRamp with AWS

Use the Cloud OnRamp screen to create virtual private cloud (VPC) instances for hosting vEdge Cloud routers in different AWS regions in the public internet. A Cloud OnRamp setup comprises three components:

- A transit VPC, which connects a Viptela overlay network to one or more cloud-based applications.
- A host VPC, which is where cloud-based applications reside.
- The connections, or mappings, between the transit VPC and one or more host VPCs.

## Screen Elements

- Top bar—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.
- Title bar—Includes the title of the screen, Cloud OnRamp.
- Add New Cloud Instance—Click to create a Cloud OnRamp VPC instance using the cloud instance configuration wizard.
- Cloud OnRamp Dashboard—Displays after you add at least one region in an Account.
   - VPC panes—Located on the Cloud OnRamp Dashboard, directly under the Add New Cloud Instance button, is a pane for each region corresponding to an account that has been created. Each pane shows:
      - Account number or account name used for logging in to AWS
      - Number of up and down IPsec connections for mapped host VPCs
      - Number of up and down control connections for vEdge router instances within the transit VPCs




## Create a Cloud Instance

1. Click Add New Cloud Instance.
2. In the Add Cloud Instance–Log In to a Cloud Server popup:
    a. In the Cloud drop-down, select the cloud type to be AWS.
    b. Click IAM Role or Key to log in to the cloud server. It is recommended that you use IAM Role.
    c. If you select IAM Role:
        i. In the Role ARN field, enter the role ARN of the IAM role.
        ii. In the External ID field, enter external ID created for the role ARN. It is recommended that the external ID include 10 to 20 characters in random order.
        To authenticate to the vManage NMS using an IAM role, vManage NMS must be hosted by Viptela on AWS and have the following attributes:
        • Trusts the AWS account, 200235630647, that hosts the vManage NMS.
        • Have all permissions for EC2 and VPC resources.
        • A default timeout of at least one hour.
        If vManage NMS is not hosted by Viptela on AWS, assign an IAM role with permissions to AssumeRole to the vManage server running the Cloud OnRamp process. Refer to the AWS documentation for details.
    d. If you select Key:
        i. In the API Key field, enter your Amazon API key.
        ii. In the Secret Key field, enter the password associated with the API key.
3. Click Login to log in to the cloud server.
The cloud instance configuration wizard opens. This wizard consists of three screens that you use to select a region and discover hosts VPCs, add transit VPC, and map host VPCs to transit VPCs.
A graphic on the right side of each wizard screen illustrates the steps in the cloud instance configuration process. Steps not yet

completed are shown in light gray. The current step is highlighted within a blue box. Completed steps are indicated with a green checkmark and are shown in light orange.

4. Select a region and discover host VPCs:
    a. In the Choose Region drop-down, select a geographical region.
    b. Click Discover Host VPCs. A list of host VPCs discovered in that region is displayed.
    c. Select the desired VPCs.
    d. Click Next.
5. Add a transit VPC:
    a. In the Transit VPC Name field, type a name for the transit VPC. The name can be up to 128 characters and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores (_). It cannot contain spaces or any other characters.
    b. Under Device Information, enter information about the transit VPC:
        i. In the vEdge Version drop-down, select the Viptela software version to run on the VPC transit.
        ii. In the Size of Transit vEdge drop-down, select how much memory and how many CPUs to create on the VPC transit.
        iii. In the Device 1 drop-down, select the serial number to use.
        iv. In the Device 2 drop-down, select the serial number to use.
        v. Click Advanced if you wish to enter more specific configuration options:
            1. In the Transit VPC Subnet field, enter a custom CIDR that has a network mask in the range of 16 to 25. If you choose to leave this field empty, the Transit VPC is created with a default CIDR of 10.0.0.0/16.
            2. In the SSH PEM Key drop-down, select a PEM key pair to log in to an instance.
            Note that the key pairs are region-specific. Refer to the AWS documentation for instructions on creating key pairs.
            3. Click Save and Finish to create the transit VPC. Or click Proceed to Mapping to continue with the wizard.
    c. Click Next.
6. Map the host VPCs to transit VPCs:
    a. In the table of host VPCs, select the desired host VPCs.
    b. Click Map VPCs. The Map Host VPCs popup opens.
    c. In the Transit VPC drop-down, select the transit VPC to map to the host VPCs.
    d. In the VPN drop-down, select the VPN in the overlay network in which to place the mapping.
    e. Click Map VPCs.
    f. Click Save and Complete.

## Display Host VPCs

1. In the Cloud OnRamp Dashboard, click the pane for the desired VPC. The Host VPCs/Transit VPCs screen opens, and Host VPCs is selected by default. In the bar below this, Mapped Host VPCs is selected by default, and the table on the screen lists the mapping between host and transit VPCs, the state of the transit VPC, and the VPN ID.

2. To list unmapped host VPCs, click Unmapped Host VPCs. Then click Discover Host VPCs.
3. To display the transit VPCs, click Transit VPCs.

## Map Host VPCs to a Transit VPC

1. In the Cloud OnRamp Dashboard, click the pane for the desired VPC. The Host VPCs/Transit VPCs screen opens.
2. Click Unmapped Host VPCs.
3. Click Discover Host VPCs.
4. From the list of discovered host VPCs, select the desired host VPCs
5. Click Map VPCs. The Map Host VPCs popup opens.
6. In the Transit VPC drop-down, select the desired transit VPC.
7. In the VPN drop-down, select the VPN in the overlay network in which to place the mapping.
8. Click Map VPCs.

## Unmap Host VPCs

1. In the Cloud OnRamp Dashboard, click the pane for the desired VPC. The Host VPCs/Transit VPCs screen opens.
2. Click Mapped Host VPCs.
3. From the list of VPCs, select the desired host VPCs.
4. Click Unmap VPCs.
5. Click OK to confirm the unmapping.

Unmapping host VPCs deletes all VPN connections to the VPN gateway in the host VPC, and then deletes the VPN gateway. When you make additional VPN connections to a mapped host VPC, they will be terminated as part of the unmapping process.

## Display Transit VPCs

1. In the Cloud OnRamp Dashboard, click the pane for the desired VPC. The Host VPCs/Transit VPCs screen opens, and Host VPCs is selected by default.
2. Click Transit VPCs.

The table at the bottom of the screen lists the transit VPCs.

## Add a Transit VPC

1. In the Cloud OnRamp Dashboard, click the pane for the desired VPC. The Host VPCs/Transit VPCs screen opens, and Host VPCs is selected by default.
2. Click Transit VPCs.
3. Click Add Transit VPC.

## Delete a Transit VPC

1. In the Cloud OnRamp Dashboard, click the pane for the desired VPC. The Host VPCs/Transit VPCs screen opens, and Host VPCs is selected by default.
2. Click Mapped Host VPCs.
3. Select the desired host VPC, and click Unmap VPCs.
4. Click OK to confirm the unmapping.
5. Click Transit VPCs.
6. Click the Trash icon to the left of the row for the transit VPC.
7. Click OK to confirm.

## Additional Information

Cloud OnRamp with Azure
**Configuring Cloud OnRamp Service**

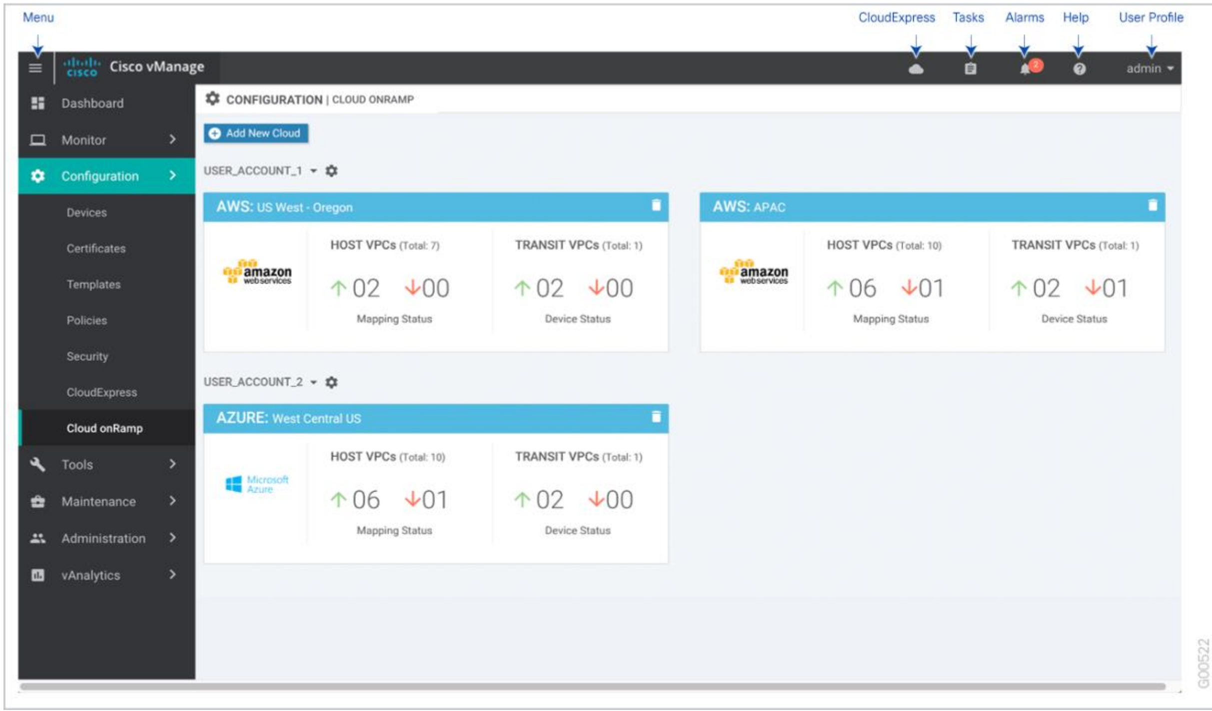
## Cloud OnRamp with Azure

Use the Cloud OnRamp screen to create transit virtual networks (VNets) for hosting vEdge Cloud router instances in different Azure locations in the public internet. A Cloud OnRamp setup comprises three components:

- A transit VNet, which connects a Viptela overlay network to one or more cloud-based applications.
- A host VNet, which is where cloud-based applications reside.
- The connections, or mappings, between the transit VNet and one or more host VNets.

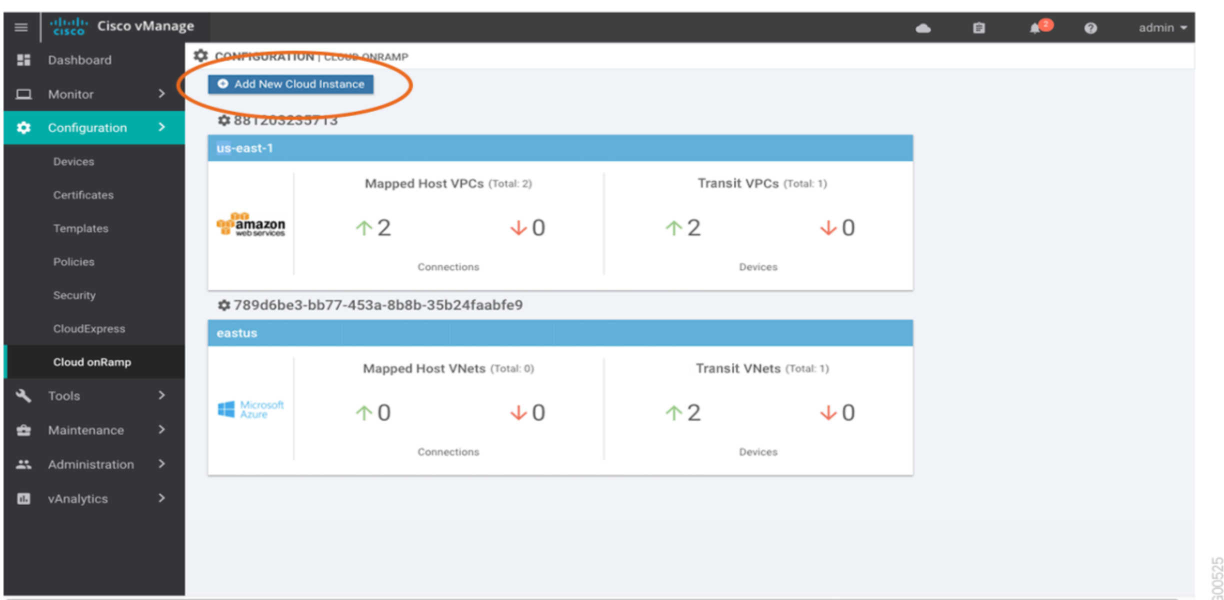
## Screen Elements

- Top bar—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.
- Title bar—Includes the title of the screen, Cloud OnRamp.
- Add New Cloud Instance—Click to create a Cloud OnRamp VNet instance using the cloud instance configuration wizard.
- Cloud OnRamp Dashboard—Displays after you add at least one cloud instance.
  - VNet panes—Located on the Cloud OnRamp Dashboard, directly under the Add New Cloud Instance button, is a pane for each VNet that has been created. For each VNet, the pane shows:
    - Credential value for the VNet
    - Name of the VNet
    - Type of VNet
    - Number of up and down connections for mapped host VNets
    - Number of up and down connections for transit VNets




# Create a Cloud Instance

1. Click Add New Cloud Instance:




2. In the Add Cloud Instance–Log In to a Cloud Server popup:

   a. In the Cloud drop-down, select the cloud type to be Azure.

b. To give vManage programmatic access to your Azure Subscription, log in to the cloud server:

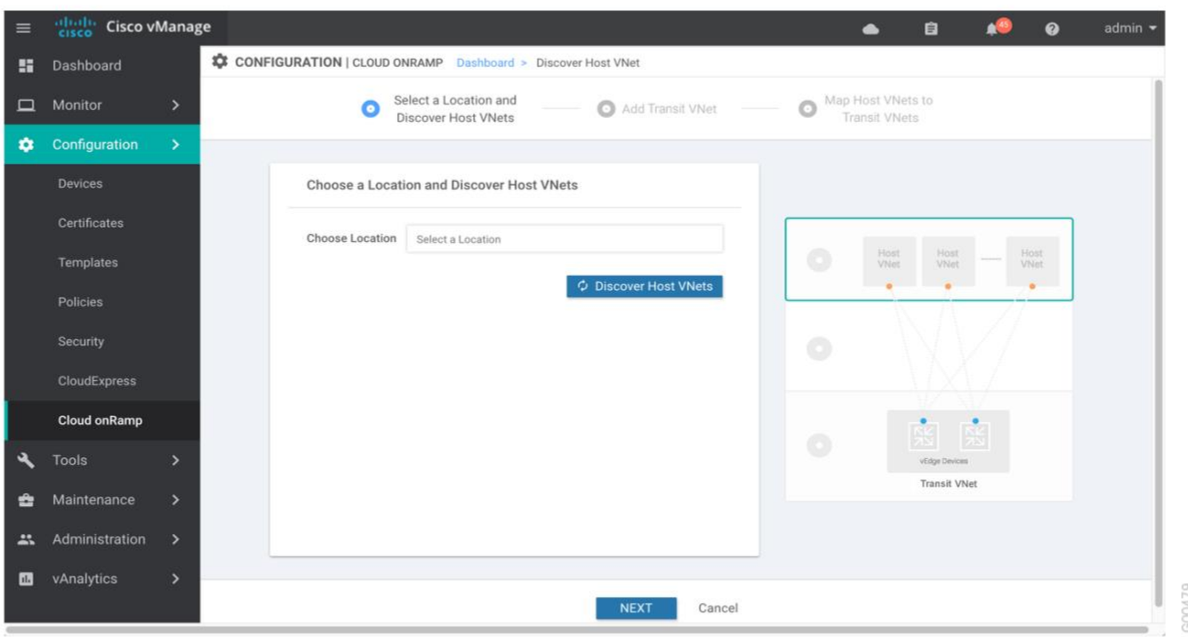
i. In the Subscription ID field, enter the ID of the Azure subscription you want to use as part of the Cloud onRamp workflow.

ii. In the Client ID field, enter the ID of an existing application or create a new application in Azure. To create a new application, go to your Azure Active Directory ► App Registrations ► New Application Registration.

iii. In the Tenant ID field, enter the ID of your Azure account. To find the tenant ID, go to your Azure Active Directory and click Properties.

iv. In the Secret Key field, enter the password associated with the client ID.

3. Click Log In.
The cloud instance configuration wizard opens. This wizard consists of three screens that you use to select a location and discover host VNets, add transit VNet, and map host VNets to transit VNets.
A graphic on the right side of each wizard screen illustrates the steps in the cloud instance configuration process. Steps not yet completed are shown in light gray. The current step is highlighted within a blue box. Completed steps are indicated with a green checkmark and are shown in light orange.




4. Select a location and discover host VNets:

a. In the Choose Location drop-down, select a geographical location.

b. Click Discover Host VNets. A list of host VNets discovered in that location is displayed.

c. Select the desired VNet.

d. Click Next.

5. Add a transit VNet:

a. In the Transit VNet Name field, type a name for the transit VNet. The name can be up to 32 characters and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores (_). It cannot contain spaces or any other characters.

b. Under Device Information, enter information about the transit VNet:

i. In the WAN Edge Version drop-down, select the Viptela software version to run on the VNet transit. The drop-down lists the published versions of the Viptela software in the Azure marketplace.

ii. In the Size of Transit VNet drop-down, select how much memory and how many CPUs to create on the VNet transit.

iii. In the Device 1 drop-down, select the serial number to use.

iv. In the Device 2 drop-down, select the serial number to use.

v. Click Advanced if you wish to enter more specific configuration options.

vi. In the Transit VPC Subnet field, enter a custom CIDR that has a network mask in the range of 16 to 25. If you choose to leave this field empty, the Transit VPC is created with a default CIDR of 10.0.0.0/16.

c. Click Next.

6. Map the host VNets to transit VNets:

a. In the table of host VNets, select the desired host VNet.

b. Click Map VNets. The Map Host VNets popup opens.

c. In the Transit VNet drop-down, select the transit VNet to map to the host VNets.

d. In the VPN drop-down, select the VPN in the overlay network in which to place the mapping.

e. In the IPSec Tunnel CIDR section, enter two pairs of interface IP addresses for each vEdge Cloud router to configure IPSec tunnels to reach the Azure virtual network transit. The IP addresses must be network addresses in the /30 subnet, be unique across the overlay network, and not be a part of the host VNet CIDR. If they are part of the host VNet CIDR, Azure will return an error while attempting to create VPN connections to the transit VNet.

f. In the Azure Information section:

i. In the BGP ASN field, enter the ASN that will be configured on the Azure Virtual Network Transit that is spun up within the host VNet. Use an ASN that is not part of an existing configuration on Azure. For acceptable ASN values, refer to Azure documentation.

ii. In the Host VNet Gateway Subnet field, enter a host VNet subnet in which the Virtual Network Gateway can reside. It is recommended you use a /28 subnet or higher. You must not provide a subnet that is already created in the VNet.

g. Click Map VNets.

h. Click Save and Complete.

When you configure the two vEdge Cloud routers that form the transit VNet, ensure that the color you assign to the tunnel interface in the VPN feature configuration template for VPN 0, is a public color, not a private color. Public colors are **3g** , **biz-internet** , **blue** , **bronze** , **custom1** , **custom2** , **custom3** , **default** , **gold** , **green** , **lte** , **metro-ethernet** , **mpls** , **public-internet** , **red** , and **silver** .

## Display Host VNets

1. In the Cloud OnRamp Dashboard, click the pane for the desired VNet. The Host VNets/Transit VNets screen opens, and Host VNets is selected by default. In the bar below this, Mapped Host VNets is selected by default, and the table on the screen lists the mapping between host and transit VNets, the state of the transit VNet, and the VPN ID.

2. To list unmapped host VNets, click Unmapped Host VNets.

3. To display the transit VNets, click Transit VNets.

## Map Host VNets to an Existing Transit VNet

1. In the Cloud OnRamp Dashboard, click the pane for the desired location of the required account. The Host VNets/Transit VNets screen opens.
2. Click Unmapped Host VNets.
3. Click Discover Host VNets.
4. From the list of discovered host VNets, select the desired host VNet.
5. Click Map VNets. The Map Host VNets popup opens.
6. In the Transit VNet drop-down, select the desired transit VNet.
7. In the VPN drop-down, select the VPN in the overlay network in which to place the mapping.
8. Click Map VNets.

## Unmap Host VNets

1. In the Cloud OnRamp Dashboard, click the pane for the desired VNet. The Host VNets/Transit VNets screen opens.
2. Click Mapped Host VNets.
3. From the list of VNets, select the desired host VNets. It is recommended that you unmap one vNet at a time. If you want to unmap multiple vNets, do not select more than three in a single unmapping operation.
4. Click Unmap VNets.
5. Click OK to confirm the unmapping.

## Display Transit VNets

1. In the Cloud OnRamp Dashboard, click the pane for the desired VNets. The Host VNets/Transit VNets screen opens, and Host VNets is selected by default.
2. Click Transit VNets.

The table at the bottom of the screen lists the transit VNets.

## Add a Transit VNet

1. In the Cloud OnRamp Dashboard, click the pane for the desired VNet. The Host VNets/Transit VNets screen opens, and Host VNets is selected by default.
2. Click Transit VNets.
3. Click Add Transit VNet.

## Delete a Transit VNet

1. In the Cloud OnRamp Dashboard, click the pane for the desired VNet. The Host VNets/Transit VNets screen opens, and Host VNets is selected by default.
2. Click Mapped Host VNets.

3. Select the desired host VNet, and click Unmap VNets.
4. Click OK to confirm the unmapping.
5. Click Transit VNets.
6. Click the Trash icon to the left of the row for the transit VNet.
7. Click OK to confirm.

## Additional Information

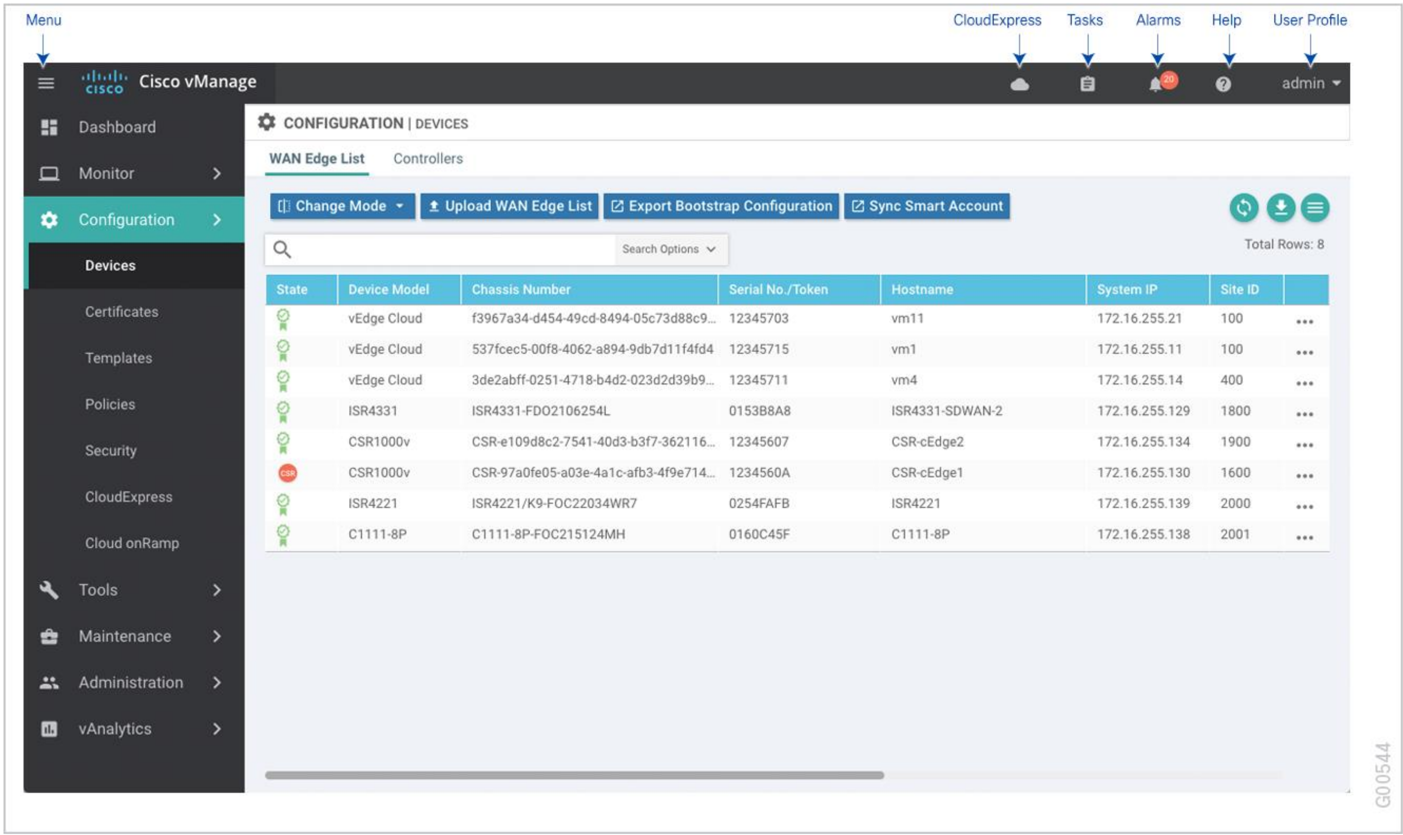
Cloud OnRamp with AWS
**Configuring Cloud OnRamp Service**

## Devices

Use the Devices screen to add or delete WAN Edge routers and controller devices from the overlay network. WAN Edge routers are vEdge and other WAN routers. Controller devices are the vManage NMS, the vSmart controller, and the vBond orchestrator.

## Screen Elements

- Top bar—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.
- Title bar—Includes the title of the screen, Devices.
- WAN Edge List tab—Upload the WAN Edge authorized serial number file to the vManage NMS. When you first open the Devices screen, the WAN Edge List tab is selected.
  - Change mode—Switch between vManage and CLI mode.
  - Upload WAN Edge List—Upload the WAN edge router authorized serial number file to the vManage NMS.
  - Export Bootstrap Configuration—Generate and download a bootstrap configuration for multiple vEdge Cloud routers.
  - Sync Smart Account—Download the updated device list to vManage NMS and send it to the vBond orchestrator.
  - Table of routers in the overlay network—To re-arrange the columns, drag the column title to the desired position.
- Controllers tab—Add controllers to the overlay network.
  - Add Controller drop-down—Add controllers to the overlay network.
  - Change mode drop-down—Switch between vManage and CLI mode.
  - Table of controller devices in the overlay network—To re-arrange the columns, drag the column title to the desired position.
- Search box—Includes the Search Options drop-down, for a Contains or Match string.
- Refresh icon—Click to refresh data in the device table with the most current data.
- Export icon—Click to download all data to a file, in CSV format.
- Show Table Fields icon—Click to display or hide columns from the device table. By default, all columns are displayed.



## Change Configuration Modes

To toggle a router from vManage mode to CLI mode:

1. In WAN Edge List tab, select a device.
2. Click the Change Mode drop-down and select CLI mode.

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

To toggle a controller device from vManage mode to CLI mode:

1. In the Controllers tab, select a device.
2. Click the Change Mode drop-down.
3. Select CLI mode and then select the device type. The Change Mode CLI window opens.
4. From the vManage mode pane, select the device and click the right arrow to move the device to the CLI mode pane.
5. Click Update to CLI Mode.

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

## Upload WAN Edge Router Authorized Serial Number File

The WAN Edge router authorized serial number file contains the chassis and serial numbers of all valid vEdge routers in the overlay network. You receive this file from Viptela. Then, from the vManage NMS, you send it to the controllers in the network. This file is required to allow the Viptela overlay network components to validate and authenticate each other and thus to allow the overlay network to become operational.

To upload the WAN edge router authorized serial number file to the vManage NMS and then download it to all the controllers in the overlay network:

1. In the WAN Edge List tab, click Upload WAN Edge List.
2. In the Upload WAN Edge List window:
    a. Click Choose File and select the WAN edge router authorized serial number file you received from Viptela.
    b. To automatically validate the routers and send their chassis and serial numbers to the controllers, ensure that the checkbox Validate the Uploaded WAN Edge List and Send to Controllers is selected. (It is selected by default.) If you do not select this option, you must individually validate each router in Configuration ► Certificates ► WAN Edge List.
    c. Click Upload.

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

## Upload WAN Edge Router Serial Numbers from Cisco Smart Account

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

1. In the WAN Edge List tab, click Sync Smart Account.
2. In the Sync Smart Account window:
    a. Enter the username and password for your Smart account..
    b. To automatically validate the routers and send their chassis and serial numbers to the controllers, ensure that the checkbox Validate the Uploaded WAN Edge List and Send to Controllers is selected. (It is selected by default.) If you do not select this option, you must individually validate each router in Configuration ► Certificates ► WAN Edge List.
    c. Click Sync.

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

## Generate Bootstrap Configuration for a vEdge Cloud Router

For vEdge Cloud routers, you need to generate a bootstrap configuration file that you use when you create vEdge cloud VM instances.

To generate and download a bootstrap configuration for one or more vEdge Cloud routers:

1. In the WAN Edge List tab, click the Export Bootstrap Configuration button.
2. In the Export Bootstrap Configuration window, in the Bootstrap Configuration field, click Cloud-Init or Encoded String, depending the Hypervisor you are using to bring up the vEdge Cloud router.
3. Select the devices to configure from the Available Devices pane, or click Select All to select all devices.
4. Click the right arrow to move the devices to the Selected Devices pane.
5. Click Generate Configuration. The configurations are downloaded to the vManage NMS.

6. Provision the vEdge Cloud router instance in AWS, KVM, or ESXi with the boostrap configuration.
   By default, ge0/0 is the device's tunnel interface and is a DHCP client. To use an interface other than ge0/0 as the tunnel interface or to use a static IP as the IP address, reconfigure the device through the CLI. For more information about configuring interfaces, see Configure Network Interfaces .

After you provision the vEdge Cloud router instance, vManage NMS installs a certificate on the device and the device's token changes to a serial number. After the device's control connections to vManage NMS come up, any templates attached to the device are automatically pushed to the device.

## Export Device Data in CSV Format

To export data for all devices to a file in CSV format, click the Export icon. This icon, which is a downward-pointing arrow, is located to the right of the filter criteria both in the WAN Edge List and in the Controllers tab.

vManage NMS downloads all data from the device table to an Excel file in CSV format. The file is downloaded to your brower's default download location and is named viptela_download.csv.

## View a Device's Running Configuration

To view a device's running configuration:

1. In the WAN Edge List or Controllers tab, select the device.
2. Click the More Actions icon to the right of the row and click Running Configuration.

## View a Device's Configuration

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

1. In the WAN Edge List or Controllers tab, select the device.
2. Click the More Actions icon to the right of the row and click Local Configuration.

## Delete a WAN Edge Router

Deleting a router removes its serial and chassis numbers from the WAN edge router serial number list and permanently removes the router's configuration from the vManage NMS.

1. In the Configuration ► Certificates screen, mark the WAN Edge router as invalid.
2. In the Configuration ► Devices screen, in the WAN Edge List tab, select the router.
3. Click the More Actions icon to the right of the row and click Delete WAN Edge.
4. Click OK to confirm deletion of the device.
5. In the Configuration ► Certificates screen, click Send to Controller.

## Copy Router Configuration

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

To copy the configuration from the old router to the new router:

1. In the Configuration ► Certificates screen, mark the new vEdge router as invalid.
2. In the Configuration ► Devices screen, in the WAN Edge List tab, select the old router.
3. Click the More Actions icon to the right of the row and click Copy Configuration.
4. In the Copy Configuration window, select the new router.
5. Click Update to confirm the copy of the configuration.

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

1. In the Configuration ► Certificates screen, mark the new router as valid.
2. Click Send to Controller.

## Decommission a vEdge Cloud Router

Decommissioning a vEdge Cloud router removes the device's serial number from vManage NMS and generates a new token for the device. To do so:

1. In the WAN Edge List tab, select a vEdge Cloud router.
2. Click the More Actions icon to the right of the row and click Decommission WAN Edge.
3. Click OK to confirm the decommissioning of the router.

## View Log of Template Activities

To view a log of activities related to creation of configuration templates and the status of attaching configuration templates to devices:

1. In the WAN Edge List or Controllers tab, select the device.
2. Click the More Actions icon to the right of the row and click Template Log.

## View Status of Device Bringup

To view the status of the operations involved in bringing a router or controller up in the overlay network:

1. In the WAN Edge List or Controllers tab, select the device.
2. Click the More Actions icon to the right of the row and click Device Bring Up.

## Add a vBond Orchestrator

1. In the Controllers tab, click the Add Controller drop-down and select vBond.
2. In the Add vBond window:
    a. Enter the management IP address of the vBond controller.
    b. Enter the username and password to access the vBond orchestrator.
    c. Select the Generate CSR checkbox to allow the certificate-generation process to occur automatically.

   d. Click Add.

3. Repeat Steps 1 and 2 to add additional vBond orchestrators.

The new vBond orchestrator is added to the list of controllers in the Controllers screen.

## Add a vSmart Controller

1. In the Controllers tab, click the Add Controller drop-down and select vSmart.
2. In the Add vSmart window:
   a. Enter the system IP address of the vSmart controller.
   b. Enter the username and password to access the vSmart controller.
   c. Select the protocol to use for control-plane connections. The default is DTLS.
   d. If you select TLS, enter the port number to use for TLS connections. The default is 23456.
   e. Select the Generate CSR checkbox to allow the certificate-generation process to occur automatically.
   f. Click Add.
3. Repeat Steps 1 and 2 to add additional vSmart controllers. The vManage NMS can support up to 20 vSmart controllers in the network.

The new vSmart controller is added to the list of controllers in the Controllers screen.

## Edit Controller Details

To edit the IP address and login credentials of a controller device:

1. In the Controllers tab, select the controller.
2. Click the More Actions icon to the right of the row and click Edit.
3. In the Edit window, edit the IP address and the login credentials.
4. Click Save.

## Delete a Controller

1. In the Controllers tab, select the controller.
2. Click the More Actions icon to the right of the row and click Invalidate.
3. Click OK to confirm the removal of the device and all its control connections.

## Configure Reverse Proxy on Controllers

To configure reverse proxy on an individual vManage NMS and vSmart controller device:

1. In the Controllers tab, select the device.
2. Click the More Actions icon to the right of the row, and click Add Reverse Proxy. The Add Reverse Proxy popup is displayed.
3. Click Add Reverse Proxy.

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

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

6. If the vManage NMS or vSmart controller has multiple cores, repeat Steps 4 and 5 for each core.

7. Click Add.

To enable reverse proxy in the overlay network, in vManage NMS select Administration ► Settings . Then click Edit to the right of the Reverse Proxy bar, click Enabled, and click Save.

## IPv6 Functionality

This article describes the options for enabling IPv6 functionality for Cisco SD-WAN templates and policies.

## Configure IPv6 Functionality for an Interface or Subinterface Template

To configure IPv6 functionality for an interface or subinterface template, follow these steps:

1. In Cisco vManage NMS, select the **Configuration** ► **Templates** screen.

2. Select **Feature** ► **Add Template** and then select an appropriate device model.

3. Select **VPN Interface Ethernet** from the list of templates.

4. In the Basic Configuration area, click the **IPv6** button and configure the parameters that the following table describes.

| Parameter Name | Description |
|---|---|
| Static | This radio button is selected by default because IPv6 addresses are static. |
| IPv6 Address | Enter the IPv6 address of the interface or subinterface. |

## Configure IPv6 Functionality for an OMP Template

To configure IPv6 functionality for an Overlay Management Protocol (OMP) template, follow these steps:

1. In Cisco vManage NMS, select the **Configuration** ► **Templates** screen.

2. Select **Feature** ► **Add Template** and then select an appropriate device model.

3. Select **OMP** from the list of templates.

4. In the Basic Configuration area, click the **IPv6** button in the ADVERTISE area and configure the parameters that the following table describes.

Parameter Name

Description

BGP

Click **On** to advertise BGP routes to OMP. By default, BGP routes are not advertised to OMP.

Connected

Click **Off** to disable advertising connected routes to OMP.

By default, connected routes are advertised to OMP.

Static

Click **Off** to disable advertising static routes to OMP.

By default static routes are advertised to OMP.

## Configure IPv6 Functionality for a BGP Template

To configure IPv6 functionality for a Border Gateway Protocol (BGP) template, follow these steps:

1. In Cisco vManage NMS, select the **Configuration ▶ Templates** screen.
2. Select **Feature ▶ Add Template** and then select an appropriate device model.
3. Select **BGP** from the list of templates.
4. In the Unicast Address Family area, click the **IPv6** button and configure the parameters that the following table describes.

Tab

Parameter Name

Description

Maximum Paths

Specify the maximum number of parallel IBGP paths that can be installed into a route table to enable IBGP multipath load sharing.
*Range:* 0 to 32

Address Family

Enter the BGP IPv6 unicast address family.

RE-DISTRIBUTE

Click the **Redistribute** tab, and then click **Add New Redistribute** .

Protocol

Select the protocols from which to redistribute routes into BGP, for all BGP sessions. Options are Connected, NAT, OMP, OSPF, and Static. At a minimum, select the following:

- For service-side BGP routing, select OMP. By default, OMP routes are not redistributed into BGP.
- For transport-side BGP routing, select Connected, and then under Route Policy, specify a route policy that has BGP advertise the loopback interface address to its neighbors.

Route Policy

Enter the name of the route policy to apply to redistributed routes.

Click **Add** to save the redistribution information.

NETWORK

Click the **Network** tab, and then click **Add New Network** .

Network Prefix

Enter a network prefix, in the format of *prefix* / *length* , to be advertised by BGP.

Click **Add** to save the network prefix.

AGGREGATE ADDRESS

Click the **Aggregate Address** tab, and then click **Add New Aggregate Address** .

Aggregate Prefix

Enter the prefix of the addresses to aggregate for all BGP sessions, in the format prefix/length.

AS Set Path

Click **On** to generate set path information for the aggregated prefixes.

Summary Only

Click **On** to filter out more specific routes from BGP updates.

Click **Add** to save the aggregate address.

5. In the Neighbor area, click the **IPv6** button, create a new neighbor or edit an existing one, and then configure the parameters that the following table describes.

Parameters marked with an asterisk are required.

Parameter Name

Description

IPv6 Address*

Specify the IPv6 address of the BGP neighbor.

Description

Enter a description of the BGP neighbor.

Remote AS*

Enter the AS number of the remote BGP peer.

Address Family

Select **Global** from the drop-down list, click **On** and select the address family. Enter the address family information.

Shutdown

To shut down a BGP neighbor when you push the template, select **Global** from the drop-down list and then click **Yes** .
*Default:* Off

## Configure IPv6 Functionality for a VRRP Template

To configure IPv6 functionality for a Virtual Router Redundancy Protocol (VRRP) template, follow these steps:

1. In Cisco vManage NMS, select the **Configuration** ► **Templates** screen.
2. Select **Feature** ► **Add Template** and then select an appropriate device model.
3. Select **VPN Interface Ethernet** from the list of templates.
4. In the VRRP area, click the **IPv6** button and then click **New VRRP** .

5. Configure the parameters that the following table describes.

Parameter Name

Description

Group ID

Enter a virtual router ID, which represents a group of routers.
*Range:* 1 through 255

Priority

Enter the priority level of the router within a VRRP group.

- *Range:* 1 through 254
- *Default:* 100

Timer

Not used.

Track OMP

Select On to track the Overlay Management Protocol (OMP) session running on the WAN connection when determining the VRRP primary virtual router.
*Default:* Off

Track Prefix List

Enter a value to track a list of IPv6 remote prefixes.
This value is an alphanumeric string that is configured under Policy.

Link Local IPv6 Address

Enter a virtual link local IPv6 address, which represents the link local address of the group.
The address should be in standard link local address format. For example, FE80::AB8.

Global IPv6 Address

Enter a virtual global unicast IPv6 address, which represents the global address of the group.
The address should be an IPv6 global prefix address that has the same mask as the interface forwarding address on which the VRRP group is configured. For example, 2001::2/124.

## Configure IPv6 Functionality for an SNMP Template

To configure IPv6 functionality for an SNMP template, follow these steps:

1. In Cisco vManage NMS, select the **Configuration** ► **Templates** screen.
2. Select **Feature** ► **Add Template** and then select an appropriate device model.
3. Select **SNM** P from the list of templates.
4. In the SNMP Version area, click the **SNMP Version** button ► **TRAP TARGET SERVER** and create or edit an SNMP trap target.

Note: Make sure that you have already configured the SNMP community and trap target group.

5. Configure the parameters that the following table describes.

Parameter Name

Description

VPN ID

Enter the number of the VPN to use to reach the trap server.
*Range:* 0 through 65530

IP Address

Enter the IP address of the SNMP server.

UDP Port

Enter the UDP port number for connecting to the SNMP server.
*Range:* 1 though 65535

Trap Group Name

Select the name of a trap group that was configured under the Group tab.

User Name

Select the name of a community that was configured under the Community tab.

Source Interface

Enter the interface to use to send traps to the SNMP server that is receiving the trap information.

## Configure IPv6 Functionality for a DHCP Relay Agent Template

To configure IPv6 functionality for a DHCP Relay Agent template, follow these steps:

1. In Cisco vManage NMS, select the **Configuration ► Templates** screen.
2. Select **Feature ► Add Template** and then select an appropriate device model.
3. Select **VPN Interface Ethernet** from the list of templates.
4. In the Basic Configuration area, click the **IPv6** button.
5. Click **Add** next to DHCP Helper.
6. Configure the parameters that the following table describes.

Parameter Name

Description

DHCPv6 Helper #

IP address of the DHCP helper

DHCPv6 Helper VPN

VPN ID of the VPN source interface for the DHCP helper.

## Configure IPv6 Functionality for an ACL Template or a QoS Template

To configure IPv6 functionality for an ACL and QoS template, follow these steps:

1. In Cisco vManage NMS, select the Configuration ► **Templates** screen.
2. Select **Feature** ► **Add Template** and then select an appropriate device model.
3. Select **VPN Interface Ethernet** from the list of templates.
4. In the ACL/QoS area, configure the parameters that the following table describes.

Parameter Name

Description

Ingress ACL – IPv6

Click **on** to enable the IPv6 ingress access list.

IPv6 Ingress Access List

Enter the name of the IPv6 ingress access list.

Egress ACL – IPv6

Click **on** to enable the IPv6 egress access list.

IPv6 Egress Access List

Enter the name of the IPv6 egress access list.

## Configure IPv6 Functionality for a Logging Template

To configure IPv6 functionality for a Logging template, follow these steps:

1. In Cisco vManage NMS, select the **Configuration** ► **Templates** screen.
2. Select **Feature** ► **Add Template** and then select an appropriate device model.
3. Select **Logging** from the list of templates.
4. In the Server area, click the **IPv6** button.
5. Configure the parameters that the following table describes.

Parameter Name

Description

IPv6 Hostname/IPv6 Address

Host name or IP address of the server to direct the logging information.

VPN ID

VPN ID of the VPN source interface.

Source Interface

Name of the source interface.

Priority

Choose the maximum severity of messages that are logged.

## Configure IPv6 Functionality for a New Prefix List

To configure an IPv6 address for a new prefix list, follow these steps:

1. In Cisco vManage NMS, select **Configuration** ► **Policies** .
2. From the Custom Options drop-down menu, select **Lists** .
   You can make this selection for a Centralized Policy or a Localized Policy
3. Select **Prefix** from the list on the left and then select **New Prefix** List.
4. Select the **IPv6** radio button and enter the IPv6 address in the Add Prefix field.

## Configure IPv6 Functionality for a Data Prefix

To configure an IPv6 address for a new prefix list, follow these steps:

1. In Cisco vManage NMS, select **Configuration** ► **Policies** .
2. From the Custom Options drop-down menu, select **Lists** .
   You can make this selection for a Centralized Policy or a Localized Policy
3. Select **Data Prefix** from the list on the left and then select **New Data Prefix List** .
4. In the Internet Protocol area, select the **IPv6** radio button and enter the IPv6 address in the Add Prefix field.

## Configure IPv6 Functionality for a Centralized Policy

To configure a centralized policy to apply to IPv6 address families, follow these steps:

1. In Cisco vManage NMS, select **Configuration** ► **Policies** .
2. From the Custom Options drop-down menu, select **Traffic Policy** under Centralized Policy.
3. Select the **Traffic Data** tab.
4. Select Add Policy ► Create New.
5. Click the **Sequence Type** button and then select **Traffic Engineering** .
6. Click the **Sequence Rule** button.
7. From the Protocol drop-down list, select **IPv6** to apply the policy only to IPv6 address families, or select **Both** to apply the policy IPv4 and IPv6 address families.
8. Click the **Sequence Type** button and then select **QoS** .
9. Click the **Sequence Rule** button.
10. From the Protocol drop-down list, select **IPv6** to apply the policy only to IPv6 address families, or select **Both** to apply the policy IPv4 and IPv6 address families.

## Configure IPv6 Functionality for a Localized Policy

To configure a localized policy to apply to IPv6 address families, follow these steps:

1. In Cisco vManage NMS, select Configuration ► Policies.

2. From the Custom Options drop-down menu, select **Access Control Lists** under Localized Policy.

3. Click the **Add Access Control List Policy** button and choose **Add IPv6 ACL Policy** .
   The policy you create will apply only to IPv6 address families.

I

## Network Design

Use the Network Design screen to create and manage an overlay network topology. From this screen, you can add circuits, data centers, and branch sites to a network topology, configure LAN, WAN, and management options for elements in the topology, review the topology, and perform related tasks. The network design operations are particularly useful for smaller-scale deployments that include data centers and branch sites.

Network design consists of these major workflows:

- Create network topology—Create circuits, data centers, and branch sites, in this order. A network topology must include at least one circuit and one data center.
- Configure device profiles—Configure global parameters and options for LAN, WAN, and management settings.

- Attach devices profiles—Attach device profiles to devices.
- Ongoing management—Add elements to the network topology and modify the configuration settings for elements as needed.

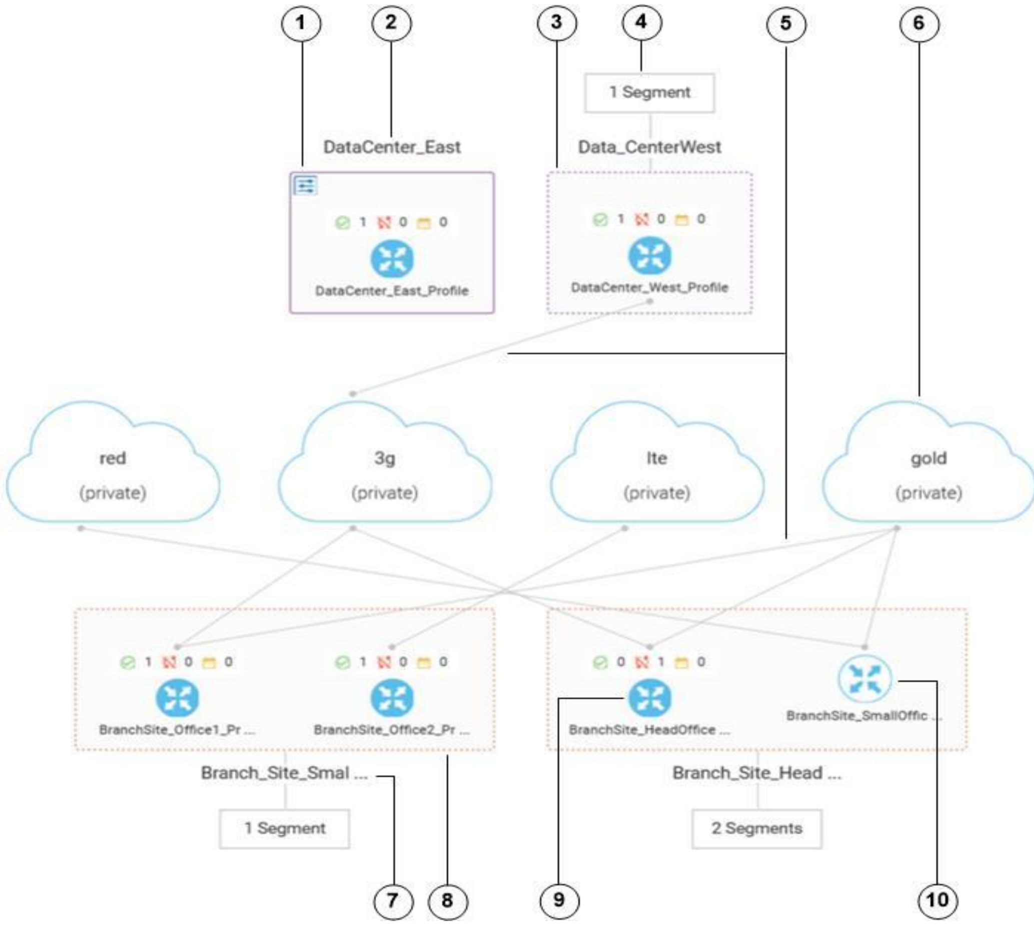
## Access Network Design Options

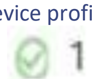
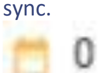
To access options for creating or updating a network design, select **Configuration ▶ Network Design** .

The Network Design screen displays. This screen includes the following items:

- **Create Network Design** button—Displays if you have not yet created a network topology. Click to create elements for the network. For more information, see Configure Network Design Elements .
- **Manage Network Design** button—Displays if you have created a network topology. Click to modify configuration setting for elements in the network. For more information, see Configure Network Design Elements .
- **Attach Devices** button—Click to access options for attaching a device profile to a device, detach a device profile from a device, export device profile configuration values to a CSV file, or modify values in a device profile. For more information, see Attach, Detach, Export, Update Device Profiles .
- Last modified information—Date and time that the network design was last modified.
- Device Attached Task option—Displays if the system is in the process of attaching a device profile to devices or updating device profile configuration information. For more information, see Attach Device Profile or Change Device Profile Values .
- Network design topology diagram—Displays if you have created a network topology. Figure 1 shows an example diagram.

Figure 1. Network Design Topology Display




| | |
|---|---|
| **1** | Custom device profile for a device in a data center.<br>Custom profiles are indicated by a solid border and the  icon at the top left corner.<br>If the partial name of a device profile displays, hover your mouse pointer over the name to see the full name.<br>If a device profile is attached to 1 or more devices, the following icons and information display:<br>•  — Indicates the number of devices that the profile is successfully attached to.<br>•  — Indicates the number of devices that the profile failed to attach to. If there are failed attachments, the device is out of sync.<br>•  — Indicates the number of devices that the profile is in the process of attaching to. |
| **2** | Name of a data center.<br>If the partial name of a data center displays, hover your mouse pointer over the name to see the full name. |
| **3** | Standard device profile for a device in a data center.<br>Standard profiles are indicated by a dashed border.<br>If the partial name of a device profile displays, hover your mouse pointer over the name to see the full name.<br>If a device profile is attached to 1 or more devices, icons and information display as described in Row 1 of this table. |
| **4** | Number of segments that are assigned to a data center or branch site.<br>Hover your mouse pointer over the segment display to see the name of each segment. |

| | |
|---|---|
| **5** | TLOC connections between elements in the topology.<br>A custom device profile does not display TLOC connections to other elements because its settings, such as LAN, WAN, and circuit configurations, have been converted to feature templates. |
| **6** | Circuit. |
| **7** | Name of a branch site.<br>If the partial name of a branch site displays, hover your mouse pointer over the name to see the full name. |
| **8** | Standard device profiles for a device in a branch site.<br>Standard profiles are indicated by a dashed border.<br>If the partial name of a device profile displays, hover your mouse pointer over the name to see the full name.<br>If a device profile is attached to 1 or more devices, icons and information display as described in Row 1 of this table. |
| **9** | A blue shaded icon with white arrows indicates that the device profile has been attached to 1 or more devices. Shaded circle with white arrows |
| **10** | An unshaded icon with blue arrows indicates that the device profile has not been attached to any devices. |

## Configure Network Design Elements

With the network design feature, you can create a new overlay network topology and modify existing elements in a topology. You perform these activities from the Network Design screen.

Creating a new network topology involves performing the following procedures in the order shown:

Procedure

Description

Reference

1

Add circuits.

See Configure Circuits .

2

Add data centers.

See Configure Data Centers .

3

Add branch sites.

See Configure Branch Sites .

4

Configure global parameters.

See Configure Global Parameters .

5

Configure device profiles.

See Configure Device Profiles .

6

Attach device profiles.

See Attach Device Profile .

A network topology must include at least one circuit and one data center. After a network topology is created, you can modify its elements directly.

## Configure Circuits

Each network topology must have at least 1 circuit and can have up to 18 circuits.

To configure circuits for a network topology, follow these steps:

1. Select **Configuration ▶ Network Design** and then click **Create Network Design** (which displays if you have not yet created a network topology) or **Manage Network Design** (which displays if you have created a network topology).

2. Click **Circuits** near the top of the Network Design screen.

A screen for configuring circuits displays. If any circuits have been created, this screen lists them. You can remove a circuit by clicking its corresponding delete icon  .

3. Click **Add New Circuit** .

4. Select the **Private** or the **Public** radio button to indicate whether the circuit is private or public.

5. From the Circuit Color drop-down list, choose a predefined color to uniquely identify the transport location (TLOC) in a circuit.

The color can be default, 3g, biz-internet, blue, bronze, custom1, custom2, custom3, gold, green, lte, metro-ethernet, mpls, private1, private2, public-internet, red, or silver. The color you choose cannot be used for a TLOC in any other circuit in the topology.

6. Repeat Steps 2 through 5 as needed to add more circuits.

To remove a circuit that you added, click its corresponding **Delete** icon  .

6. Click **Finish** .

7. Click **Save** on the Network Design screen.

Or, if you do not want to save the updates that you made, click **Cancel** .

## Configure Data Centers

Configuring a data center involves assigning a name and adding device profiles and segments to the data center. Each network topology must have at least one data center.

To configure data centers for a network topology, follow these steps:

1. Select **Configuration ▶ Network Design** and then click **Create Network Design** (which displays if you have not yet created a network topology) or **Manage Network Design** (which displays if you have created a network topology).

2. Click **Data Center** near the top of the Network Design screen.

This option appears dimmed if you have not added at least one circuit as described in Configure Circuits .

A screen for configuring data centers displays. If any data centers have been created, this screen lists them. If you are creating a network topology for the first time, skip to Step 4 .

3. If any data centers are listed on the screen that displays, you can take any of these actions:

- To add another data center, click **Add Data Center** and then continue to Step 4 .
- To view information about device profiles that have been added to a data center, click the **Devices** button to the right of the data center name.
- To view information about segments that have been added to a data center, click the **Segments** button to the right of the data center name.
- To update configuration items for a data center, including its name, device profiles, and segments, click the pencil icon to the right of the data center name and then continue to Step 4 .
- To remove a data center from the network topology, click the trash can icon to the right of the data center name and then skip to Step 8 .
  You cannot delete a data center that includes any device profiles that are attached to one or more devices. To delete a data center in this situation, first detach the device profiles from devices. For instructions, see Detach Device Profile .

4. In the Data Center Name field, enter a unique name for the data center.

This name cannot be used for any other data center, branch site, or device profile in the topology. The name can include letters, numbers, underscores, and hyphens, but no spaces or special characters.

5. Take the following actions to add device profiles to the data center or to update device profile configuration settings:

Each data center must have at least one device profile. A device profile is associated with a specific device type in the data center and provides configuration settings that are pushed to those device types.

a. If you are adding a new device profile, click **Add a Device Profile** .

b. In the Name field, enter a name for the device profile. This name cannot be used for any other device profile, data center, or branch site in the topology. The name can include letters, numbers, underscores, and hyphens, but no spaces or special characters.

c. From the Device Model drop-down list, choose the device type with which to associate the device profile.

d. Click the Circuits field to display a list of circuits that you created as described in Configure Circuits and then check the box next to each circuit that the device profile should be associated with. The circuit names that you check appear in the Circuits field. You can remove a circuit from this field by unchecking its check box or by clicking the X next to its name. You can use the same circuit in multiple data centers and branch sites.

e. Repeat Steps 5a through 5d as needed to add more device profiles.

f. Click **Next** .

6. Take the following actions to add one or more segments.

Each data center must have at least one segment. A segment is a service side VPN that is associated with all device profiles in the data center. You can use the same segment in multiple data centers and branch sites.

a. Click **Add Segment** and choose one of these options:

- New Segment—Creates a new segment with a new name and VPN ID
- Existing Segment—Lets you choose a segment that you already created

b. In the Segment Name field, take one of these actions:

- If you chose New Segment, enter a name for the segment. The name can include letters, numbers, underscores, and hyphens, but no spaces or special characters.

- If you chose Existing Segment, choose a segment from the drop-down list. The VPN Number field populates automatically with the VPN ID that was configured for the segment.

c. If you chose New Segment, in the VPN Number field, enter a LAN side VPN ID to associate with the segment. This value cannot be used for any other VPN number in the topology. Valid values are 1 through 65535, except 512.

d. Repeat Steps 6a through 6c as needed to add more segments. To remove a segment that you added, click its corresponding Delete icon  .

e. Click **Add** .

The system displays a list of data centers.

7. Repeat Steps 2 through 6 as needed to add more data centers.

8. Click **Finish** .

9. Click **Save** on the Network Design screen.

Or, if you do not want to save the updates that you made, click **Cancel** .

## Configure Branch Sites

Configuring a branch site involves assigning a name and adding device profiles and segments to the branch site. A network topology does not require branch sites.

To configure branch sites for a network topology, follow these steps:

1. Select **Configuration ▶ Network Design** and then click **Create Network Design** (which displays if you have not yet created a network topology) or **Manage Network Design** (which displays if you have created a network topology).

2. Click **Branch Sites** near the top of the Network Design screen.

This option appears dimmed if you have not added at least one circuit when you added a data center as described in Configure Data Center .

A screen for configuring branch sites displays. If any circuits have been created, this screen lists them. If you are creating a network design for the first time, skip to Step 4 .

3. If any branch sites are listed on the screen that displays, you can take any of these actions:

- To add another branch site, click **Add Branch** and then continue to Step 4 .

- To view information about device profiles that have been added to a branch site, click the **Devices** button to the right of the branch site name.

- To view information about segments that have been added to a branch site, click the **Segments** button to the right of the branch site name.

- To update configuration items for a branch site, including its name, device profiles, circuits, and segments, click the pencil item to the right of the branch site name and then continue to Step 4 .

- To remove a branch site from the network topology, click the trash can icon to the right of the branch site name and then skip to Step 8 . You cannot delete a branch site that includes any device profiles that are attached to one or more devices. To delete a branch site in this situation, first detach device profiles from devices. For instructions, see Detach Device Profile .

4. In the Branch Name field, enter a name for the branch site.

This name cannot be used for any other branch site, data center, or device profile in the topology. The name can include letters, numbers, underscores, and hyphens, but no spaces or special characters.

5. Take the following actions to add or update device profiles.

Each branch site must have at least one device profile. A device profile is associated with a specific device type in the branch site and provides configuration settings that are pushed to those device types.

a. If you are adding a new device profile, click **Add a Device Profile** .

b. In the Name field, enter a name for the device profile. This name cannot be used for any other device profile, data center, or branch site in the topology. The name can include letters, numbers, underscores, and hyphens, but no spaces or special characters.

c. From the Device Model drop-down list, choose the device type with which to associate the device profile.

d. Click the Circuits field to display a list of circuits that you created as described in Configure Circuits and then check the box next to each circuit that the device profile should be associated with. The circuit names that you check appear in the Circuits field. You can remove a circuit from this field by unchecking its check box or by clicking the X next to its name. You can use the same circuit in multiple data centers and branch sites.

e. Repeat Steps 5a through 5d as needed to add more device profiles.

f. Click **Next** .

6. Take the following actions to add one or more segments.

Each branch site must have at least one segment. A segment is a service side VPN that is associated with all device profiles in the branch site. You can use the same segment in multiple branch sites and data centers.

a. Click **Add Segment** and choose one of these options:

- New Segment—Creates a new segment with a new name and VPN ID
- Existing Segment—Lets you choose a segment that you already created

b. In the Segment Name field, take one of these actions:

- If you chose New Segment, enter a name for the segment. The name can include letters, numbers, underscores, and hyphens, but no spaces or special characters.
- If you chose Existing Segment, choose a segment from the drop-down list. The VPN Number field populates automatically with the VPN ID that was configured for the segment.

c. If you chose New Segment, in the VPN Number field, enter a LAN side VPN ID to associate with the segment. This value cannot be used for any other VPN number in the topology. Valid values are 1 through 65535, except 512.

d. Repeat Steps 6a through 6c as needed to add more segments. To remove a segment that you added, click its corresponding Delete icon  .

e. Click **Add** .

The system displays a list of branch sites.

7. Repeat Steps 2 through 6 as needed to add more branch sites.

8. Click **Finish** .

9. Click **Save** on the Network Design screen.

Or, if you do not want to save the updates that you made, click **Cancel** .

## Configure Global Parameters

Global parameters are configuration settings that are used in all device profiles in a network topology. If you do not configure global parameters, factory default configuration settings are used for device profiles.

To configure global parameters, follow these steps:

1. Select **Configuration ► Network Design** and then click **Create Network Design** (which displays if you have not yet created a network topology) or **Manage Network Design** (which displays if you have created a network topology).

2. Click **Global Parameters** near the top of the Network Design screen and choose the desired template from the drop-down list that displays.

A screen for configuring the selected template displays.

3. Configure the template as described in the “Create a Device Template” section in Templates .

The template name and description are filled in automatically and cannot be changed. There is no option for selecting a device type because the template is used for all devices throughout your network.

4. Click **Update** .

5. Click **Save** on the Network Design screen.

Or, if you do not want to save the updates that you made, click **Cancel** .

## Configure Device Profiles

You must configure a device profile for each router in a data center or branch site before the device profile can be attached to the router. Configuring a profile involves configuring its TLOC, LAN side, and management interfaces, and configuring related settings.

There are two types of device profiles:

- Standard device profile—Contains basic LAN, WAN, and management interface configuration options
- Custom device profile—Contains more advanced configuration options for a variety of items such as routing and other services for the interfaces

Each new device profile that you create is saved as a standard type. After you create a standard device profile and attach it to a device, you can convert it to a custom device profile as described in the following instructions.

To configure a device profile for a router in a network topology, follow these steps:

1. Select **Configuration ► Network Design** and then click **Create Network Design** (which displays if you have not yet created a network topology) or **Manage Network Design** (which displays if you have created a network topology).

2. In the network diagram that displays on the Network Design screen, click the image that represents the device for which you want to build or modify a device profile.

The image of the device displays in one of these ways:

- Blue shaded icon—Indicates that the device has a profile. When you hover your mouse pointer over this image, “Manage profile” displays.

  If you choose this option for a standard device profile, the Manage Profile screen displays. From this screen, you can modify configuration settings for the device profile or convert it to a custom device profile. Continue to Step 3 .

  If you choose this option for a custom device profile, a template screen displays. Skip to Step 4 .

- Unshaded icon—Indicates that the device does not yet have a profile. When you hover your mouse pointer over this image, “Build profile” displays.

  If you choose this option, the Build Profile screen displays. From this screen, you can create a standard device profile. Skip to Step 5 .

3. If you chose to manage a device profile for a standard device profile, take one of these actions:

- To update existing options for the standard device profile, click the pencil icon that appears near the top right of the screen for managing a profile. The Build Profile screen displays. Skip to Step 5 .

- To convert the standard device profile to a custom device profile, click **Custom Profile** and then click **Proceed** in the dialog box that pops up. A template screen displays with some options pre-populated based on options that you have already configured for this device profile. Configure the options as desired. (For information about configuring a template, see the “Create a Device Template” section in Templates .) When you are finished, click **Update** and then skip to Step 17 .

4. If you chose to manage a custom device profile, configure the options as desired. (For information about configuring a template, see the “Create a Device Template” section in Templates .) When you are finished, click **Done** and then skip to Step 17 .

5. If you chose to build a device profile or to manage a standard device profile, In the Interface Name field, enter the name of a TLOC interface to associate with the circuit that is associated with this router.

6. Click one of these radio buttons:

- **DHCP** —Selects a dynamic IP address for the interface

- **Static** — Indicates that you will assign a static IP address to the interface and a prefix and next hop to the VPN later, as described in Attach Device Profile

7. (Optional) In the DNS server field, enter the IP address of the primary DNS server in the network.

8. Click **Next** .

9. In the Interface Name field, enter the name of a LAN side interface to associate with the segment.

10. (Optional) In the VLAN field, enter a sub-interface, if needed for your deployment.

11. Click one of these radio buttons:

- **None** —Indicates that you will assign a static IP address to this interface later, as described in Attach Device Profile

- **DHCP** —Indicates that you will assign a DHCP address pool to this interface late, as described in Attach Device Profile

- **DHCP** Relay—Indicates that you will assign a DHCP helper address to this interface later, as described in Attach Device Profile

12. Click **Next** .

13. In the Interface Name field, enter the name for the management interface to associate with the device.

14. Click one of these radio buttons:

- **DHCP** —Selects a dynamic IP address for the interface

- **Static** —Indicates that you will assign a static IP address to the interface and a prefix and next hop to the VPN later, as described in Attach Device Profile

15. (Optional) In the DNS server field, enter the IP address of the primary DNS server in the network.

16. Click **Done** .

17. Click **Save** on the Network Design screen.

Or, if you do not want to save the updates that you made, click **Cancel** .

## Attach, Detach, Export, Update Device Profiles

From the Network Design screen, you can perform the following tasks for existing device profiles.

Task

Description

Reference

Attach a device profile to devices.

Makes the devices available to be controlled and configured through the SD-WAN.

See Attach Device Profile .

Detach a device profile from devices.

Puts the devices into CLI mode.

See Detach Device Profile .

Export device profile settings

Creates a CSV file that contains configuration information of a selected device profile. This tasks is useful for backing up of device profile configuration information.

See Export Device Profile Settings .

Change configuration information for a device profile.

Updates device profile configuration information on the devices to which the profile is attached.

See Change Device Profile Values .

For information about creating a device profile, see Configure Device Profiles .

### Attach Device Profile

Attaching a device profile to devices makes the devices available to be controlled and configured through the SD-WAN. A device to which a device profile is not attached is in CLI mode.

A device can have only one device profile. The same device profile can be attached to multiple devices.

To attach a device profile to devices, follow these steps:

1. Select **Configuration ► Network Design** and then click **Attach Device** .

2. In the network diagram that displays, click the device profile that you want to attach to devices and then choose **Attach Devices** from the pop-up list.

The Attach Devices window displays.

Configure options on this window as described in the “Attach Devices to a Device Template” section in Templates .

If, when you configured a device profile, if you configured static for a TLOC interface, or DHCP or DCHP relay for a VLAN subinterface, make sure to configure the static IP address, DHCP IP address, prefix information, and next hop information, as applicable.

After you configure devices, the Network Design screen displays and the configuration updates are pushed to the selected devices.

You can click the **Device Attached Task** option near the top right of the screen to view the progress of the configuration push operation.

## Detach Device Profile

Detaching a device profile puts the devices to which it was attached into CLI mode.

To detach a device, follow these steps:

1. Select **Configuration ► Network Design** and then click **Detach Device** .
2. In the network diagram that displays, click the device profile that you want to detach from devices and then choose **Detach Devices** from the pop-up list.

The Detach Device window displays.

3. In the Available Devices column on the left, either select a group and search for one or more devices, select a device from the list, or click **Select All** .
4. Click the arrow pointing right to move the device to the Selected Devices column on the right.
5. Click **Detach** .

The device profile is detached from the devices that you selected.

## Export Device Profile Settings

Exporting device profile settings creates a CSV file that contains the configuration information of a selected device profile. You can save this CSV file in the location of your choice. This export feature is useful for creating a backup of device profile configuration information.

A device profile must be attached to at least one device before you can export its configuration information.

To export a CSV file, follow these steps:

1. Select **Configuration ► Network Design** and then click **Export** .
2. In the network diagram that displays, click the device profile whose configuration information you want to export and then choose **Export CSV** from the pop-up list.
3. Follow the on-screen prompts to create the CSV file and save it to the location of your choice.

## Change Device Profile Values

Changing device profile values updates device profile configuration information on the devices to which the profile is attached.

A device profile must be attached to at least one device before you can update its configuration information.

To change device values, follow these steps:

1. Select **Configuration ► Network Design** and then click **Profile** .
2. In the network diagram that displays, click the device profile whose configuration values you want to update and then choose **Change Device Values** from the pop-up list.
3. In the window that displays, use the Search field and options to locate a device to which the profile is attached.
4. Click the **More Actions** icon to the right of the row for the applicable device and select **Edit Device Template** .
5. In the Update Device Template window that pops-up, modify values as desired, and then click **Update** .
6. Click **Next** .
7. Select a device from the list of devices that displays at the left of the window.
8. Click **Configure Devices** to push the configuration to all devices that the device profile is attached to.

The Network Design screen displays and the configuration updates are pushed to the selected devices. You can click the **Device Attached Task** option near the top right of the screen to view the progress of the configuration push operation.

## Add Network Circuits

You configure centralized policy with a configuration wizard. The wizard is a UI policy builder that consists of four screens to configure and modify the following centralized policy components:

- Groups of interest, also called lists
- Topologies and VPN membership
- Traffic rules
- Applying policies to sites and VPNs

You configure some or all these components depending on the specific policy you are creating. To skip a component, click the Next button at the bottom of the screen. To return to a component, click the Back button at the bottom of the screen.

You apply centralized policies by activating them, as described later in the article, to push the policies to all reachable vSmart controllers.

## Add Data Centers

You configure centralized policy with a configuration wizard. The wizard is a UI policy builder that consists of four screens to configure and modify the following centralized policy components:

- Groups of interest, also called lists
- Topologies and VPN membership
- Traffic rules
- Applying policies to sites and VPNs

You configure some or all these components depending on the specific policy you are creating. To skip a component, click the Next button at the bottom of the screen. To return to a component, click the Back button at the bottom of the screen.

You apply centralized policies by activating them, as described later in the article, to push the policies to all reachable vSmart controllers.

## Add Branch Sites

You configure centralized policy with a configuration wizard. The wizard is a UI policy builder that consists of four screens to configure and modify the following centralized policy components:

- Groups of interest, also called lists
- Topologies and VPN membership

- Traffic rules
- Applying policies to sites and VPNs

You configure some or all these components depending on the specific policy you are creating. To skip a component, click the Next button at the bottom of the screen. To return to a component, click the Back button at the bottom of the screen.

You apply centralized policies by activating them, as described later in the article, to push the policies to all reachable vSmart controllers.

## Configure Global Parameters

You configure centralized policy with a configuration wizard. The wizard is a UI policy builder that consists of four screens to configure and modify the following centralized policy components:

- Groups of interest, also called lists
- Topologies and VPN membership
- Traffic rules
- Applying policies to sites and VPNs

You configure some or all these components depending on the specific policy you are creating. To skip a component, click the Next button at the bottom of the screen. To return to a component, click the Back button at the bottom of the screen.

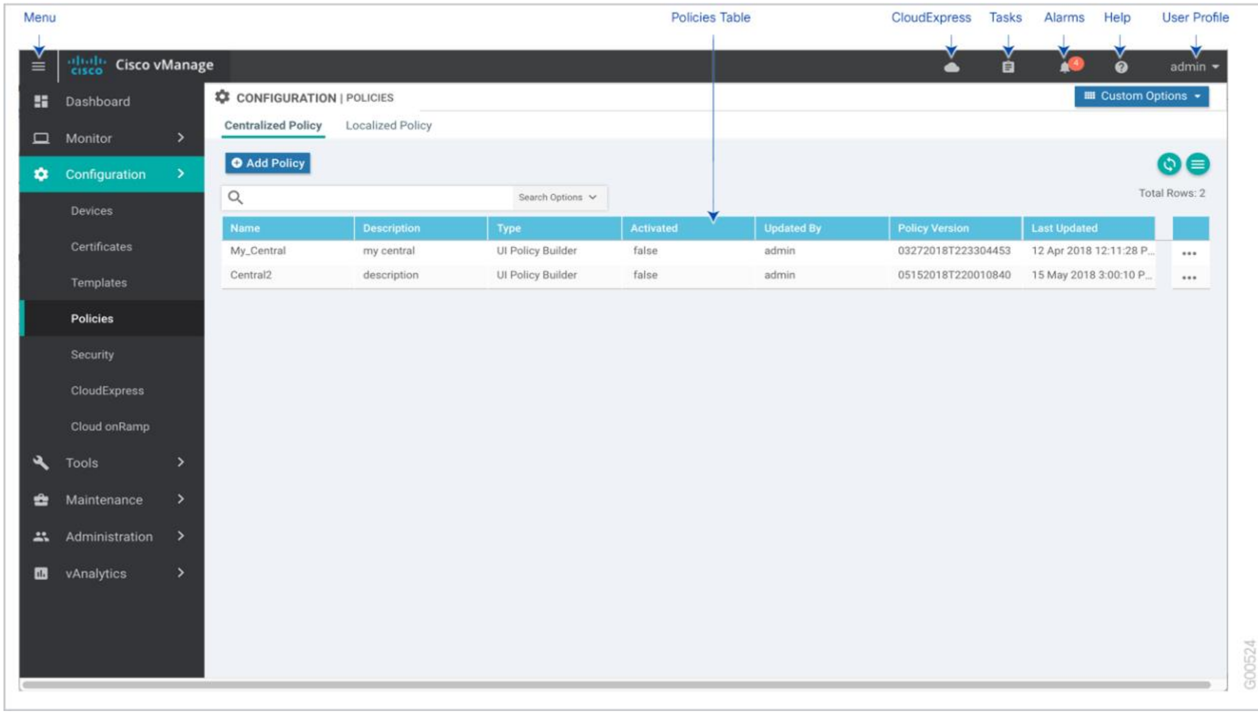
You apply centralized policies by activating them, as described later in the article, to push the policies to all reachable vSmart controllers.

## Policies

Use the Policies screen to create and activate centralized and localized control and data policies for vSmart controllers and vEdge routers.

## Screen Elements

- Top bar—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.
- Title bar—Includes the title of the screen, Policies, and the following:
  - Custom Options—Click to display, create, and edit a components for use in policy. For centralized policy, the components are CLI policies, lists, topologies, and traffic policies. For localized policy, the components are CLI policies, lists, forwarding class/QoS definitions, access control lists (ACLs), and route policies.
- Centralized Policy tab—Create a centralized policy. When you first open the Policies screen, the Centralized Policy tab is selected.
  - Add Policy—Click to create a centralized policy using a policy configuration wizard.
- Localized Policy tab—Create a localized policy.
  - Add Policy—Click to create a localized policy using a policy configuration wizard.
- Search box—Includes the Search Options drop-down, for a Contains or Match string.
- Refresh icon—Click to refresh data in the policies table with the most current data.
- Show Table Columns icon—Click to display or hide columns from the policies table. By default, all columns are displayed.
- Policies table—To re-arrange the columns, drag the column title to the desired position.




# Configure Policies

- [Configure Centralized Policy]
- [Configure Localized Policy]

# View a Policy

1. In the Centralized Policy or Localized Policy tab, select a policy.
2. Click the More Actions icon to the right of the column and click View. Policies created with the UI policy builder are displayed in graphical format. Policies created using the CLI are displayed in text format.
3. Click Cancel to return to the policies table.

For a policy created using the vManage policy configuration wizard, you can view the policy in text format:

1. In the Centralized Policy or Localized Policy tab, select a policy.
2. Click the More Actions icon to the right of the column and click Preview.
3. Click Cancel to return to the policies table.

# Copy a Policy

1. In the Centralized Policy or Localized Policy tab, select a policy.
2. Click the More Actions icon to the right of the column and click Copy.
3. In the Policy Copy popup window, enter the policy name and a description of the policy.

4. Click Copy.

## Edit a Policy

For policies created using the vManage policy configuration wizard:

1. In the Centralized Policy or Localized Policy tab, select a policy.
2. Click the More Actions icon to the right of the column and click Edit.
3. Edit the policy as needed.
4. Click Save Policy Changes.

For polices created using the CLI:

1. In the Custom Options drop-down, click CLI Policy.
2. Click the More Actions icon to the right of the column and click Edit.
3. Edit the policy as needed.
4. Click Update.

## Edit or Create a Policy Component

You can create individual policy components directly and then use them or import them when you are using the policy configuration wizard:

1. In the Title bar, click the Custom Options drop-down.
2. For centralized policy, select the policy component:

- CLI policy—Create the policy using the command-line interface rather than the policy configuration wizard.
- Lists—Create groups of interest to import in the Group of Interest screen in the policy configuration wizard.
- Topology—Create a hub-and-spoke, mesh, or custom topology or a VPN membership to import in the Topology screen in the policy configuration wizard.
- Traffic Policy—Create an application-aware routing, traffic data, or cflowd policy to import in the Traffic Rules screen in the policy configuration wizard.

3. For localized policy, select the policy component:

- CLI policy—Create the policy using the command-line interface rather than the policy configuration wizard.
- Lists—Create groups of interest to import in the Group of Interest screen in the policy configuration wizard.
- Forwarding Class/QoS—Create QoS mappings and rewrite rules to import in the Forwarding Classes/QoS screen in the policy configuration wizard.
- Access Control Lists—Create ACLs of interest to import in the Configure Access Lists screen in the policy configuration wizard.
- Route Policy—Create route policies to import in the Configure Route Policies screen in the policy configuration wizard.

## Delete a Policy

1. In the Centralized Policy or Localized Policy tab, select a policy.
2. Click the More Actions icon to the right of the column and click Delete.
3. Click OK to confirm deletion of the policy.

## Activate a Centralized Policy on vSmart Controllers

1. In the Centralized Policy tab, select a policy.
2. Click the More Actions icon to the right of the column and click Activate.
3. In the Activate Policy popup, click Activate to push the policy to all reachable vSmart controllers in the network.
4. Click OK to confirm activation of the policy on all vSmart controllers.

## Deactivate a Centralized Policy on vSmart Controllers

1. In the Centralized Policy tab, select a policy.
2. Click the More Actions icon to the right of the column and click Deactivate.
3. In the Deactivate Policy popup, click Deactivate to confirm that you want to remove the policy from all reachable vSmart controllers.

## Additional Information

Application-Aware Routing
Centralized Control Policy
Centralized Data Policy
Configure Policies
Localized Control Policy
Localized Data Policy

## Configure Centralized Policy

You configure centralized policy with a configuration wizard. The wizard is a UI policy builder that consists of four screens to configure and modify the following centralized policy components:

- Groups of interest, also called lists
- Topologies and VPN membership
- Traffic rules
- Applying policies to sites and VPNs

You configure some or all these components depending on the specific policy you are creating. To skip a component, click the Next button at the bottom of the screen. To return to a component, click the Back button at the bottom of the screen.

You apply centralized policies by activating them, as described later in the article, to push the policies to all reachable vSmart controllers.

For more information about the centralized policy components, see Configuring Centralized Control Policy . For information about application-aware routing policy components, see Configuring Application-Aware Routing .

## Step 1: Start the Policy Configuration Wizard

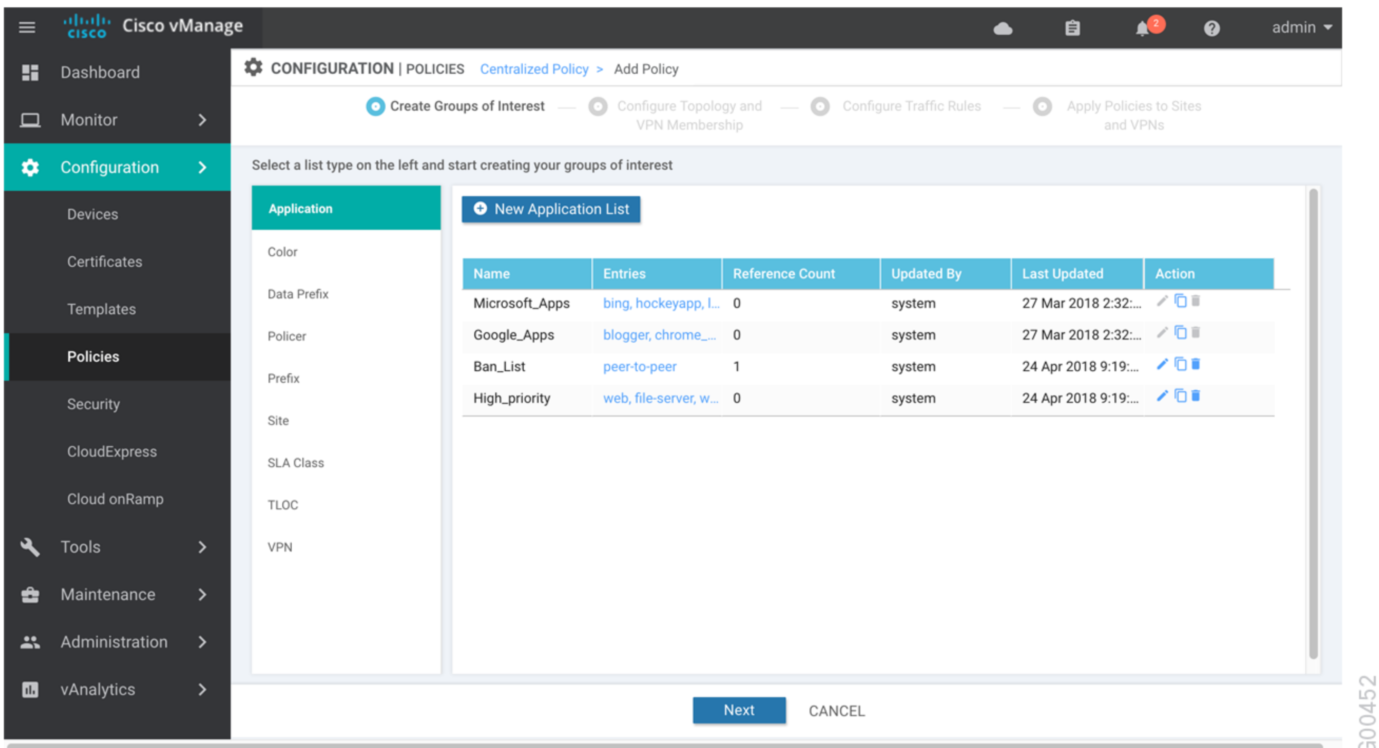
To start the policy configuration wizard:

1. In vManage NMS, select the Configure ► Policies screen.
2. Select the Centralized Policy tab.
3. Click Add Policy.

The policy configuration wizard opens, and the Create Groups of Interest screen displays.

## Step 2: Configure Groups of Interest

In Create Groups of Interest, create lists of groups to use in centralized policy:

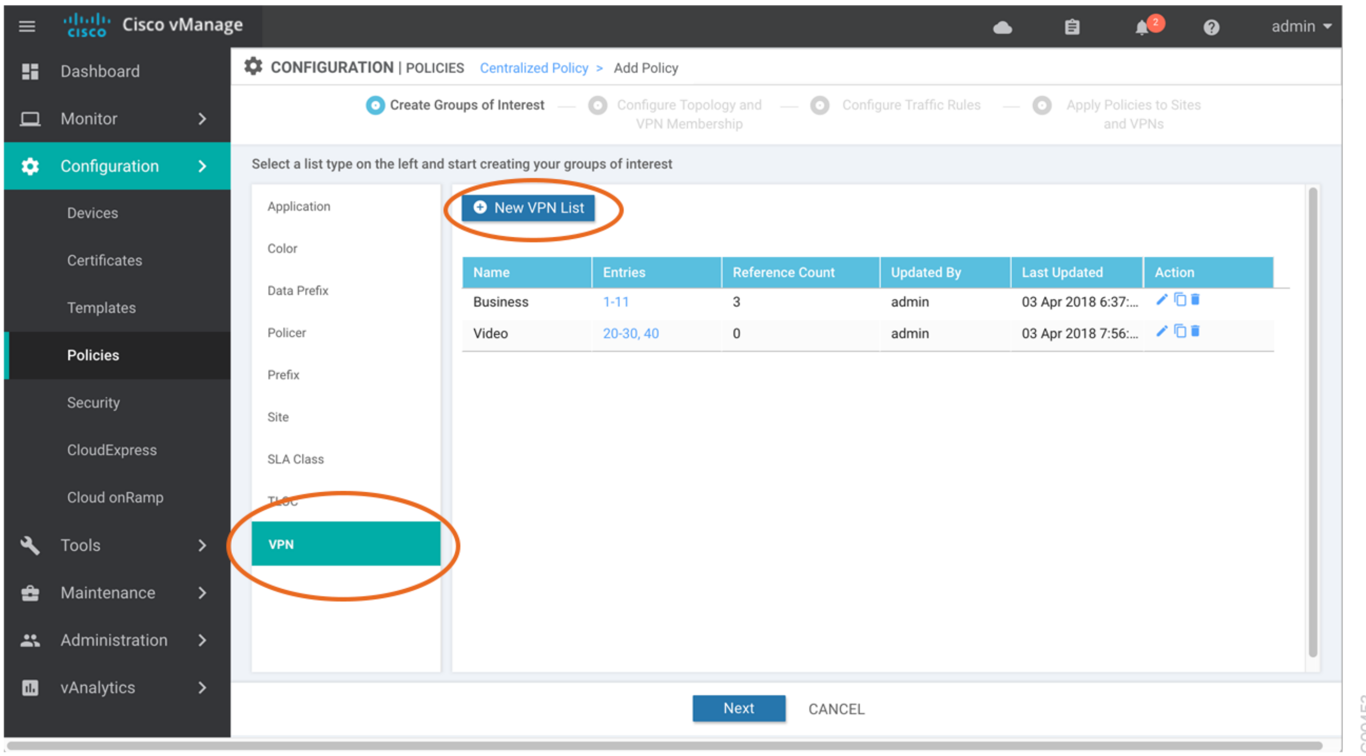



1. In the left pane, select the type of list to use with the localized policy. It can be one of the following:

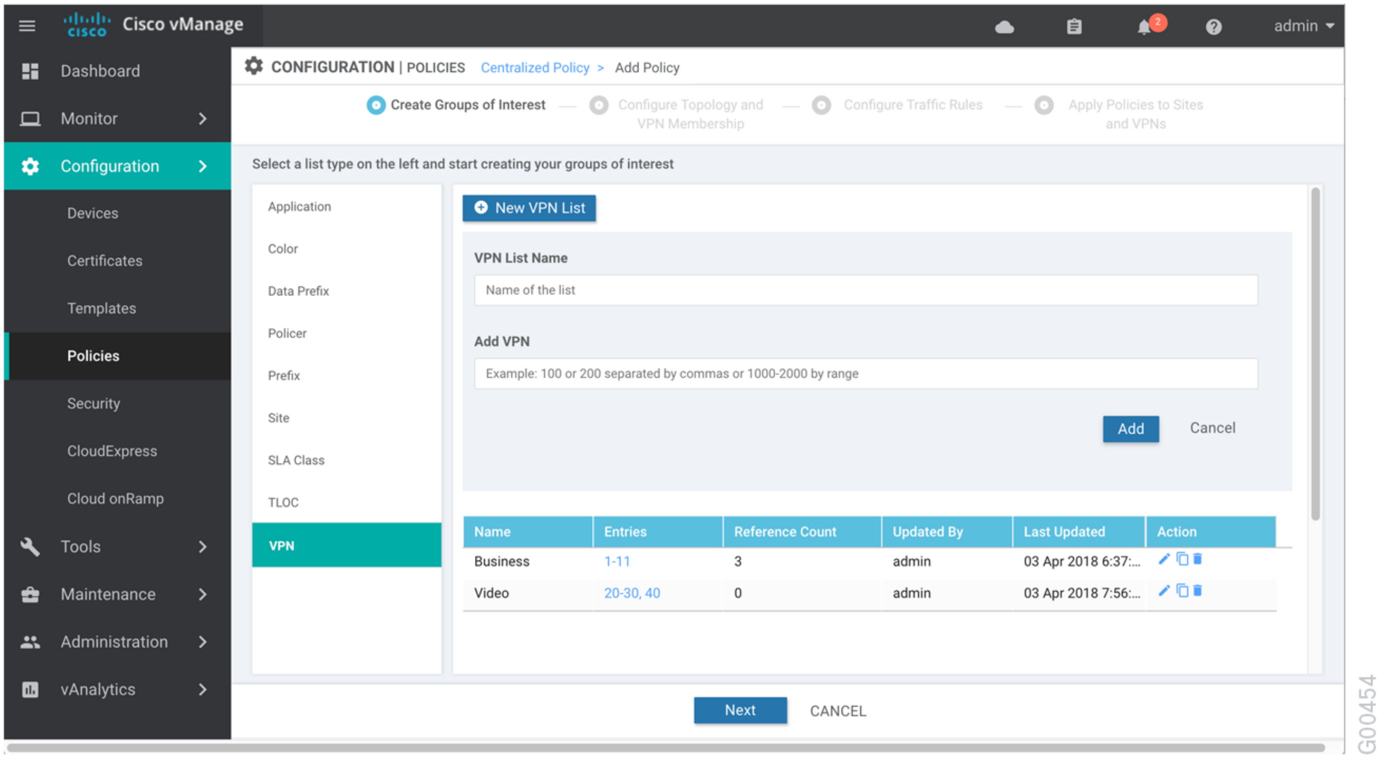
- Application
- Color
- Data Prefix
- Policer
- Prefix
- Site

- SLA Class
- TLOC
- VPN

2. In the right pane, click the New button. The New List portion of the screen opens. For example:




3. Enter a name for the list, and enter or select the components to include in the list.
   For application lists, note that the Google_Apps and Microsoft_Apps lists are preconfigured, and you cannot edit or delete them.
   For example:




4. Click Add to create the new list.

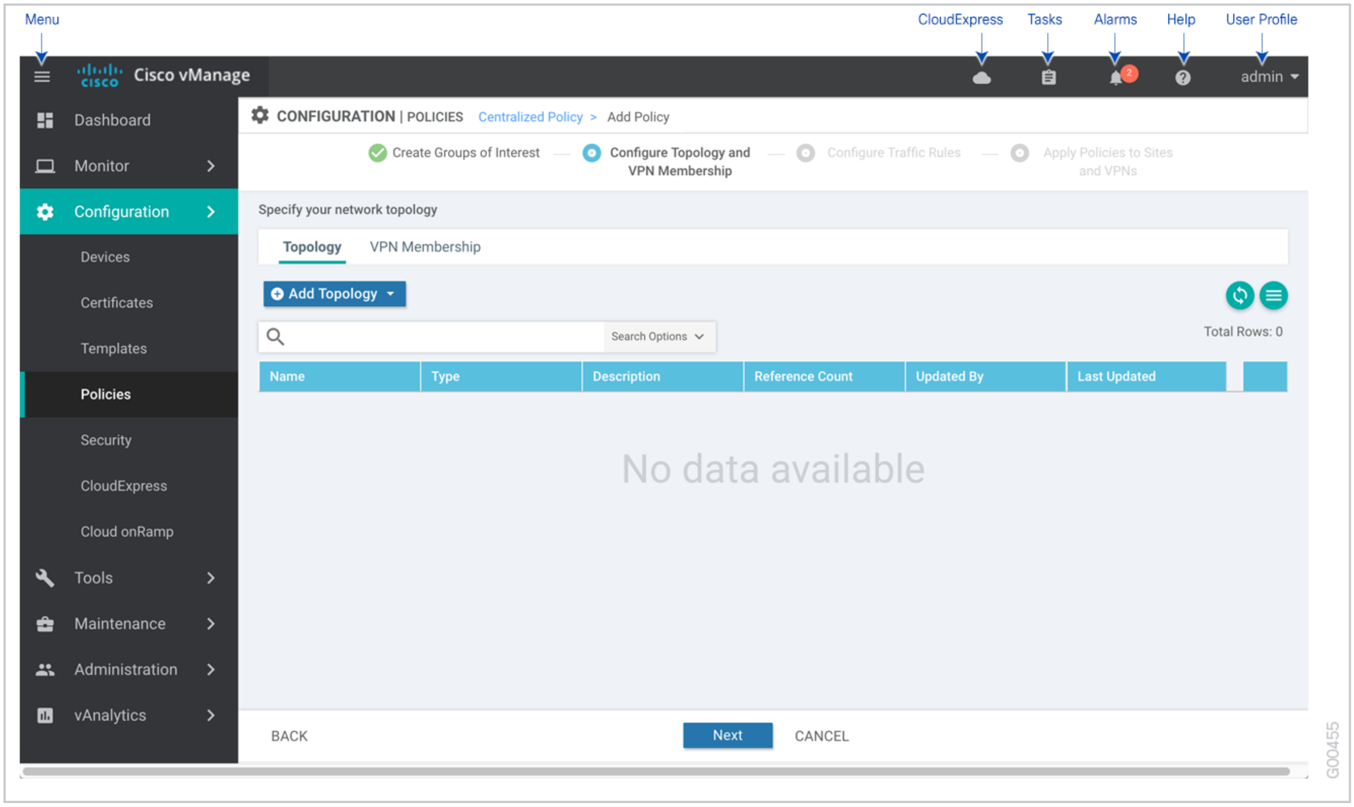
5. Repeat Steps 1 through 4 to create additional lists.

6. To edit, copy, or delete an existing list, click the Edit, Copy, or Trash Bin icon in the Action column.

7. Click Next to move to Configure Topology and VPN Membership in the wizard.

## Step 3: Configure Topology and VPN Membership

When you first open the Configure Topology and VPN Membership screen, the Topology tab is selected by default:

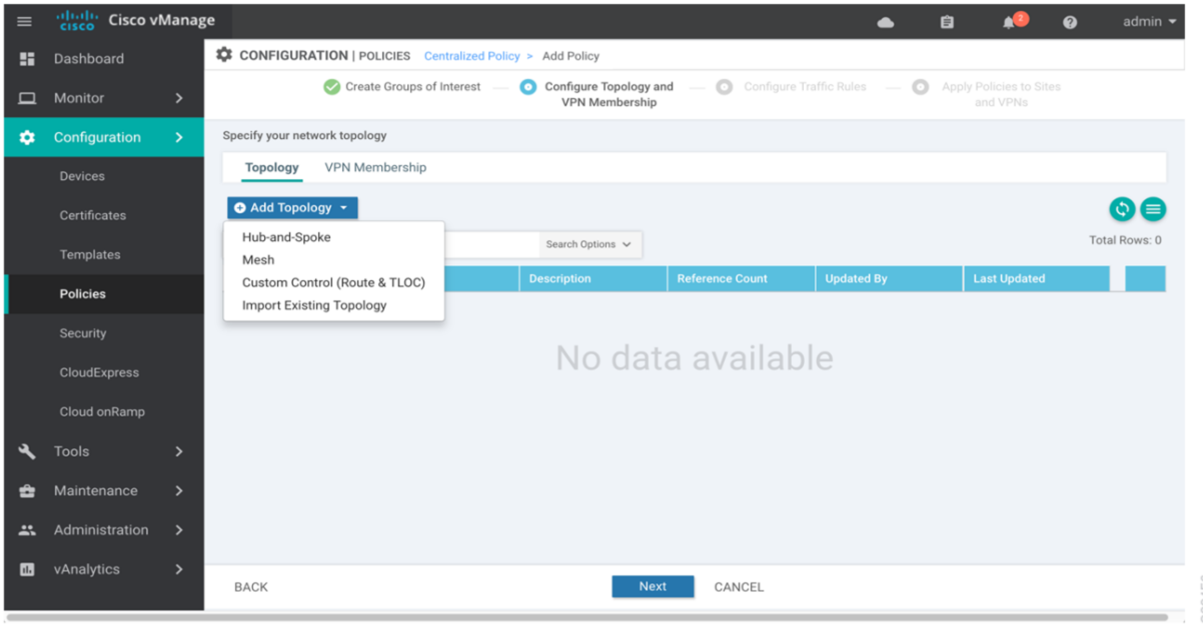



To configure topology and VPN membership:

1. To configure a topology policy component:

   a. In the Topology tab, click the Add Topology drop-down.

   b. Select the desired network topology:




c. Enter a name and description for the topology, and select the VPN list to which the topology applies.

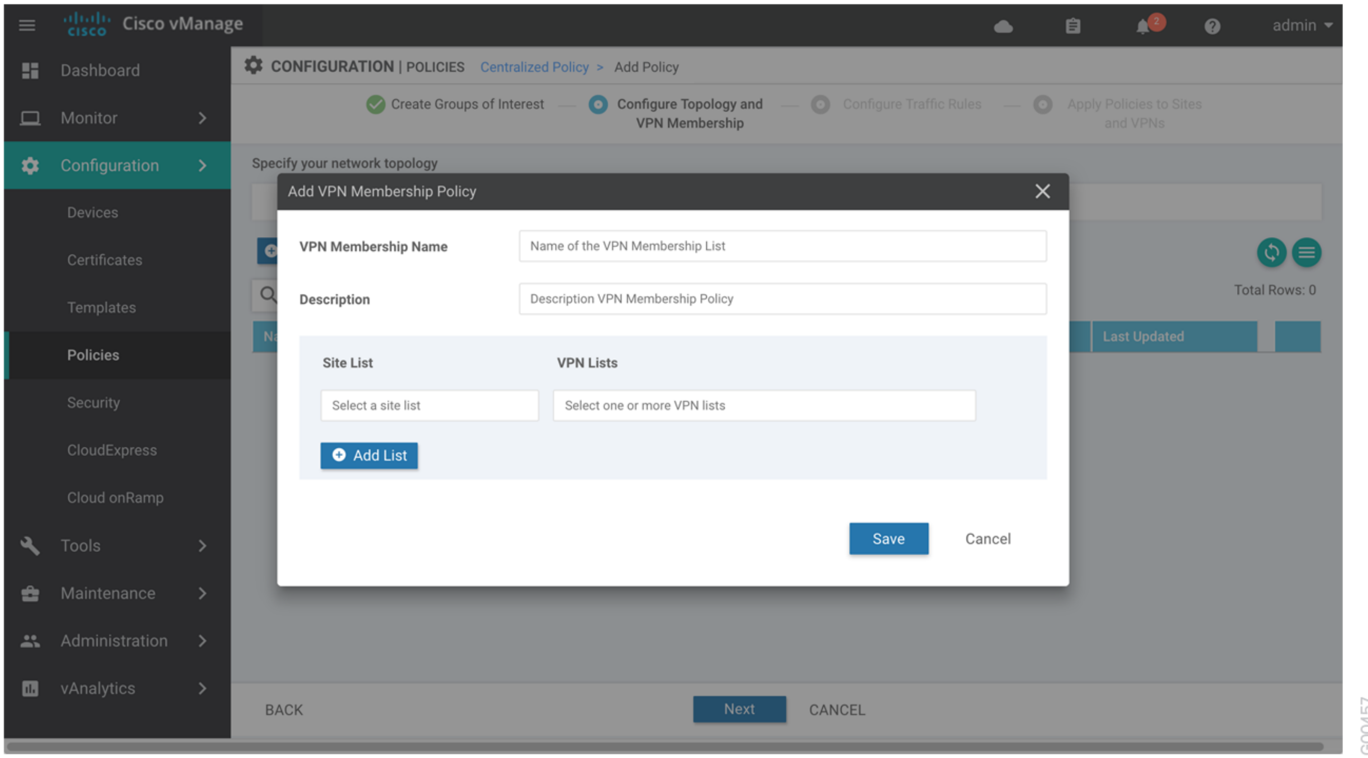
d. Click the New button, and enter the information for the topology component.

e. Enter a name for the topology component, and enter or select the components to include in it.

f. Click Save.

2. To configure a VPN membership policy component:

1. In the VPN Membership tab, click Add VPN Membership Policy:




a. In the Update VPN Membership Policy popup, enter a name and description of the VPN membership, and select site lists and VPN lists. To create new lists, click Add List.

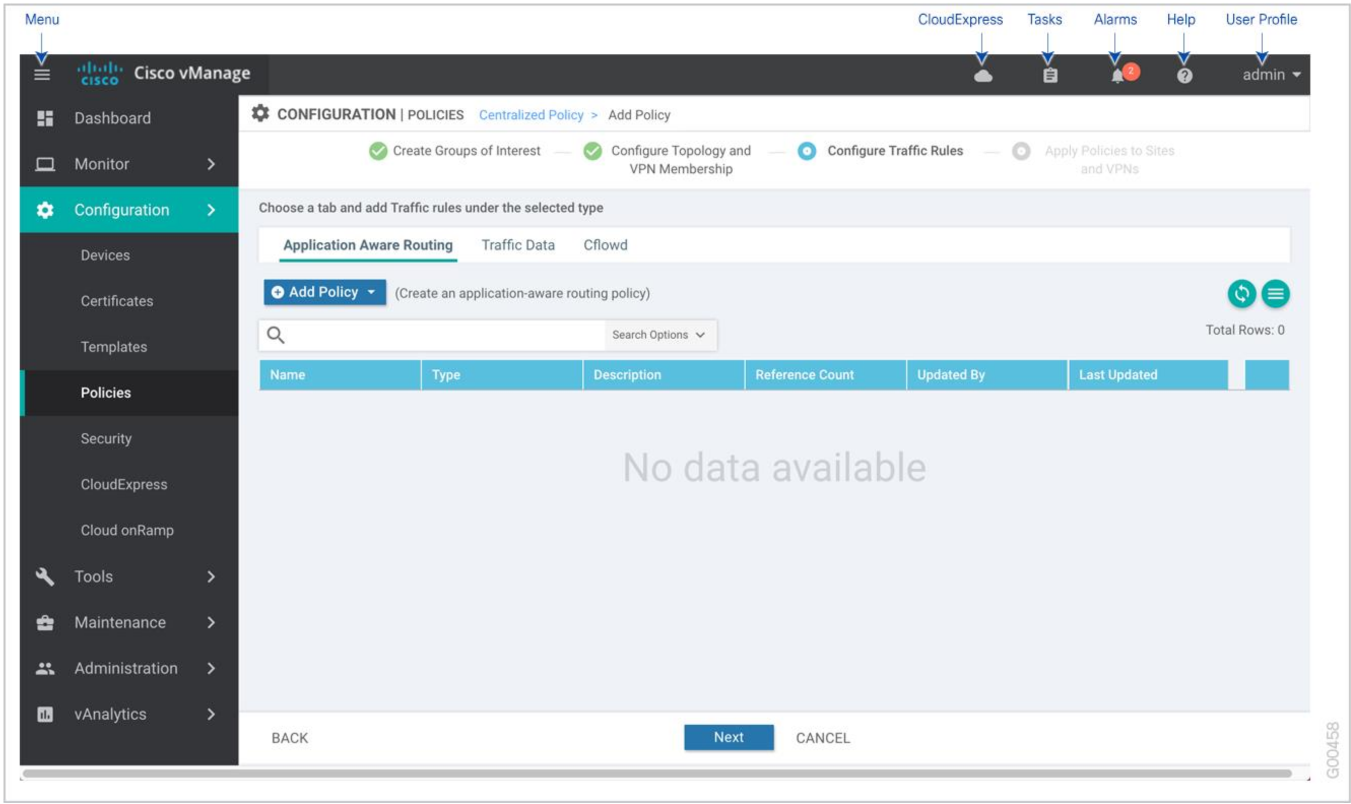
b. Click Save.

2. To edit, copy, or delete an existing topology or VPN membership policy, select it and click the Edit, Copy, or Trash Bin icon in the Action column.

3. Click Next to move to Configure Traffic Rules in the wizard.

## Step 4: Configure Traffic Rules

When you first open the Traffic Rules screen, the Application-Aware Routing tab is selected by default:




To configure traffic rules:

1. In the Application-Aware Routing tab, select the desired policy type—Application-Aware Routing, Traffic Data, or Cflowd.

2. Click the Add Policy drop-down.

3. To import an existing policy, select Import Existing. In the Import Existing Data Policy popup, select the name of the file containing the data policy. Then click Import.

4. To create a new policy, select Create New, and in the left pane, click Sequence Type.

5. For an application-aware routing policy:

    a. In the right pane, click Sequence Rule.

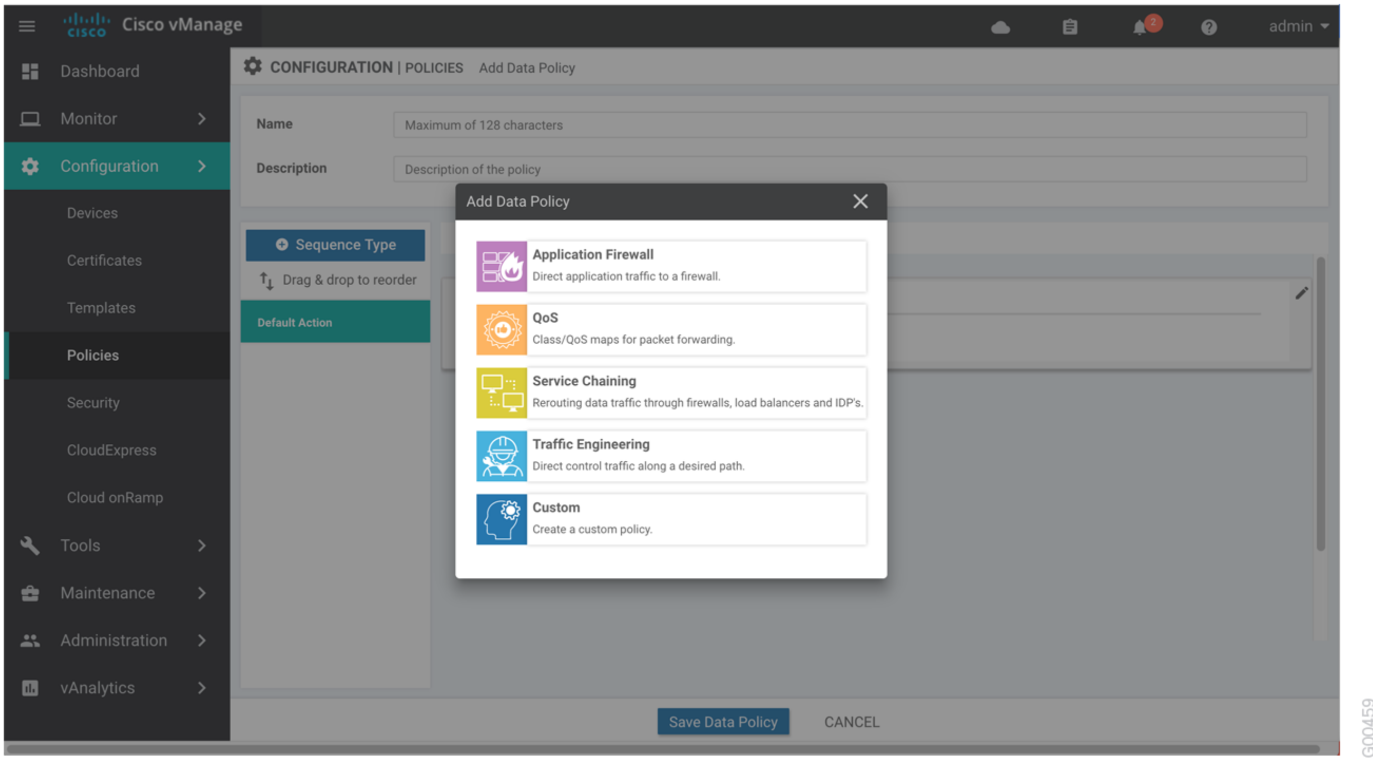
    b. Add the match and action rules. You can select the modifiers OR, AND, or EXACT to focus the scope of a rule. OR applies to multiple community lists and is valid for all platforms; AND and EXACT apply to only one community list at a time and are not valid for vEdge devices.

    c. Add additional sequences as needed. Drag and drop sequences to re-order them

    d. Click Save Application-Aware Routing Policy.

6. For a traffic data policy:

    a. From the Add Data Policy popup, select the policy type:




b. In the right pane, click Sequence Rule.

c. Add the match and action rules.

d. Add additional sequences as needed. Drag and drop sequences to re-order them

e. Click Save Data Policy.

7. For cflowd policy:

a. To configure the cflowd template, enter values for the active flow timeout, inactive flow timeout, flow refresh interval, and sampling interval.

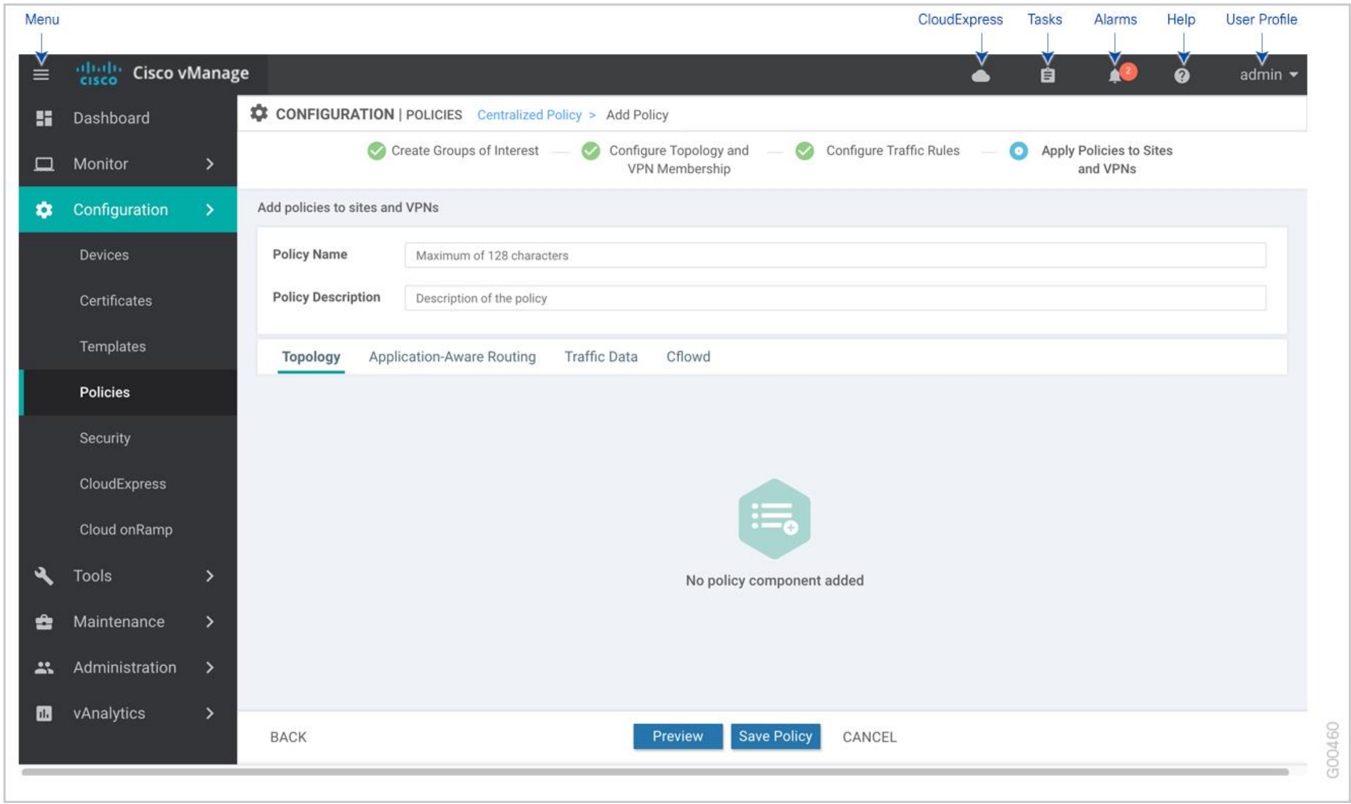
b. To configure a collector list, click Add New Collector. Enter the VPN ID where the collector is located, its IP address, port number, transport protocol, and source interface. Click Add.

c. Click Save Cflowd Policy.

8. Click Next to move to Apply Policies to Sites and VPNs in the wizard.

## Step 5: Apply Policy to Sites and VPNs

In Apply Policies to Sites and VPNs, apply a policy to overlay network sites and VPNs:




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

2. Enter a description of the policy. This field is mandatory, and it can contain any characters and spaces. It can contain up to 2048 characters.

3. From the Topology bar, select the tab that corresponds to the type of policy block—Topology, Application-Aware Routing, Traffic Data, or Cflowd. The table then lists policies that you have created for that type of policy block.

4. Associate the policy with VPNs and sites. The choice of VPNs and sites depends on the type of policy block:

    a. For a Topology policy block, click Add New Site List and VPN List or Add New Site. Some topology blocks might have no Add buttons. Select one or more site lists, and select one or more VPN lists. Click Add.

    b. For an Application-Aware Routing policy block, click Add New Site List and VPN list. Select one or more site lists, and select one or more VPN lists. Click Add.

    c. For a Traffic Data policy block, click Add New Site List and VPN List. Select the direction for applying the policy (From Tunnel, From Service, or All), select one or more site lists, and select one or more VPN lists. Click Add.

    d. For a cflowd policy block, click Add New Site List. Select one or more site lists, Click Add.

5. Click Preview to view the configured policy. The policy is displayed in CLI format.

6. Click Save Policy. The Configuration ► Policies screen opens, and the policies table includes the newly created policy.

## Configure Localized Policy

You configure localized policy with a configuration wizard. The wizard is a UI policy builder that consists of five screens to configure and modify the following localized policy components:

- Groups of interest, also called lists

- Forwarding classes to use for QoS
- Access control lists (ACLs)
- Route policies
- Policy settings

You configure some or all these components depending on the specific policy you are creating. To skip a component, click the Next button at the bottom of the screen. To return to a component, click the Back button at the bottom of the screen.

You apply localized policies to specific vEdge router interfaces. You associate a localized policy with an interface in the VPN Interface Bridge, VPN Interface Ethernet, VPN Interface GRE, VPN Interface PPP, or VPN Interface PPP Ethernet feature configuration template.

For more information about the localized policy components, see Configuring Localized Data Policy for IPv4 and Configuring Localized Data Policy for IPv6 .

## Step 1: Start the Policy Configuration Wizard

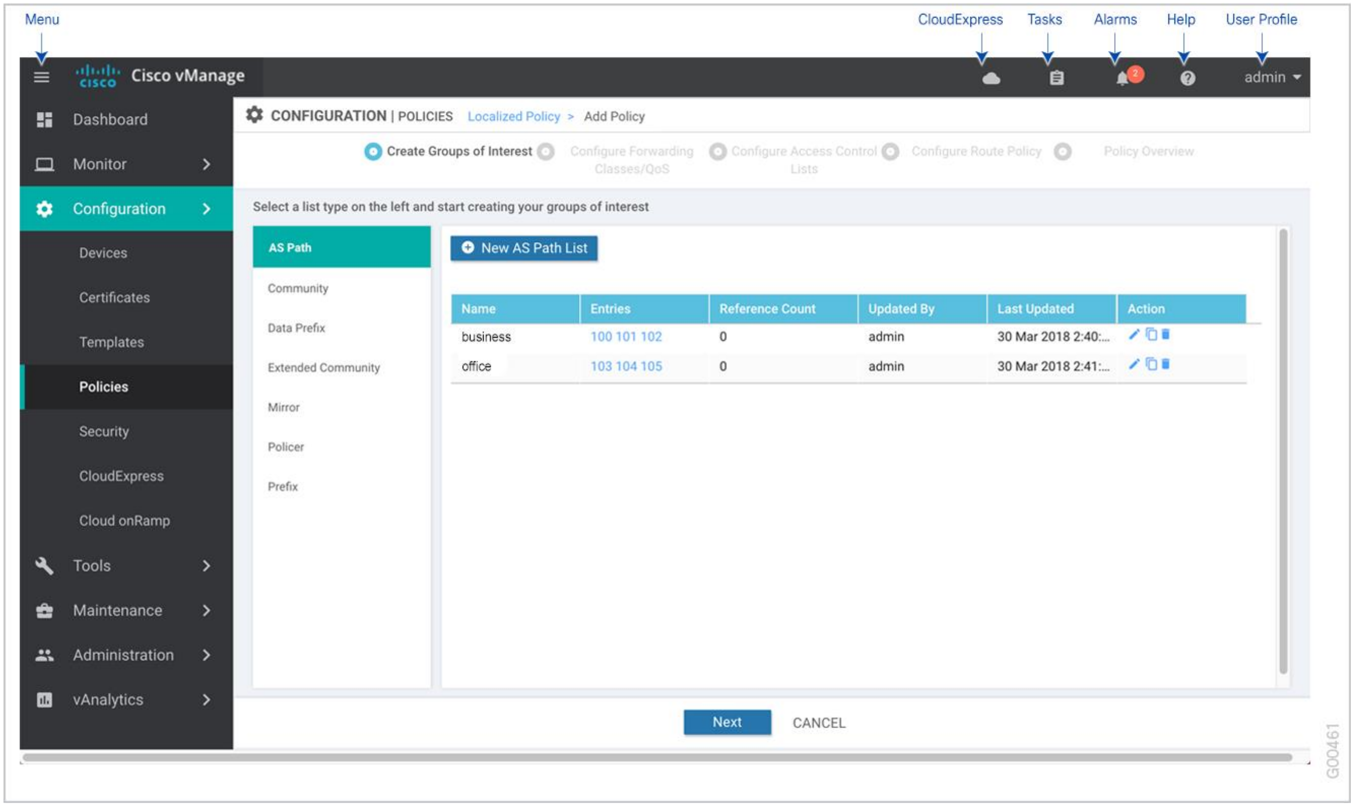
To start the policy configuration wizard:

1. In vManage NMS, select the Configure ► Policies screen.
2. Select the Localized Policy tab.
3. Click Add Policy.

The policy configuration wizard opens, and the Create Groups of Interest screen displays.

## Step 2: Configure Groups of Interest

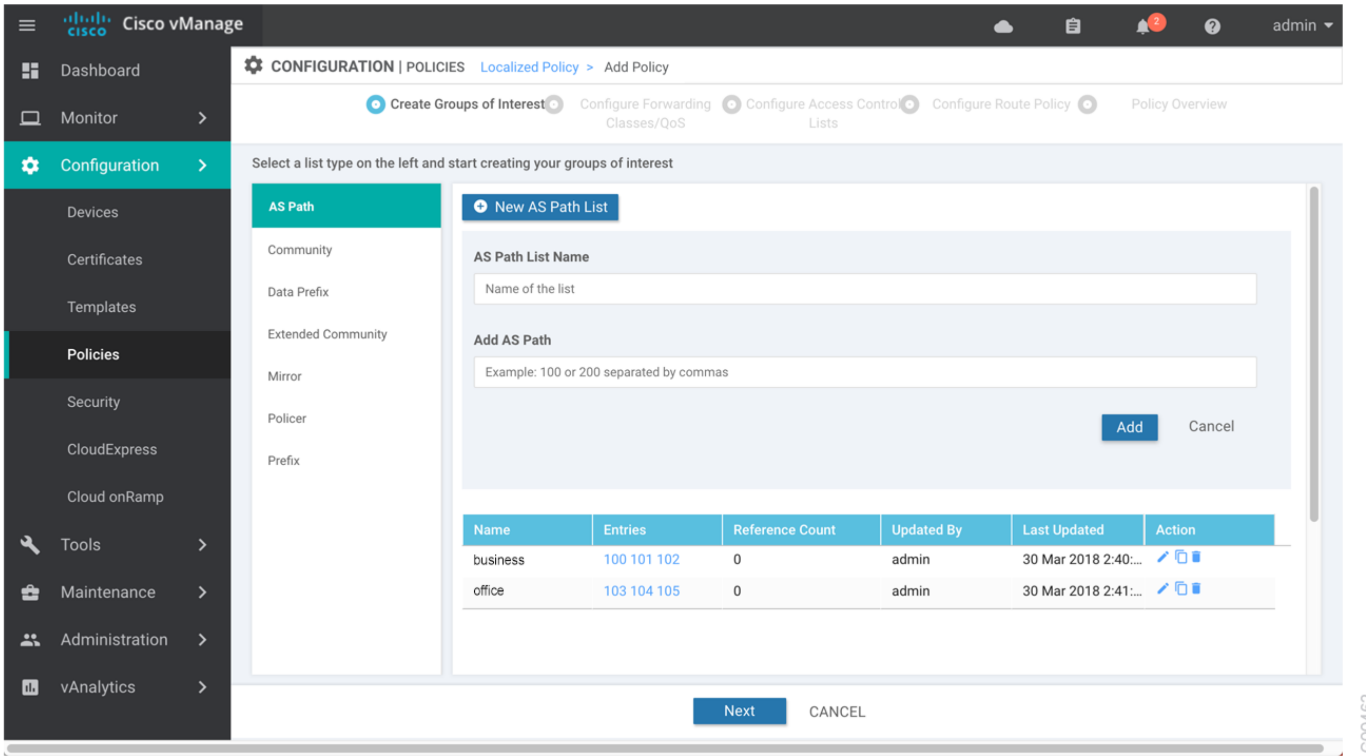
In the Create Groups of Interest screen, create lists to use in localized policy:




1. In the left pane, select the type of list to use with the localized policy. It can be one of the following:

- AS Path
- Community
- Data Prefix
- Extended Community
- Mirror
- Policer
- Prefix

2. In the right pane, click the New button. The New List portion of the screen opens. For example:




3. Enter a name for the list, and enter or select the components to include in the list. For information entering AS path, community and extended community, and data prefix and prefix values, see [Configuring Localized Control Policy](). For information about entering mirroring and policer parameters, see [Configuring Localized Data Policy for IPv4]().

4. Click Add to create the new list.

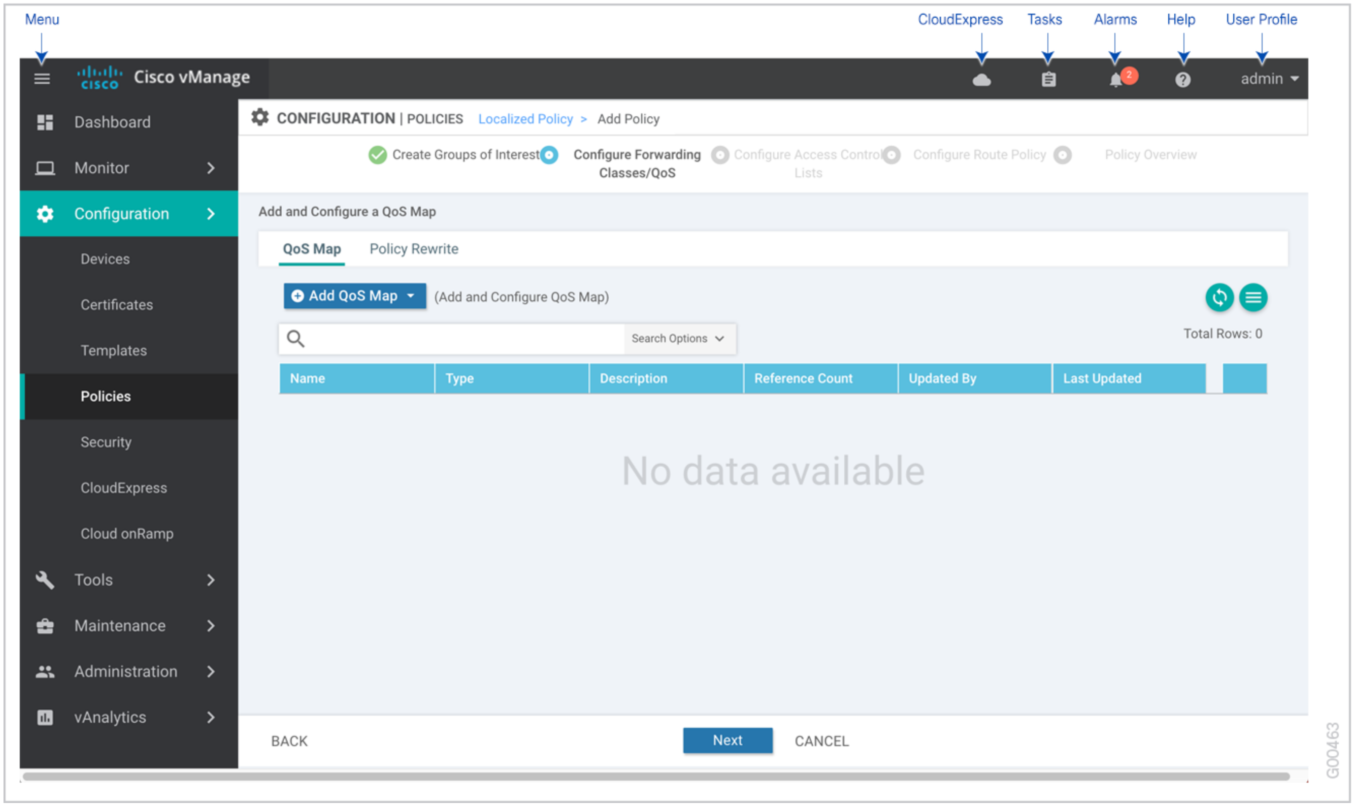
5. Repeat Steps 1 through 4 to create additional lists.

6. To edit, copy, or delete an existing list, click the Edit, Copy, or Trash Bin icon in the Action column.

7. Click Next to move to Configure Forwarding Classes/QoS in the wizard. When you first open this screen, the QoS tab is selected by default.

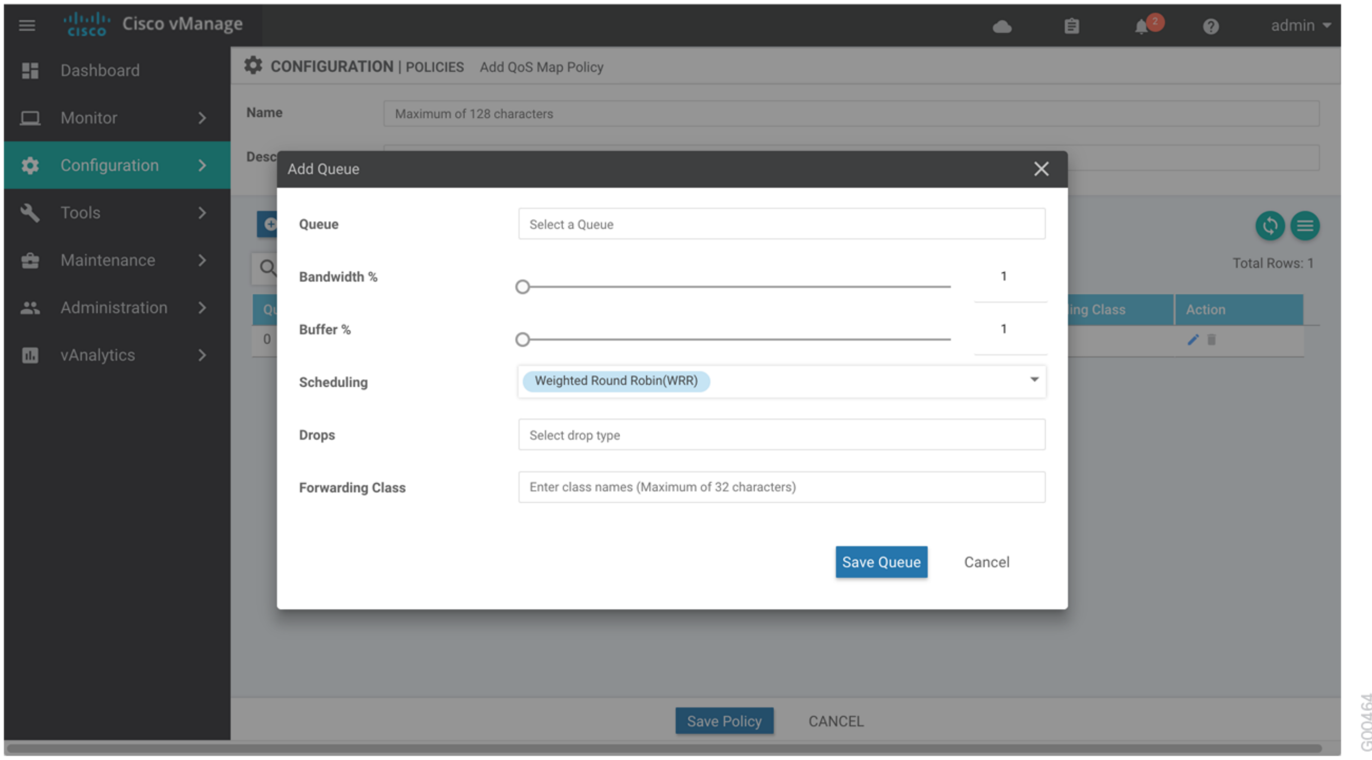
## Step 3: Configure Forwarding Classes for QoS

When you first open the Forwarding Classes/QoS screen, the QoS tab is selected by default:




To configure forwarding classes for use by QoS:

1. To create a new QoS mapping:
   a. In the QoS tab, click the Add QoS drop-down.
   b. Select Create New.
   c. Enter a name and description for the QoS mapping.
   d. Click Add Queue. The Add Queue popup displays:




e. Select the queue number from the Queue drop-down.

f. Select the maximum bandwidth and buffer percentages, and the scheduling and drop types. Enter the forwarding class.

g. Click Save.

2. To import an existing QoS mapping:

   a. In the QoS tab, click the Add QoS drop-down.

   b. Select Import Existing.

   c. Select a QoS mapping.

   d. Click Import.

3. To view or copy a QoS mapping or to remove the mapping from the localized policy, click the More Actions icon to the right of the row, and select the desired action.

4. To configure policy rewrite rules for the QoS mapping:

   a. In the QoS tab, click the Add Rewrite Policy drop-down..

   b. Select Create New.

   c. Enter a name and description for the rewrite rule.

   d. Click Add Rewrite Rule. The Add Rule popup displays.

   e. Select a class from the Class drop-down.

   f. Select the priority (Low or High) from the Priority drop-down.

g. Enter the DSCP value (0 through 63) in the DSCP field.

h. Enter the class of service (CoS) value (0 through 7) in the Layer 2 Class of Service field to include an 802.1p marking in the packet.

i. Click Save.

5. To import an existing rewrite rule:

   a. In the QoS tab, click the Add Rewrite Policy drop-down..

   b. Select Import Existing.

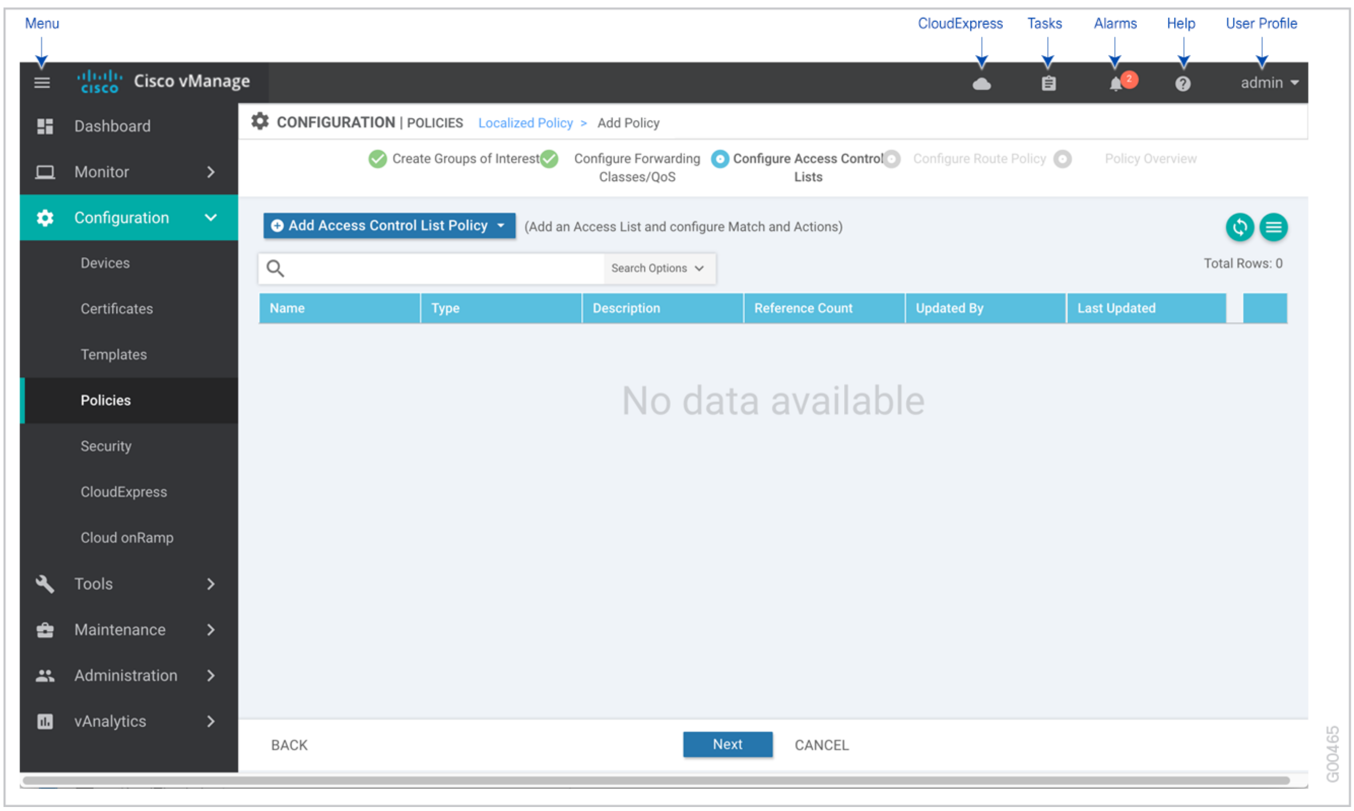
   c. Select a rewrite rule.

   d. Click Import.

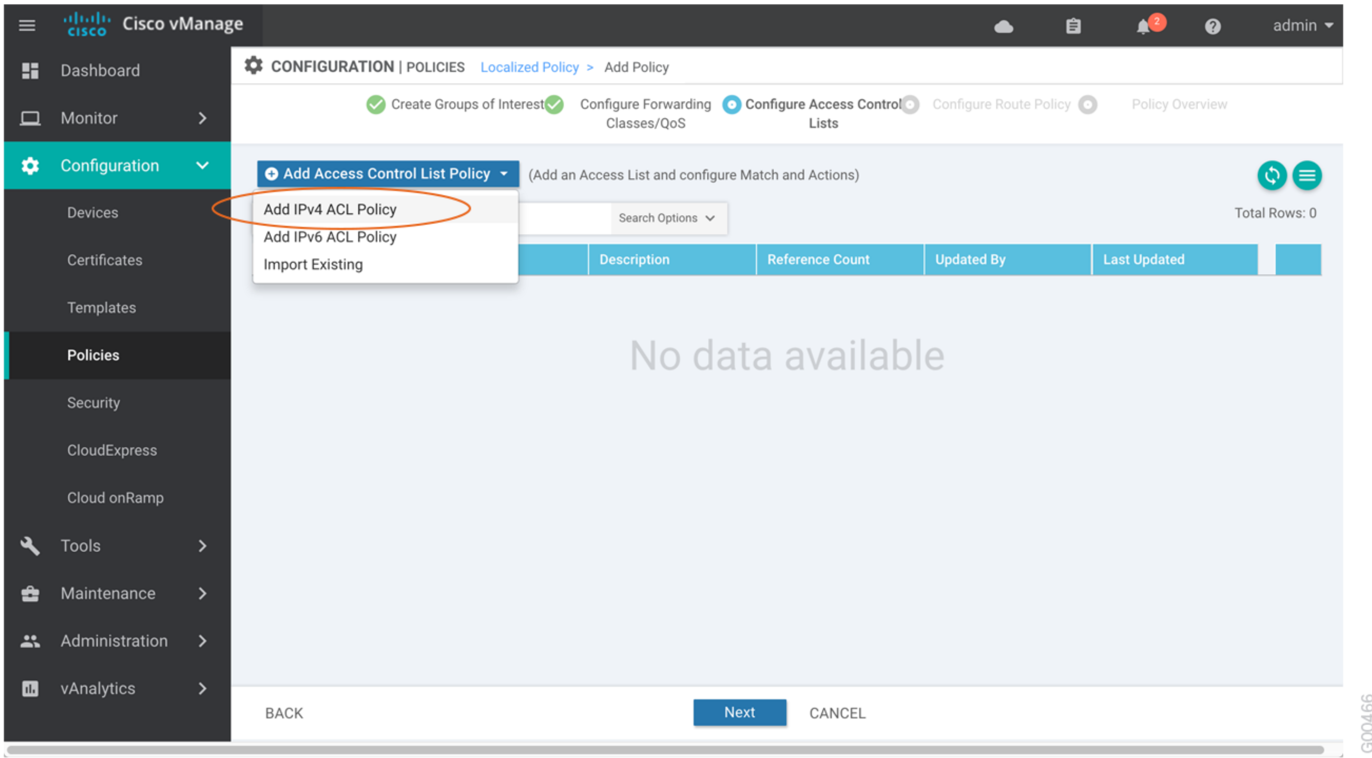
6. Click Next to move to Configure Access Lists in the wizard.

## Step 4: Configure ACLs

In the Configure Access Control Lists screen, configure ACLs:




1. To create a new IPv4 ACL, click the Add Access Control List Policy drop-down. Then select Add IPv4 ACL Policy:




2. To create a new IPv6 ACL, click the Add Access Control List Policy drop-down. Then select Add IPv6 ACL Policy.
3. Enter a name and description for the ACL.
4. In the left pane, click Add ACL Sequence. An Access Control List box is displayed in the left pane.
5. Double-click the Access Control List box, and type a name for the ACL.
6. In the right pane, click Add Sequence Rule to create a single sequence in the ACL. The Match tab is selected by default.
7. Click a match condition.
8. On the left, enter the values for the match condition.
9. On the right enter the action or actions to take if the policy matches.
10. Repeat Steps 6 through 8 to add match–action pairs to the ACL.
11. To rearrange match–action pairs in the ACL, in the right pane drag them to the desired position.
12. To remove a match–action pair from the ACL, click the X in the upper right of the condition.
13. Click Save Match and Actions to save a sequence rule.
14. To rearrange sequence rules in an ACL, in the left pane drag the rules to the desired position.
15. To copy, delete, or rename an ACL sequence rule, in the left pane, click More Options next to the rule's name and select the desired option.
16. If no packets match any of the ACL sequence rules, the default action is to drop the packets. To change the default action:
    a. Click Default Action in the left pane.

b. Click the Pencil icon.

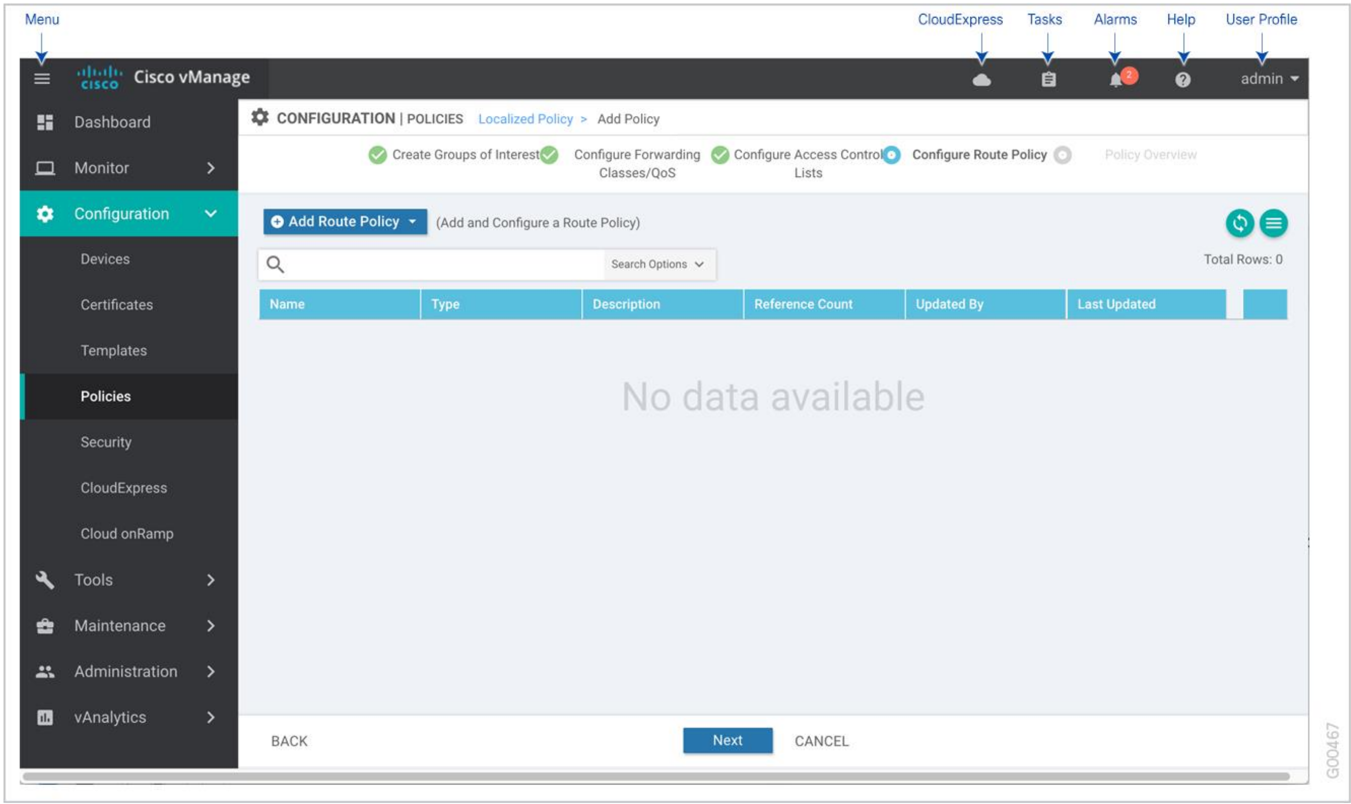
c. Change the default action to Accept.

d. Click Save Match and Actions.

17. Click Next to move to Configure Route Policy in the wizard.

## Step 5: Configure Route Policies

In Configure Route Policy, configure route policies:




1. In the Add Route Policy tab, select Create New.

2. Enter a name and description for the route policy.

3. In the left pane, click Add Sequence Type. A Route box is displayed in the left pane.

4. Double-click the Route box, and type a name for the route policy.

5. In the right pane, click Add Sequence Rule to create a single sequence in the policy. The Match tab is selected by default.

6. Click a match condition.

7. On the left, enter the values for the match condition. You can select the modifiers OR, AND, or EXACT to focus the scope of a rule. OR applies to multiple community lists and is valid for all platforms; AND and EXACT apply to only one community list at a time and are not valid for vEdge devices.

8. On the right enter the action or actions to take if the policy matches.

9. Repeat Steps 6 through 8 to add match–action pairs to the route policy.

10. To rearrange match–action pairs in the route policy, in the right pane drag them to the desired position.

11. To remove a match–action pair from the route policy, click the X in the upper right of the condition.

12. Click Save Match and Actions to save a sequence rule.

13. To rearrange sequence rules in an route policy, in the left pane drag the rules to the desired position.

14. To copy, delete, or rename an route policy sequence rule, in the left pane, click More Options next to the rule's name and select the desired option.

15. If no packets match any of the route policy sequence rules, the default action is to drop the packets. To change the default action:

    a. Click Default Action in the left pane.

    b. Click the Pencil icon.

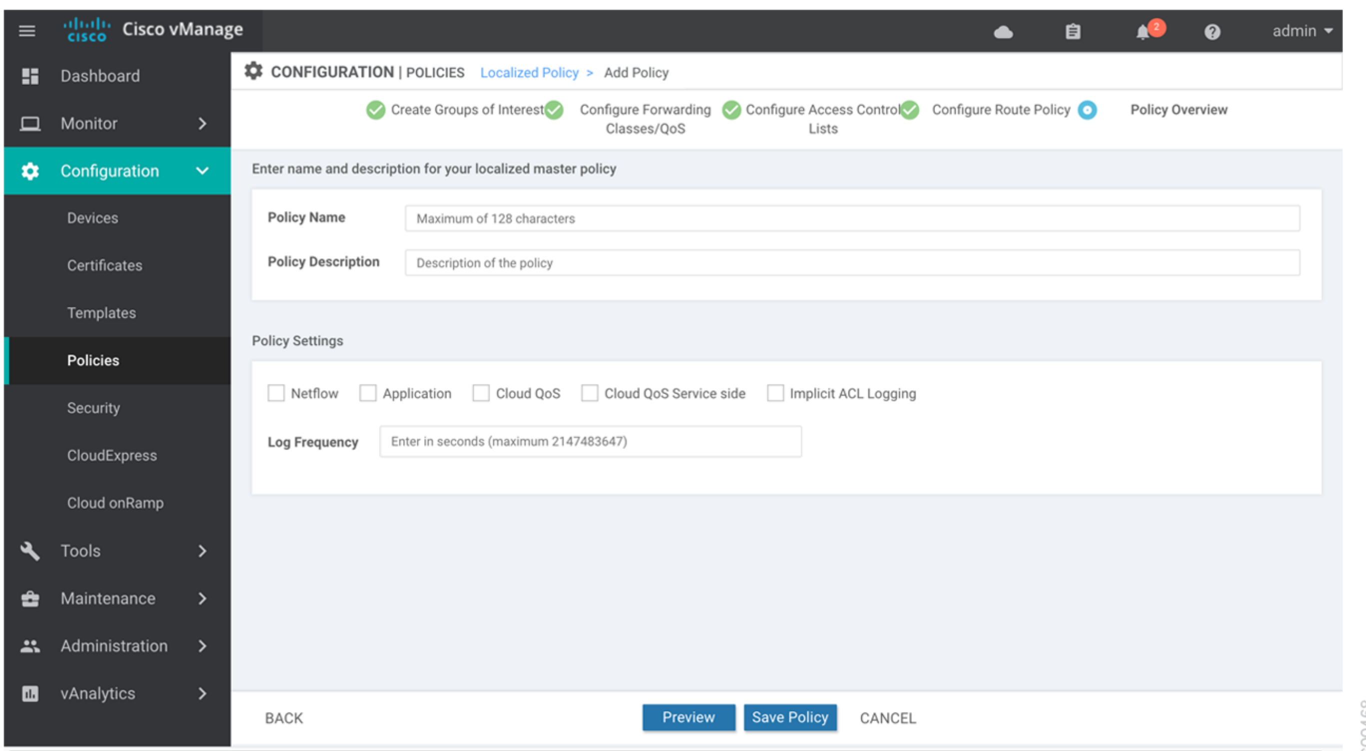
    c. Change the default action to Accept.

    d. Click Save Match and Actions.

16. Click Next to move to Policy Overview in the wizard.

## Step 6: Configure Policy Settings

In Policy Overview, configure policy settings:




1. Enter a name and description for the route policy.

2. To enable cflowd visibility so that a vEdge router can perform traffic flow monitoring on traffic coming to the router from the LAN, click Netflow.
3. To enable application visibility so that a vEdge router can monitor and track the applications running on the LAN, click Application.
4. To enable QoS scheduling and shaping for traffic that a vEdge Cloud router receives from transport-side interfaces, click Cloud QoS.
5. To enable QoS scheduling and shaping for traffic that a vEdge Cloud router receives from service-side interfaces, click Cloud QoS Service Side.
6. To log the headers of all packets that are dropped because they do not match a service configured by an Allow Service parameter on a tunnel interface, click Implicit ACL Logging.
7. To configure how often packets flows are logged, click Log Frequency. Packet flows are those that match an access list (ACL), a cflowd flow, or an application-aware routing flow.
8. Click Preview to view the full policy in CLI format.
9. Click Save Policy.

# Security

# Templates

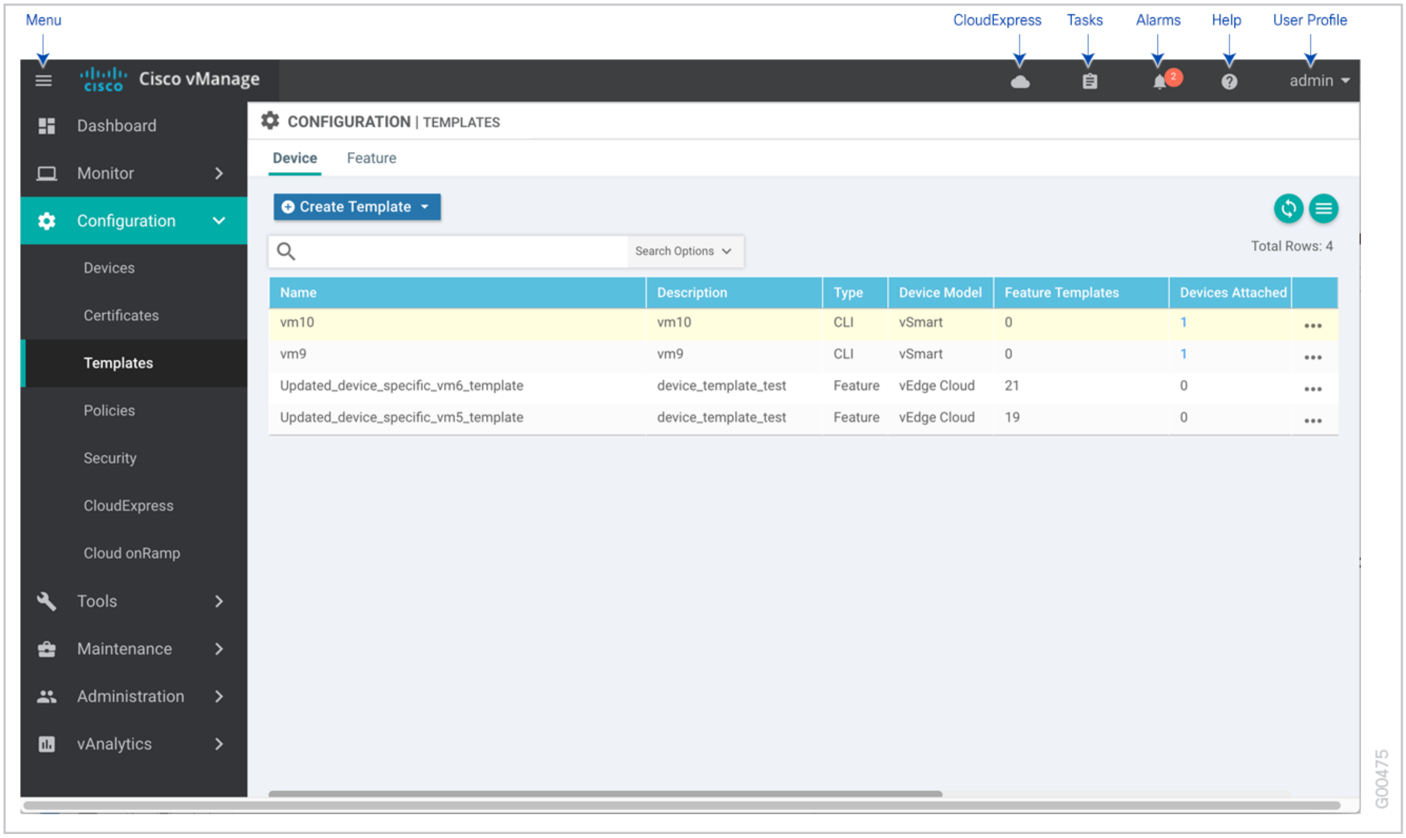
Use the Templates screen to configure all Viptela devices in the overlay network that are managed by the vManage NMS. To do so:

1. **Create a device template** .
2. **Attach Viptela devices to the device template** .

Note: To create and modify a device's configuration, use vManage templates, along with other configuration-related screens in the vManage Configuration and Administration menus. Do not modify configurations from the command-line interface (CLI) unless you are explicitly directed to do so.

## Screen Elements

- Top bar—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.
- Title bar—Includes the title of the screen, Templates.
- Device tab—Create device templates for configuring Viptela devices.
  - Create Template drop-down—Click to create device templates from feature template or the CLI.
  - Device template table—Table of all device templates. To re-arrange the columns, drag the column title to the desired position.
- Feature tab—Create feature templates for configuring software features that you can enable on a Viptela device.
  - Add Template button—Click to create feature templates.
  - Feature template table—Table of all feature templates. To re-arrange the columns, drag the column title to the desired position.
- Search box—Includes the Search Options drop-down, for a Contains or Match string.
- Refresh icon—Click to refresh data in the templates table with the most current data.
- Show Table Columns icon—Click to display or hide columns from the templates table. By default, all columns are displayed.
- Templates table—To re-arrange the columns, drag the column title to the desired position.




# Create a Device Template

Device templates define a device's complete operational configuration. A device template consists of a number of feature templates. Each feature template defines the configuration for a particular Cisco SD-WAN software feature. Some feature templates are mandatory, indicated with an asterisk (*), and some are optional. Each mandatory feature template, and some of the optional ones too, have a factory-default template. For software features that have a factory-default template, you can use either the factory-default template (named Factory_Default_ *feature-name* _Template) or you can create a custom feature template.

## Create a Device Template from Feature Templates

To create a device template:

1. In the Device tab, click the Create Template drop-down and select From Feature Template.
2. From the Device Model drop-down, select the type of device for which you are creating the template. vManage NMS displays all the feature templates for that device type. The required feature templates are indicated with an asterisk (*), and the remaining templates are optional. The factory-default template for each feature is selected by default.
3. In the Template Name field, enter a name for the device template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.
4. In the Description field, enter a description for the device template. This field is mandatory, and it can contain any characters and spaces.
5. To view the factory-default configuration for a feature template, select the desired feature template and click View Template. Click Cancel to return to the Configuration Template screen.

6. To create a custom template for a feature, select the desired factory-default feature template and click Create Template. The template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining feature parameters.

7. In the Template Name field, enter a name for the feature template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.

8. In the Description field, enter a description for the feature template. This field is mandatory, and it can contain any characters and spaces.

9. For each field, enter the desired value. You may need to click a tab or the plus sign (+) to display additional fields.

10. 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:

| 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 Viptela device to a device template** .<br><br>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 Use Variable Values in Configuration Templates .<br><br>To change the default key, type a new string and move the cursor out of the Enter Key box.<br><br>Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID. |
| Global (indicated by a globe icon) | Enter a value for the parameter, and apply that value to all devices.<br><br>Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs. |

12. For some groups of parameters, you can mark the entire group as device-specific. To do this, click the Mark as Optional Row box. These parameters are then grayed out so that you cannot enter a value for them in the feature template. You enter the value or values when you attach a Viptela device to a device template.

13. Click Save.

14. Repeat Steps 7 through 13 to create a custom template for each additional software feature. For details on creating specific feature templates, see the templates listed in **Available Feature Templates.**

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

Another way to create device templates from feature templates is to first create one or more custom feature templates and then create device templates. You can create multiple feature templates for the same feature. For a list of feature templates, see Available Feature Templates .

1. From the Templates title bar, select Feature.

2. Click the Add Template button.

3. In the left pane, from Select Devices, select the type of device for which you are creating a template. You can create a single feature template for features that are available on multiple device types. You must, however, create separate feature templates for software features that are available only on the device type you are configuring.

4. In the right pane, select the feature template. The template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining required parameters. If the feature has optional parameters, the bottom of the template form shows a plus sign (+) after the required parameters.

5. In the Template Name field, enter a name for the feature template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.

6. In the Description field, enter a description for the feature template. This field is mandatory, and it can contain any characters and spaces.

7. For each required parameter, choose the desired value, and if applicable, select the scope of the parameter. Select the scope from the drop-down menu to the left of each parameter's value box

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

9. Click Save.

10. Repeat Steps 2 to 9 for each additional feature template you wish to create.

11. From the Templates title bar, select Device.

12. Click the Create Template drop-down and select From Feature Template.

13. From the Device Model drop-down, select the type of device for which you are creating the device template. vManage NMS displays the feature templates for the device type you selected. The required feature templates are indicated with an asterisk (*). The remaining templates are optional.

14. In the Template Name field, enter a name for the device template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.

15. In the Description field, enter a description for the device template. This field is mandatory, and it can contain any characters and spaces.

16. To view the factory-default configuration for a feature template, select the desired feature template and click View Template. Click Cancel to return to the Configuration Template screen.

17. To use the factory-default configuration, click Create to create the device template. The new device template is displayed in the Device Template table. The Feature Templates column shows the number of feature templates that are included in the device template, and the Type column shows "Feature" to indicate that the device template was created from a collection of feature templates.

18. To modify the factory-default configuration, select the feature template for which you do not wish to use the factory-default template. From the drop-down list of available feature templates, select a feature template that you created.

19. Repeat Step 18 for each factory-default feature template you wish to modify.

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

## Create a Device Template from the CLI

To create a device template by entering a CLI text-style configuration directly on the vManage NMS:

1. In the Device tab, click the Create Template drop-down and select CLI Template.

2. From the Device Type drop-down, select the type of device for which you are creating the template.

3. In the Template Name field, enter a name for the device template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores (_). It cannot contain spaces or any other characters.

4. In the Description field, enter a description for the device template. This field is mandatory, and it can contain any characters and spaces.

5. In the CLI Configuration box, enter the configuration either by typing it, cutting and pasting it, or uploading a file.
6. To convert an actual configuration value to a variable, select the value and click Create Variable. Enter the variable name, and click Create Variable. You can also type the variable name directly, in the format {{ *variable-name* }}; for example, {{hostname}}.
7. Click Add. The new device template is displayed in the Device Template table. The Feature Templates column shows the number of feature templates that are included in the device template, and the Type column shows "CLI" to indicate that the device template was created from CLI text.

## Edit a Template

1. In the Device or Feature tab, select a template.
2. Click the More Actions icon to the right of the row and click Edit.

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

Note that you can edit templates simultaneously from one or more vManage servers. For simultaneous template edit operations, the following rules apply:

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

## View a Template

1. In the Device or Feature tab, select a template.
2. Click the More Actions icon to the right of the row and click View.

## Delete a Template

1. In the Device or Feature tab, select a template.
2. Click the More Actions icon to the right of the row and click Delete.
3. Click OK to confirm deletion of the template.

## View Device Templates Attached to a Feature Template

1. In the Feature tab, select a template.
2. Click the More Actions icon to the right of the row and click Show Attached Device Templates.
   The View Attached Device Templates popup window opens, displaying the names of the device templates to which the feature template is attached.

## View Devices Attached to a Device Template

For a device template that you created from feature templates:

1. In the Device tab, select a template.
2. Click the More Actions icon to the right of the row and click Attach Devices.
3. In the Attach Devices window, click the Attached Devices tab.

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

1. In the Device tab, select a template.
2. Click the More Actions icon to the right of the row and click Show Attached Devices.

## Perform Parallel Template Operations

On Viptela devices in the overlay network, you can perform the same operations, in parallel, from one or more vManage servers. You can perform the following template operations in parallel:

- Attach devices to a device template
- Detach devices from a device template
- Change the variable values for a device template that has devices attached to it

For template operations, the following rules apply:

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

## Attach Devices to a Device Template

To attach one or more devices to a device template:

1. In the Device tab, select a template.
2. Click the More Actions icon to the right of the row and click Attach Devices. The Attach Devices dialog box opens with the Select Devices tab selected
3. In the Available Devices column on the left, select a group and search for one or more devices, select a device from the list, or click Select All.
4. Click the arrow pointing right to move the device to the Selected Devices column on the right.
5. Click Attach.
6. If the template contains variables, enter the missing variable values for each device you selected in one of the following ways:

- Enter the values manually for each device either in the table column or by clicking the More Actions icon to the right of the row and clicking Edit Device Template. When you are using optional rows, if you do not want to include the parameter for the specific device, do not specify a value.
- Click Import File in the upper right corner of the screen to upload a CSV file that lists all the variables and defines each variable's value for each device.

7. Click Update

8. Click Next.
If any devices have the same system IP address, a pop-up or an error message is displayed when you click Next. Modify the system IP addresses so that there are no duplicates, and click Save. Then click Next again.

9. In the left pane, select the device, to preview the configuration that is ready to be pushed to the device. The right pane displays the device's configuration and the Config Preview tab in the upper right corner is selected.
Click the Config Diff tab to view the differences between this configuration and the configuration currently running on the device, if applicable.
Click the Back button to edit the variable values entered in the previous screen.

10. If you are attaching a vEdge router, click Configure Device Rollback Timer located at the bottom of the left pane, to configure the time interval at which the device rolls back to its previous configuration if the router loses its control connection to the overlay network. The Configure Device Rollback Time dialog box is displayed.

    a. From the Devices drop-down, select a device.

    b. To enable the rollback timer, in the Set Rollback slider beneath the Devices drop-down, drag the slider to the left to enable the rollback timer. When you do this, the slider changes in color from gray to green.

    c. To disable the rollback timer, click the Enable Rollback slider. When you disable the timer, the Password field pops up. Enter the password that you used to log in to the vManage NMS.

    d. In the Device Rollback Time slider, drag the slider to the desired value. The default time is 5 minutes. You can configure a time from 6 to 15 minutes.

    e. To exclude a device from the rollback timer setting, click Add Exception and select the devices to exclude.

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

    g. Click Save.

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

## Copy a Template

1. In the Device or Feature tab, select a template.

2. Click the More Actions icon to the right of the row and click Copy.

3. Enter a new template name and description.

4. Click Copy.

## Edit a CLI Device Template

1. In the Device tab, select a template.

2. Click the More Actions icon to the right of the row and click Edit.

3. In the Device CLI Template window, edit the template.

4. Click Update.

## Export a Variables Spreadsheet in CSV Format for a Template

1. In the Device tab, select a device template.
2. Click the More Actions icon to the right of the row and click Export CSV.

## Change the Device Rollback Timer

By default, when you attach a vEdge router to a configuration template, if the router is unable to successfully start after 5 minutes, it returns to, or rolls back to, the previous configuration For a configuration that you have created from the CLI, you can change the device's rollback timer:

1. In the Device tab, select a device template.
2. Click the More Actions icon to the right of the row and click Change Device Values. The right pane displays the device's configuration, and the Config Preview tab in the upper right corner is selected.
3. In the left pane, click the name of a device.
4. Click Configure Device Rollback Timer located at the bottom of the left pane. The Configure Device Rollback Time dialog box is displayed.
5. From the Devices drop-down, select a device.
6. To enable the rollback timer, in the Set Rollback slider beneath the Devices drop-down, drag the slider to the left to enable the rollback timer. When you do this, the slider changes in color from gray to green.
7. To disable the rollback timer, click the Enable Rollback slider. When you disable the timer, the Password field pops up. Enter the password that you used to log in to the vManage NMS.
8. In the Device Rollback Time slider, drag the slider to the desired value. The default time is 5 minutes. You can configure a time from 6 to 15 minutes.
9. To exclude a device from the rollback timer setting, click Add Exception and select the devices to exclude.
10. The table at the bottom of the Configure Device Rollback Time dialog box lists all the devices to which you are attaching the template and their rollback time. To delete a configured rollback time, click the Trash icon to right right of the device name.
11. Click Save.
12. Click Configure Devices to push the configuration to the devices.
    The Status column displays whether the configuration was successfully pushed. Click the right angle bracket to the left of the row to display details of the push operation.

## Preview the Configuration and View Configuration Differences

For a configuration that you have created from the CLI:

1. In the Device tab, select a device template.
2. Click the More Actions icon to the right of the row and click Change Device Values. The right pane displays the device's configuration, and the Config Preview tab in the upper right corner is selected.
3. In the left pane, click the name of a device.
4. Click the Config Diff tab to view the differences between this configuration and the configuration currently running on the device, if applicable.
   Click the Back button to edit the variable values entered in the previous screen.

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

## Change Variable Values for a Device

For a configuration that you have created from device configuration templates, if the templates contain variables, the vManage NMS can automatically populate the variables with actual values when you attach the templates to the devices. To do this, you create an Excel file that lists the variable values for each device and save the file in CSV format. You can also enter values for these variables manually.

After you have pushed the configuration to a device, you can change the value assigned to any variable:

1. In the Device tab, select the device template.
2. Click the More Actions icon to the right of the row, and click Change Device Values. The screen displays a table of all the devices that are attached to that device template.
3. For the desired device, click the More Actions icon to the right of the row, and click Edit Device Template.
4. In the Update Device Template pop-up, enter values for the items in the variable list.
5. Click Update.
6. Click Next.
7. Click Configure Devices to push the configuration to the device.
   The Status column displays if the configuration was successfully pushed or not. Click the right angle bracket to the left of the row to display details of the push operation.

## Available Feature Templates

vManage NMS provides the following feature templates to configure Viptela devices in the overlay network:

- AAA
- Archive
- Banner
- BFD
- BGP
- Bridge
- Cellular Controller
- Cellular Profile
- DHCP Server
- GPS
- IGMP
- Logging
- Multicast

# AAA

Use the AAA template for vBond controllers, vManage NMSs, vSmart controllers, vEdge routers, and Cisco IOS XE routers.

Viptela devices support configuration of authentication, authorization, and accounting (AAA) in combination with RADIUS and TACACS+.

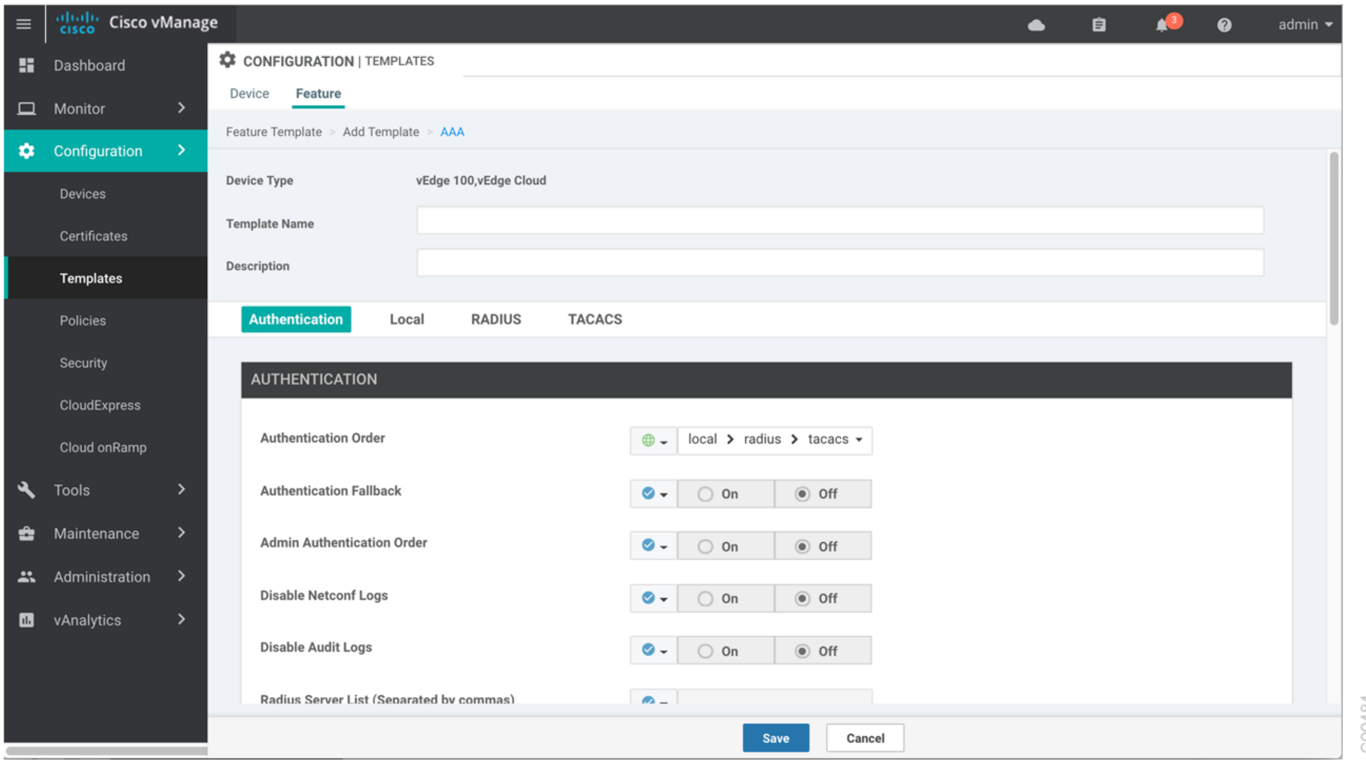
## Navigate to the Template Screen and Name the Template

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. Select the Basic Information tab.

6. To create a custom template for AAA, select the Factory_Default_AAA_Template and click Create Template. The AAA template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining AAA 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 and select one of the following:

| 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 Viptela device to a device template** .<br><br>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 .<br><br>To change the default key, type a new string and move the cursor out of the Enter Key box.<br><br>Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID. |

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

## Configure Authentication Order and Fallback

To configure AAA authentication order and authentication fallback on a Viptela device, select the Authentication tab and configure the following parameters:

| 1. Parameter Name | Description |
|---|---|
| Authentication Order | The default order is local, then radius, and then tacacs.<br><br>To change the default order of authentication methods that the software tries when verifying user access to a Viptela device:<br><br>1. Click the dropdown arrow to display the list of authentication methods.<br><br>2. In the list, click the up arrows to change the order of the authentication methods and click the boxes to select or deselect a method.<br><br>If you select only one authentication method, it must be **local** . |
| Authentication Fallback | Click On to configure authentication to fall back from RADIUS or TACACS+ to the next priority authentication method if the user cannot be authenticated or if the RADIUS or TACACS+ servers are unreachable. With the default configuration (Off), authentication falls back only if the RADIUS or TACACS+ servers are unreachable. |
| Admin Authentication Order | Have the "admin" user use the authentication order configured in the Authentication Order parameter. If you do not configure the admin authentication order, the "admin" user is always authenticated locally. |
| Disable Netconf Logs | Click On to disable the logging of Netconf events. By default, these events are logged to the auth.info and messages log files. |
| Disable Audit Logs | Click On to disable the logging of AAA events. By default, these events are logged to the auth.info and messages log files. |
| RADIUS Server List | List the tags for one or two RADIUS servers. Separate the tags with commas. You set the tag under the RADIUS tab. |

*CLI equivalent:*

```
system
  aaa
    admin-auth-order
    auth-fallback
    auth-order (local | radius | tacacs)
    logs
      [no] audit-disable
      [no] netconf-disable
    radius-servers tag
```

## Configure Local Access for Users and User Groups

To configure local access for individual users, select the Local tab. To add a new user, select the User tab, click Add New User, and configure the following parameters:

| Parameter Name | Description |
|---|---|

| | |
|---|---|
| Name | Enter a name for the user. It can be 1 to 128 characters long, and it must start with a letter. The name can contain only lowercase letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.). The name cannot contain any uppercase letters.<br><br>The following usernames are reserved, so you cannot configure them: backup, basic, bin, daemon, games, gnats, irc, list, lp, mail, man, news, nobody, proxy, quagga, root, sshd, sync, sys, uucp, and www-data. Also, names that start with viptela-reserved are reserved. |
| Password | Enter a password for the user. The password is an MD5 digest string, and it can contain any characters, including tabs, carriage returns, and linefeeds. For more information, see Section 9.4 in RFC 7950, *The YANG 1.1 Data Modeling Language.*<br><br>Each username must have a password. Each user is allowed to change their own password.<br><br>The default password for the admin user is admin. It is strongly recommended that you change this password. |
| Description | Enter a description for the user. |
| User Groups | Select from the list of configured groups. You must assign the user to at least one group. The admin user is automatically placed in the netadmin group and is the only member of this group. |

Click Add to add the new user. Click Add New User again to add additional users.

To configure local access for user groups, you first place the user into either the basic or operator group. The admin is automatically placed in the netadmin group. Then you configure user groups. To do this, select the Local tab, select the User Group tab, click Add New User Group, and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Name | Name of an authentication group. It can be 1 to 128 characters long, and it must start with a letter. The name can contain only lowercase letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.). The name cannot contain any uppercase letters.<br>The Viptela software provides three standard user groups, basic, netadmin, and operator. The user admin is automatically placed in the group netadmin and is the only user in this group. All users learned from a RADIUS or TACACS+ server are placed in the group basic. All users in the basic group have the same permissions to perform tasks, as do all users in the operator group.<br>The following groups names are reserved, so you cannot configure them: adm, audio, backup, bin, cdrom, dialout, dip, disk, fax, floppy, games, gnats, input, irc, kmem, list, lp, mail, man, news, nogroup, plugdev, proxy, quagga, quaggavty, root, sasl, shadow, src, sshd, staff, sudo, sync, sys, tape, tty, uucp, users, utmp, video, voice, and www-data. Also, group names that start with the string viptela-reserved are reserved. |
| Feature | The feature table lists the roles for the user group. These roles are Interface, Policy, Routing, Security, and System. Each role allows the user group to read or write specific portions of the device's configuration and to execute specific types of operational commands. Click the appropriate boxes for Read, Write, and None to assign privileges to the group for each role. |

Click Add to add the new user group.

To add another user group, click Add New User Group again.

To delete a user group, click the trash icon at the right side of the entry. You cannot delete the three standard user groups, basic, netadmin, and operator.

*CLI equivalent:*

```
system
  aaa
    user username
      group group-name
      password password
    usergroup group-name
      task (interface | policy | routing | security | system) (read | write)
```

## Configure RADIUS Authentication

To configure RADIUS authentication, select the RADIUS tab and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Retransmit Count | Specify how many times to search through the list of RADIUS servers while attempting to locate a server.<br><br>*Range:* 1 through 1000<br>*Default:* 3 |
| Timeout | Specify how long to wait to receive a reply form the RADIUS server before retransmitting a request.<br><br>*Range:* 1 through 1000<br>*Default:* 5 seconds |

To configure a connection to a RADIUS server, select the RADIUS tab, click Add New Radius Server, and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Address | Enter the IP address of the RADIUS server host. |
| Tag | Enter a text string to identify the RADIUS server. The tag can be 4 to 16 characters long. The tag allows you to configure authentication for AAA, IEEE 802.1X, and IEEE 802.11i to use a specific RADIUS server or servers.<br>For Cisco routers running Viptela software, this field is ignored. |
| Authentication Port | Enter the UDP destination port to use for authentication requests to the RADIUS server. If the server is not used for authentication, configure the port number to be 0.<br>*Default:* Port 1812 |
| Accounting Port | Enter the UDP port to use to send 802.1X and 802.11i accounting information to the RADIUS server.<br>*Range:* 0 through 65535<br>*Default:* 1813 |
| Key (Deprecated) | This field is deprecated. Use the Secret Key field instead. |
| Secret Key | Enter the key the Viptela device passes to the RADIUS server for authentication and encryption. You can type the key as a text string from 1 to 32 characters long, and it is immediately encrypted, or you can type an AES 128-bit encrypted key. The key must match the AES encryption key used on the RADIUS server. |
| Source Interface | Enter the name of the interface on the local device to use to reach the RADIUS server. |
| VPN ID | Enter the number of the VPN in which the RADIUS server is located or through which the server can be reached. If you configure multiple RADIUS servers, they must all be in the same VPN. |
| Priority | Enter the priority of a RADIUS server. A server with a lower number is given priority.<br>*Range:* 0 through 7<br>*Default:* 0 |

Click Add to add the new RADIUS server.

To add another RADIUS server, click Add New RADIUS Server again.

To remove a server, click the trash icon on the right side of the line.

*CLI equivalent:*

```
system
  radius
    retransmit number
    server ip-address
```

```
    acct-port port-number
    auth-port port-number
    priority number
    secret-key key
    source-interface interface-name
    tag tag
    vpn vpn-id
  timeout seconds
```

## Configure TACACS+ Authentication

To configure the device to use TACACS+ authentication, select the TACACS tab and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Timeout | Enter how long to wait to receive a reply from the TACACS+ server before retransmitting a request.<br><br>*Range:* 1 through 1000<br>*Default:* 5 seconds |
| Authentication | Set the type of authentication to use for the server password. The default authentication type is PAP. You can change it to ASCII. |

To configure a connection to a TACACS+ server, select the TACACS tab, click Add New TACSCS Server, and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Address | Enter the IP address of the TACACS+ server host. |
| Authentication Port | Enter the UDP destination port to use for authentication requests to the TACACS+ server. If the server is not used for authentication, configure the port number to be 0.<br><br>*Default:* Port 49 |
| Key (Deprecated) | This field is deprecated. Use the Secret Key field instead. |
| Secret Key | Enter the key the Viptela device passes to the TACACS+ server for authentication and encryption. You can type the key as a text string from 1 to 32 characters long, and it is immediately encrypted, or you can type an AES 128-bit encrypted key. The key must match the AES encryption key used on the TACACS+ server. |
| Source Interface | Enter the name of the interface on the local device to use to reach the TACACS+ server. |
| VPN ID | VPN in which the TACACS+ server is located or through which the server can be reached. If you configure multiple TACACS+ servers, they must all be in the same VPN. |
| Priority | Set the priority of a TACACS+ server. A server with lower priority number is given priority over one with a higher number.<br>*Range:* 0 through 7<br>*Default:* 0 |

Click Add to add the new TACACS server.

To add another TACACS server, click Add New TACACS Server again.

To remove a server, click the trash icon on the right side of the line.

*CLI equivalent:*

```
system
  tacacs
    authentication password-authentication
    server ip-address
      auth-port port-number
      priority number
      key key
      source-interface interface-name
      vpn vpn-id
    timeout seconds
```

## Release Information

Introduced in vManage NMS in Release 15.2.
In Release 17.1, add Disable Netconf Logs and Disable Audit Logs fields.

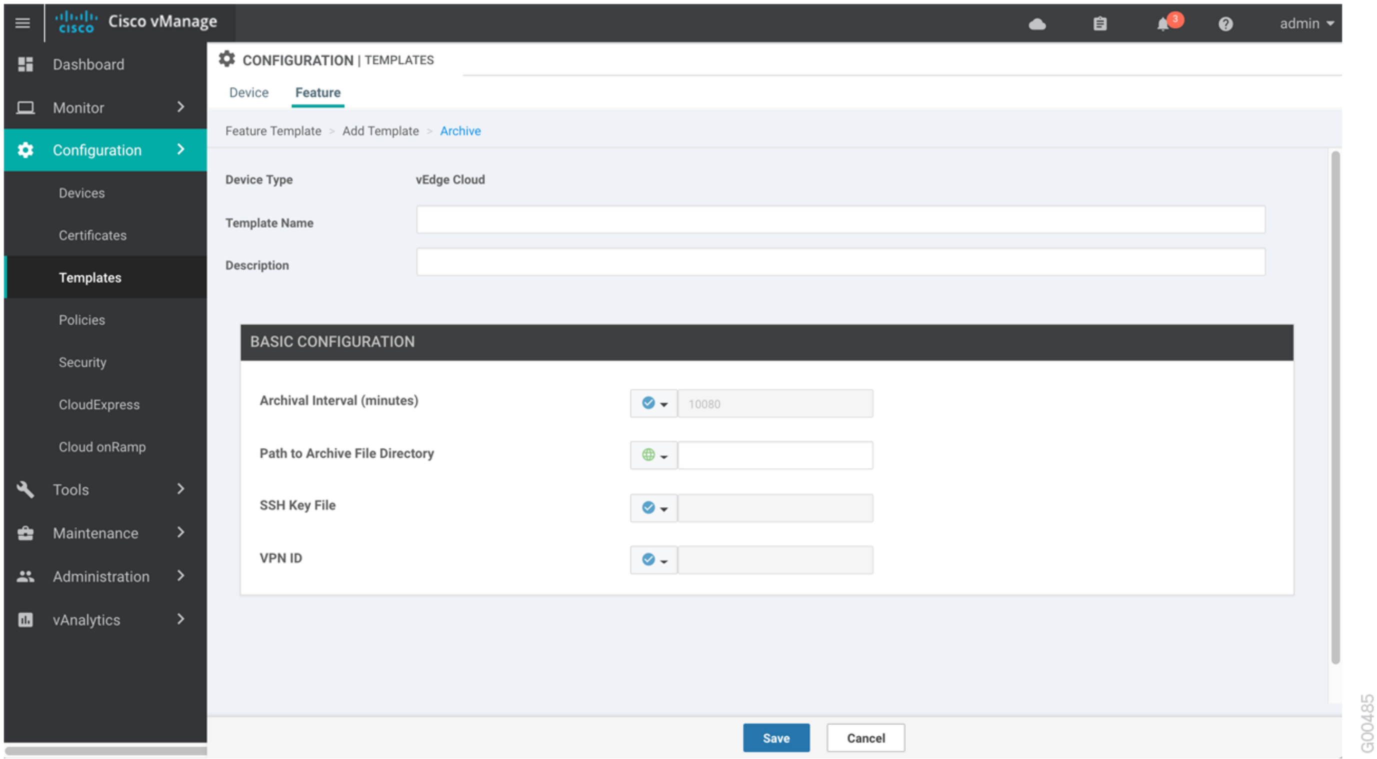
## Archive

Use the Archive template for vBond controllers, vManage NMSs, vSmart controllers, and vEdge routers.

You can configure a Viptela device to periodically archive a copy of the full running configuration to an archival file. The running configuration that is archived is viewable by the user "admin".

## 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. Under Additional System Templates, located to the right of the screen, click Archive.
6. From the Archive drop-down, click Create Template. The Archive template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining Archive 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 and select one of the following:

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

## Configure Configuration Archive Configuration

To configure archiving of running configurations, configure the following parameters:

| Parameter Name | Description |
|---|---|
| Archival Interval | Specify how often to archive the full running configuration. In addition, the running configuration is archived each time you issue the **commit** command on the device.<br>*Range:* 5 minutes through 525600 minutes (about one year)<br>*Default* : 10080 minutes (7 days) |
| Path to Archive File Directory | Specify the path to the directory in which to store the archival file and the base name of the file. The path can be one of the following:<br>• **ftp:** *file-path* —Path to a file on an FTP server.<br>• **scp:** *user* **@** *host* **:** *file-path*<br>• **path** *file-path* / *filename* **/** *file-path* **/** *filename* —Path to a file on the local Viptela device.<br>A separate file is created for each archiving operation. To distinguish the files, a timestamp is appended to the filename. The timestamp has the format *yyyy* - *mm* - *dd* _ *hh* - *mm* - *ss* . |
| SSH Key File | Enter the name of the SSH private key file on the local Viptela device. This file is used to SCP into a remote file server. The Viptela software automatically generates a public and a private key and places the public key in the SSH key file archive_id_rsa.pub, which is located in /home/admin directory on the Viptela device.<br>If you do not enter the name of an SSH private key file, the software uses the automatically generated private key. |
| VPN ID | Enter the ID for the VPN in which the archival file server is located or through which the server can be reached. On vEdge routers, *vpn-id* can be a value from 0 through 65530. On vSmart controllers, *vpn-id* can be either 0 or 512. |

To save the feature template, click Save.

*CLI equivalent:*

```
system
  archive
    interval minutes
    path file-path
    ssh-id-file filename
    vpn vpn-id
```

## Release Information

Introduced in vManage NMS in Release 15.2.

## Banner

Use the Banner template for vBond controllers, vManage NMSs, vSmart controllers, vEdge routers, and Cisco IOS XE routers.

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

- To configure the banner text for login screens using vManage templates, create a Banner feature template to configure PIM parameters, as described in this article.
- To configure a login banner for the vManage NMS system, see the Administration ► Settings help file.

## Navigate to the Template Screen and Name the Template

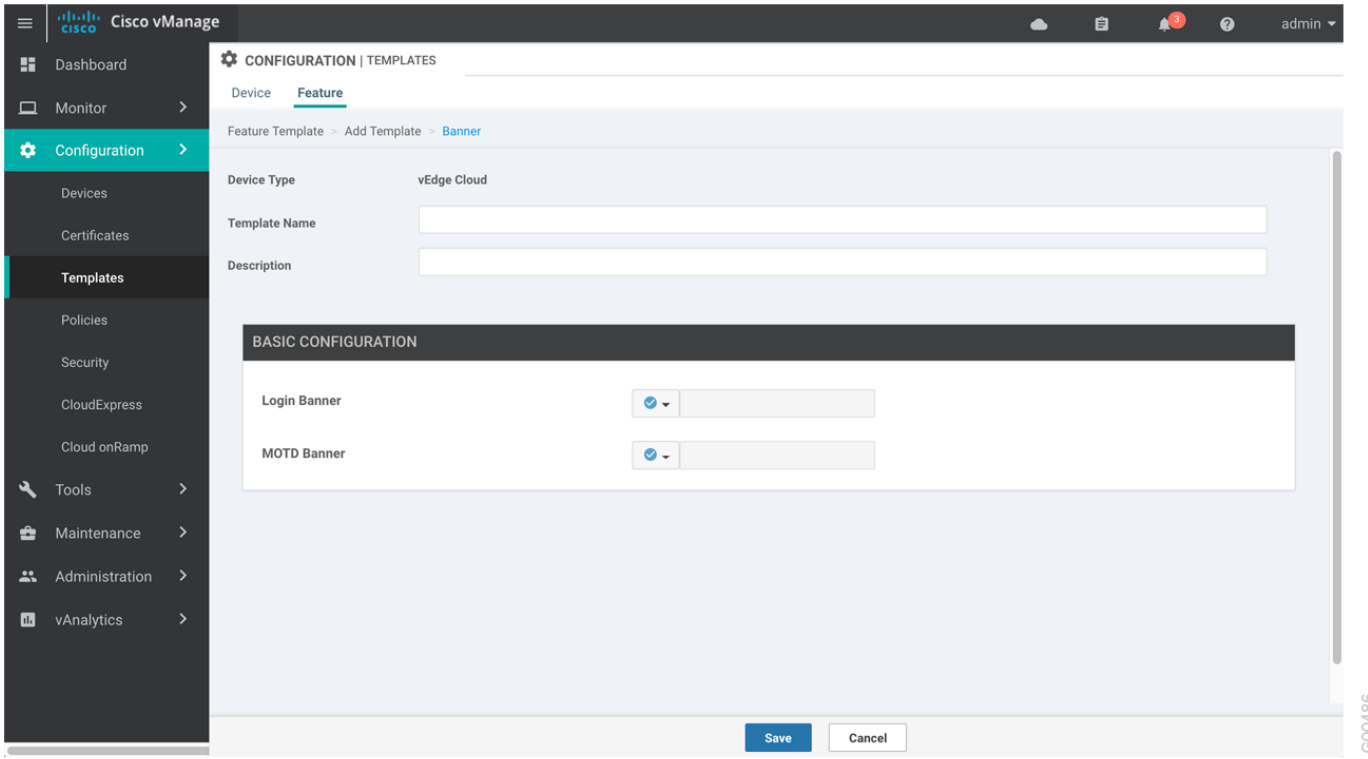
1. In vManage NMS, select the Configuration ► Templates screen.
2. In the Device tab, click Create Template.

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. 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 and select one of the following:

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

## Configure the Banner

To set a banner, configure the following parameters:

| Parameter Name | Description |
|---|---|
| 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** . |
| MOTD Banner | 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** . |

To save the feature template, click Save.

*CLI equivalent:*

```
banner
  login "text"
  motd "text"
```

## Release Information

Introduced in vManage NMS in Release 15.2.

## BFD

Use the BFD template for vEdge routers and Cisco IOS XE routers.

The BFD protocol, which detects link failures as part of the Viptela high availability solution, is enabled by default on all vEdge routers, and you cannot disable it.

## Navigate to the Template Screen

1. In vManage NMS, select the Configuration ▶ Templates screen.

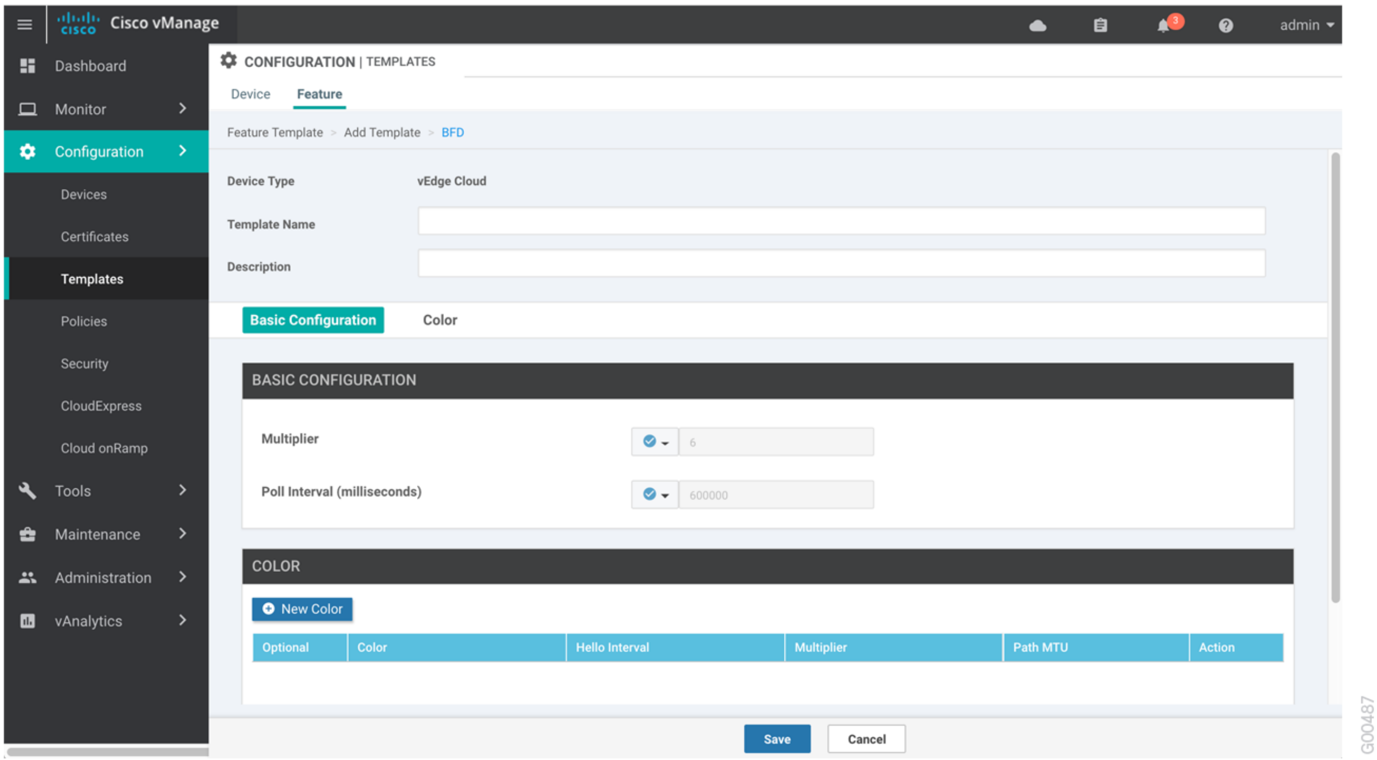
2. In the Device tab, click Create Template.

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 BFD, select the Factory_Default_BFD_Template and click Create Template. The BFD template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining BFD parameters. You may need to click a tab or the plus sign (+) to display additional fields.

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:

| 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 Viptela device to a device template** .<br><br>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 .<br><br>To change the default key, type a new string and move the cursor out of the Enter Key box.<br><br>Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID. |

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

## Configure BFD for Application-Aware Routing

To configure the BFD timers used by application-aware routing, click the Basic Configuration tab and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Multiplier | Specify the value by which to multiply the poll interval, to set how often application-aware routing acts on the data plane tunnel statistics to figure out the loss and latency and to calculate new tunnels if the loss and latency times do not meet configured SLAs.<br>*Range:* 1 through 6<br>*Default:* 6 |
| Poll Interval | Specify how often BFD polls all data plane tunnels on a vEdge router to collect packet latency, loss, and other statistics used by application-aware routing.<br>*Range:* 1 through 4,294,967,296 ($2^{32} - 1$) milliseconds<br>*Default:* 600,000 milliseconds (10 minutes) |

To save the feature template, click Save.

*CLI equivalent:*

```
bfd app-route
  multiplier number
  poll-interval milliseconds
```

## Configure BFD on Transport Tunnels

To configure the BFD timers used on transport tunnels, click the Color tab, click Add New Color, and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Color | From the drop-down, choose the color of the transport tunnel for data traffic moving between vEdge routers. The color identifies a specific WAN transport provider.<br>*Values:* 3g, biz-internet, blue, bronze, custom1, custom2, custom3, default, gold, green, lte, metro-ethernet, mpls, private1 through private6, public-internet, red, silver<br>*Default:* default |
| Hello Interval | Specify how often BFD sends Hello packets on the transport tunnel. BFD uses these packets to detect the liveness of the tunnel connection and to detect faults on the tunnel.<br>*Range:* 100 through 60000 milliseconds<br>*Default:* 1000 milliseconds (1 second) |
| Multiplier | Specify how many Hello packet intervals BFD waits before declaring that a tunnel has failed. BFD declares that the tunnel has failed when, during all these intervals, BFD has received no Hello packets on the tunnel. This interval is a multiplier of the Hello packet interval time.<br>*Range:* 1 through 60<br>*Default:* 7 (for hardware vEdge routers), 20 (for vEdge Cloud software routers) |
| Path MTU Discovery | Click On to enable path MTU discovery for the transport tunnel, or Off to disable. When PMTU discovery is enabled, the path MTU for the tunnel connection is checked periodically, about once per minute, and it is updated dynamically. When PMTU discovery is disabled, the expected tunnel MTU is 1472 bytes, but the effective tunnel MTU is 1468 bytes.<br>*Default:* Enabled |

| | |
|---|---|
| Add | Click Add to save the data traffic transport tunnel color. |

To add another color, click Add New Color.

A table lists the transport tunnel colors.

To edit a color, click the Pencil icon. The Update Color popup is displayed. After you make the desired changes, click Save Changes.

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

To save the feature template, click Save.

*CLI equivalent:*

```
bfd color color
  hello-interval milliseconds
  multiplier number
  pmtu-discovery
```

## Release Information

Introduced in vManage NMS in Release 15.2.

## BGP

Use the BGP template for all vEdge Cloud and vEdge router devices.

To configure the BGP routing protocol using vManage templates:

1. Create a BGP feature template to configure BGP parameters, as described in this article. BGP can be used for service-side routing, to provide reachability to networks at the local site, and it can be used for transport-side routing, to enable communication between the vEdge router and other Viptela devices when the router is not directly connected to the WAN cloud. Create separate BGP templates for the two BGP routing types.
2. Create a VPN feature template to configure VPN parameters for either service-side BGP routing (in any VPN other than VPN 0 or VPN 512) or transport-side BGP routing (in VPN 0). See the VPN help topic.

## Navigate to the Template Screen and Name the Template

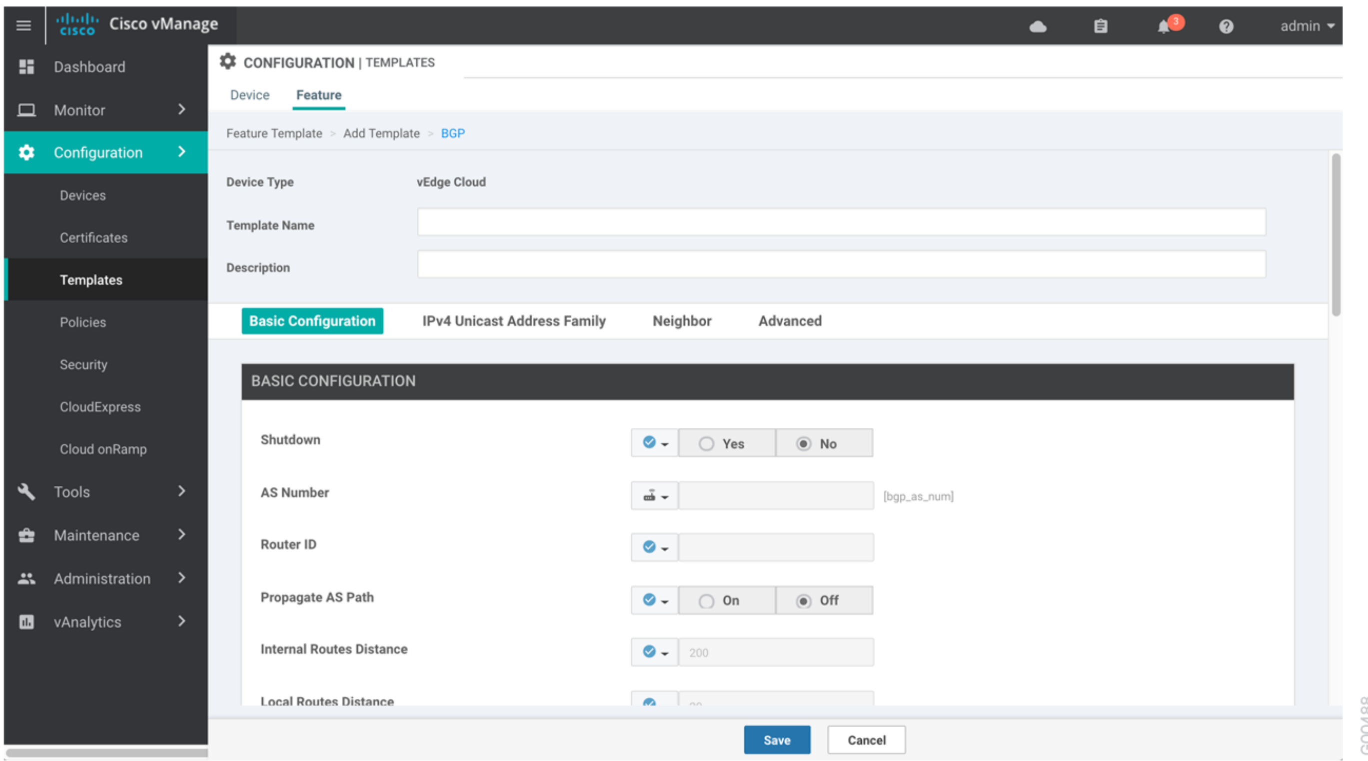
1. In vManage NMS, select the Configuration ► Templates screen.
2. In the Device tab, click Create Template.
3. From the Create Template drop-down, select From Feature Template.
4. From the Device Model drop-down, select the type of device for which you are creating the template.
5. To create a template for VPN 0 or VPN 512:
    a. Click the Transport & Management VPN tab located directly beneath the Description field, or scroll to the Transport & Management VPN section.
    b. Under Additional VPN 0 Templates, located to the right of the screen, click BGP.
    c. From the BGP drop-down, click Create Template. The BGP template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining BGP parameters.
6. To create a template for VPNs 1 through 511, and 513 through 65530:

a. Click the Service VPN tab located directly beneath the Description field, or scroll to the Service VPN section.

b. Click the Service VPN drop-down.

c. Under Additional VPN Templates, located to the right of the screen, click BGP.

d. From the BGP drop-down, click Create Template. The BGP template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining BGP 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 and select one of the following:

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

## Configure Basic BGP

The following parameters are required (unless otherwise indicated) to configure BGP on a vEdge router:

To configure BGP, select the Basic Configuration tab and configure the following parameters. Parameters marked with an asterisk are required to configure BGP.

| Parameter Name | Description |
|---|---|
| Shutdown* | Ensure that No is selected, to enable BGP. |
| AS number* | Enter the local AS number. |
| Router ID | Enter the BGP router ID, in decimal four-part dotten notation. |
| Propagate AS Path | Click On to carry BGP AS path information into OMP. |
| Internal Routes Distance | Enter a value to apply as the BGP route administrative distance for routes coming from one AS into another.<br>*Range:* 0 through 255<br>*Default:* 0 |
| Local Routes Distance | Specify the BGP route administrative distance for routes within the local AS. By default, a route received locally from BGP is preferred over a route received from OMP.<br>*Range:* 0 through 255<br>*Default:* 0 |
| External Routes Distance | Specify the BGP route administrative distance for routes learned from other sites in the overlay network.<br>*Range:* 0 through 255<br>*Default:* 0 |

For service-side BGP, you might want to configure OMP to advertise to the vSmart controller any BGP routes that the vEdge router learns. By default, a vEdge router advertises to OMP both the connected routes on the vEdge router and the static routes that are configured on the vEdge router, but it does not advertise BGP external routes learned by the vEdge router. You configure this route advertisement in the OMP template for vEdge routers or vEdge software. See the OMP help topic.

For transport-side BGP, you must also configure a physical interface and a loopback interface in VPN 0. In addition, you should create a policy for BGP to advertise the loopback interface address to its neighbors, and apply the policy in the BGP instance or to a specific neighbor. See the **Configuring Unicast Overlay Routing** article for your software release.

To save the feature template, click Save.

*CLI equivalent:*

```
vpn vpn-id
  router
    bgp local-as-number
      distance
        external number
        internal number
        local number
      propagate-aspath
      router-id ip-address
      [no] shutdown
```

## Configure the IPv4 Unicast Address Family

To configure global BGP address family information, select the IPv4 Unicast Address Family tab and configure the following parameters:

Tab

Parameter Name

Description

Maximum Paths

Specify the maximum number of parallel IBGP paths that can be installed into a route table to enable IBGP multipath load sharing.

*Range:* 0 to 32

Address Family

Enter the BGP IPv4 unicast address family. Currently, only IPv4 is supported.

**Redistribute**

Click the Redistribute tab, and then click Add New Redistribute.

Protocol

Select the protocols from which to redistribute routes into BGP, for all BGP sessions. Options are Connected, NAT, OMP, OSPF, and Static. At a minimum, select the following:

- For service-side BGP routing, select OMP. By default, OMP routes are not redistributed into BGP.
- For transport-side BGP routing, select Connected, and then under Route Policy, specify a route policy that has BGP advertise the loopback interface address to its neighbors.

Route Policy

Enter the name of the route policy to apply to redistributed routes.

Click Add to save the redistribution information.

**Network**

Click the Network tab, and then click Add New Network.

Network Prefix

Enter a network prefix, in the format of *prefix/length* , to be advertised by BGP.

Click Add to save the network prefix.

**Aggregate Address**

Click the Aggregate Address tab, and then click Add New Aggregate Address.

Aggregate Prefix

Enter the prefix of the addresses to aggregate for all BGP sessions, in the format *prefix/length.*

AS Set Path

Click On to generate set path information for the aggregated prefixes.

Summary Only

Click On to to filter out more specific routes from BGP updates.

Click Add to save the aggregate address.

To save the feature template, click Save.

*CLI equivalent:*

```
vpn vpn-id
  router
    bgp local-as-number
      address-family ipv4-unicast
        aggregate-address prefix/length [as-set] [summary-only]
        maximum-paths paths number
        network prefix/length
        redistribute (connected | nat | omp | ospf | static)
```

## Configure Neighbors

To configure a neighbor, select the Neighbor tab and click Add New Neighbor and configure the following parameters. For BGP to function, you must configure at least one neighbor.

| Parameter Name | Description |
|---|---|
| Address | Specify the IP address of the BGP neighbor. |
| Description | Enter a description of the BGP neighbor. |
| Remote AS | Enter the AS number of the remote BGP peer. |

| | |
|---|---|
| Address Family | Click On and select the address family. Currently, the Viptela software supports only the BGP IPv4 unicast address family. Enter the address family information:<br>• Address Family—Select the address family. Currently, the Viptela software supports only the BGP IPv4 unicast address family.<br>• Maximum Number of Prefixes—Specify the maximum number of prefixes that can be received from the neighbor.<br>*Range:* 1 through 4294967295<br>*Default:* 0<br>If you specify a maximum number of prefixes, you can also configure:<br>– Threshold—Threshold at which to generate a warning message or restart the BGP connection. The threshold is a percentage of the maximum number of prefixes.<br>– Restart Interval—How long to wait to restart the BGP connection.<br>*Range:* 1 through 65535 minutes<br>– Warning Only—Click On to only display a warning message, without restarting the BGP connection.<br>You can specify either a restart interval or a warning only.<br>• Route Policy In—Click On and specify the name of a route policy to apply to prefixes received from the neighbor.<br>• Route Policy Out—Click On and specify the name of a route policy to apply to prefixes sent to the neighbor. |
| Shutdown | Click On to enable the connection to the BGP neighbor. |

To configure advanced parameters for the neighbor, click the Neighbor tab, and then click Advanced Options:

| Parameter Name | Description |
|---|---|
| Next-Hop Self | Click On to configure the router to be the next hop for routes advertised to the BGP neighbor. |
| Send Community | Click On to send the local router's BGP community attribute to the BGP neighbor. |
| Send Extended Community | Click On to send the local router's BGP extended community attribute to the BGP neighbor. |
| Negotiate Capability | Click On to allow the BGP session to learn about the BGP extensions that are supported by the neighbor. |
| Source Interface Address | Enter the IP address of a specific interface of the neighbor that BGP is to use for the TCP connection to the neighbor. |
| Source Interface Name | Enter the name of a specific interface of the neighbor that BGP is to use for the TCP connection to the neighbor, in the format **ge** *port* / *slot* . |
| EBGP Multihop | Set the time to live (TTL) for BGP connections to external peers.<br>*Range:* 0 to 255<br>*Default:* 1 |
| Password | Enter a password to use to generate an MD5 message digest. Configuring the password enables MD5 authentication on the TCP connection with the BGP peer. The password is case-sensitive and can be up to 25 characters long. It can contain any alphanumeric characters, including spaces. The first character cannot be a number. |
| Keepalive Time | Specify the frequency at which keepalive messages are advertised to a BGP peer. These messages indicate to the peer that the local router is still active and should be considered to be available.<br>Specify the keepalive time for the neighbor, to override the global keepalive time.<br>*Range:* 0 through 65535 seconds<br>*Default:* 60 seconds (one-third the hold-time value) |

| | |
|---|---|
| Hold Time | Specify the interval after not receiving a keepalive message that the local BGP session considers its peer to be unavailable. The local router then terminates the BGP session to that peer.<br>Specify the hold time for the neighbor, to override the global hold time.<br>*Range:* 0 through 65535 seconds<br>*Default:* 180 seconds (three times the keepalive timer) |
| Connection Retry Time | Specify the number of seconds between retries to establish a connection to a configured BGP neighbor peer that has gone down.<br>*Range:* 0 through 65535 seconds<br>*Default:* 30 seconds |
| Advertisement Interval | For the BGP neighbor, set the minimum route advertisement interval (MRAI) between when BGP routing update packets are sent to that neighbor.<br>*Range:* 0 through 600 seconds<br>*Default:* 5 seconds for IBGP route advertisements; 30 seconds for EBGP route advertisements |

To save the feature template, click Save.

*CLI equivalent:*

```
vpn vpn-id
  router
    bgp local-as-number
      neighbor ip-address
        address-family ipv4-unicast
          maximum-prefixes number [threshold] [restart minutes | warning-only]
          route-policy policy-name (in | out)
        capability-negotiate
        description string
        ebgp-multihop ttl
        next-hop-self
        password md5-digest-string
        remote-as remote-as-number
        send-community
        send-ext-community
        [no] shutdown
        timers
          advertisement-interval number
          connect-retry seconds
          holdtime seconds
          keepalive seconds
        update-source ip-address
```

## Configure Advanced Parameters

To configure advanced parameters for BGP, click the Advanced tab and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Hold Time | Specify the interval after not receiving a keepalive message that the local BGP session considers its peer to be unavailable. The local router then terminates the BGP session to that peer.<br>This hold time is the global hold time.<br>*Range:* 0 through 65535 seconds<br>*Default:* 180 seconds (three times the keepalive timer) |
| Keepalive | Specify the frequency at which keepalive messages are advertised to a BGP peer. These messages indicate to the peer that the local router is still active and should be considered to be available.<br>This keepalive time is the global keepalive time.<br>*Range:* 0 through 65535 seconds<br>*Default:* 60 seconds (one-third the hold-time value) |

| | |
|---|---|
| Compare MED | Click On to compare the router IDs among BGP paths to determine the active path. |
| Deterministic MED | Click On to compare MEDs from all routes received from the same AS regardless of when the route was received. |
| Missing MED as Worst | Click On to consider a path as the worst path if the path is missing a MED attribute. |
| Compare Router ID | Click On to always compare MEDs regardless of whether the peer ASs of the compared routes are the same. |
| Multipath Relax | Click On to have the BGP best-path process selct from routes in different in ASs. By default, when you are using BGP multipath, the BGP best path process selects from routes in the same AS to load-balance across multiple paths. |

To save the feature template, click Save.

*CLI equivalent:*

```
vpn vpn-id
  router
    bgp local-as-number
      best-path
        as-path multipath-relax
        compare-router-id
        med (always-compare | deterministic | missing-as-worst)
      timers
        holdtime seconds
        keepalive seconds
```

## Release Information

Introduced in vManage NMS in Release 15.2.
In Release 17.1, add Propagate AS Path field.

## Bridge

Use the Bridge template for all vEdge Cloud and vEdge router devices.

To have a vEdge router act as a transparent bridge, configure bridging domains on the router. A router can have up to 16 bridging domains.

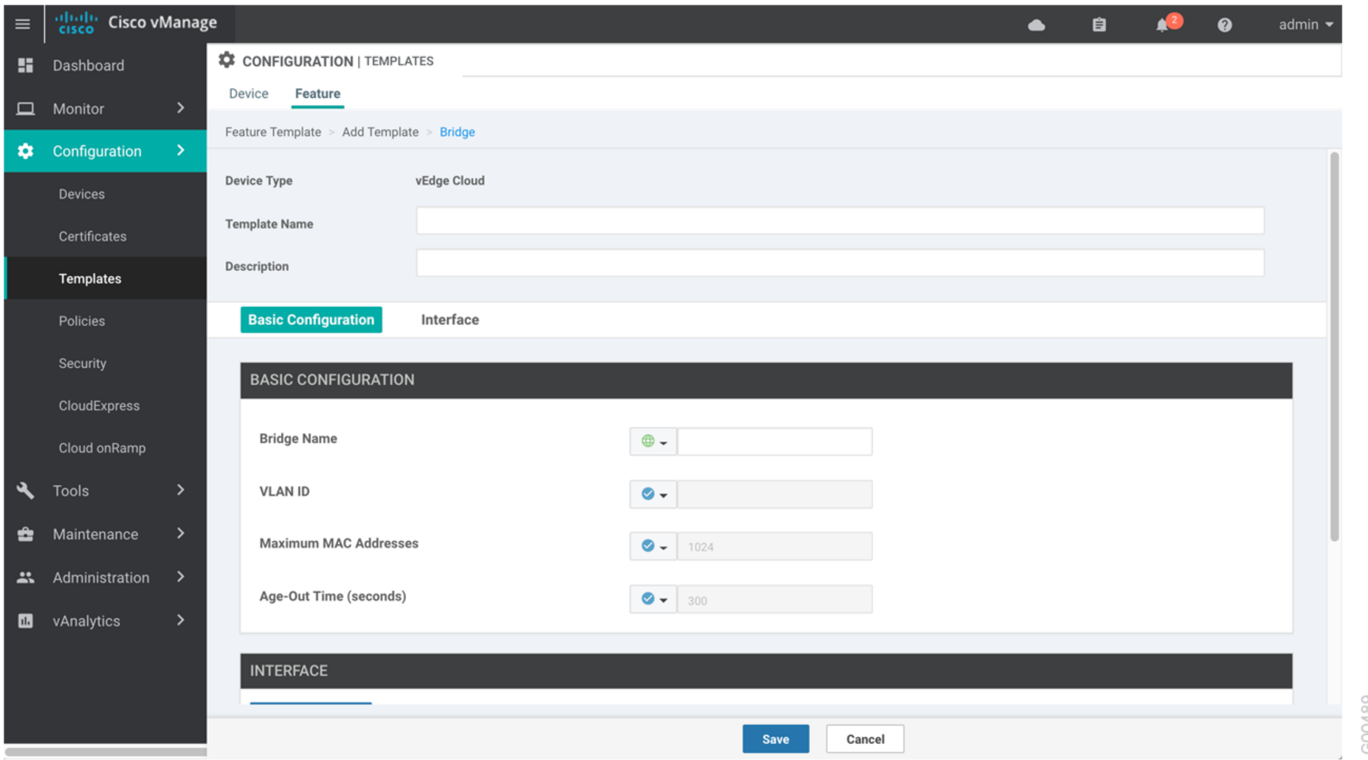
To configure the bridging domains using vManage templates:

1. Create a Bridge feature template, as described in this article.
2. Create a VPN Interface Bridge feature template to enable integrated routing and bridging (IRB). See the VPN Interface Bridge help topic.

## 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. Click the Additional Templates tab located directly beneath the Description field, or scroll to the Additional Templates section.

6. Click the plus sign (+) next to Bridge.




7. From the Bridge drop-down, click Create Template. The Bridge template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining Bridge 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:

| 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 Viptela device to a device template** .<br><br>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 .<br><br>To change the default key, type a new string and move the cursor out of the Enter Key box.<br><br>Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID. |

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

## Configure Bridging Domains

To configure bridging domains, select the Basic Configuration tab and configure the following parameters. For bridging to work, you must also associate interfaces with the bridging domain. Parameters marked with an asterisk are required to configure bridging.

| Parameter Name | Description |
|---|---|
| Bridge Name* | Enter a text description of the bridging domain. It can be up to 32 characters. |
| VLAN ID* | Enter the VLAN identifier to associate with the bridging domain.<br>*Range:* 0 through 4095 |
| Maximum MAC Addresses | Specify the maximum number of MAC addresses that the bridging domain can learn.<br>*Range:* 0 through 4096<br>*Default:* 1024 |
| Age-Out Time | Specify how long to store an entry in the MAC table before it ages out.<br>*Range:* 10 through 4096 seconds<br>*Default:* 300 seconds (5 minutes) |

To save the feature template, click Save.

*CLI equivalent:*

```
bridge bridge-id
  age-time seconds
  max-macs number
  name text
  vlan number
```

## Associate Interfaces with the Bridge Domain

To associate an interface with the bridge domain, click the Interface tab and click Add New Interface:

| Parameter Name | Description |
|---|---|
| Interface Name* | Enter the name of the interface to associate with the bridging domain, in the format **ge** *slot* / *port* . |
| Description | Enter a text description of the interface. |
| Native VLAN Support | Click Enabled to configure the interface to carry untagged traffic. By default, native VLAN is disabled. |
| Shutdown | Click No to enable the interface. By default, an interface in a bridge domain is disabled. |
| Static MAC Address | Click Add Static MAC Address, and in the MAC Static Address field that appears, enter a static MAC address entry for the interface in the bridge domain. Click Add MAC Address to add another static MAC address entry for the interface. Click Save to save the MAC address or addresses. |

To save the feature template, click Save.

*CLI equivalent:*

```
bridge bridge-id
  interface interface-name
    description "text description"
    native-vlan
    [no] shutdown
    static-mac-address mac-address
```

## Release Information

Introduced in vManage NMS in Release 15.3.

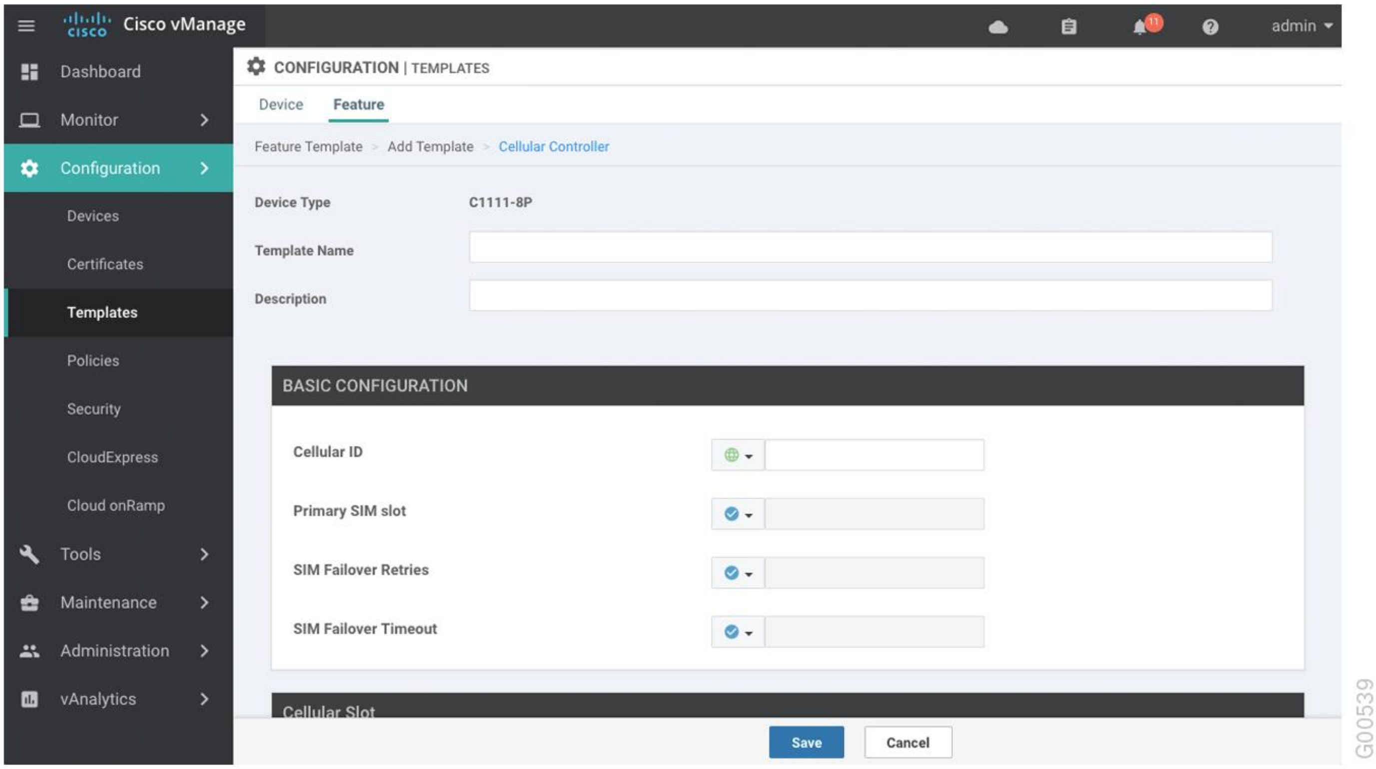
## Cellular Controller

Use the Cellular Controller template for Cisco IOS XE routers running the SD-WAN software.

To use vManage templates to configure a cellular controller for a 4G network interface module (NIM) installed in a router, create a Cellular Controller template to configure cellular controller properties. This template is mandatory if the 4G NIM module is installed in the router.

## 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. Select the Cellular tab.
6. To create a cellular controller template, in the Cellular Controller drop-down click Create Template. The Cellular Controller template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining cellular controller 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 and select one of the following:

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

## Configure a Cellular Controller

To configure a cellular controller, configure the following parameters. Parameters marked with an asterisk are required to configure an interface.

| Parameter Name | Description |
|---|---|
| Cellular ID* | Enter the interface slot and port number in which the cellular NIM card is installed. Currently, it can be 0/1/0 or 0/2/0. |
| Primary SIM Slot* | Enter the number of the primary SIM slot. It can be 0 or 1. The other slot is automatically set to be the secondary. If there is a single SIM slot, this parameter is not applicable. |
| SIM Failover Retries | Specify the maximum number of times to retry connecting to the secondary SIM when service on the primary SIM becomes unavailable. If there is a single SIM slot, this parameter is not applicable.<br><br>*Range:* 0 through 65535<br>*Default:* 10 |
| SIM Failover Timeout | Specify how long to wait before switching from the primary SIM to the secondary SIM if service on the primary SIM becomes unavailable. If there is a single SIM slot, this parameter is not applicable.<br><br>*Range:* 3 to 7 minutes<br>*Default:* 3 minutes |

To save the feature template, click Save.

## Release Information

Introduced in vManage NMS Release 18.1.1.

## Cellular Profile

Use the Cellular Profile feature template to configure the profiles used by cellular modems on vEdge routers and Cisco IOS XE routers running the SD-WAN software.

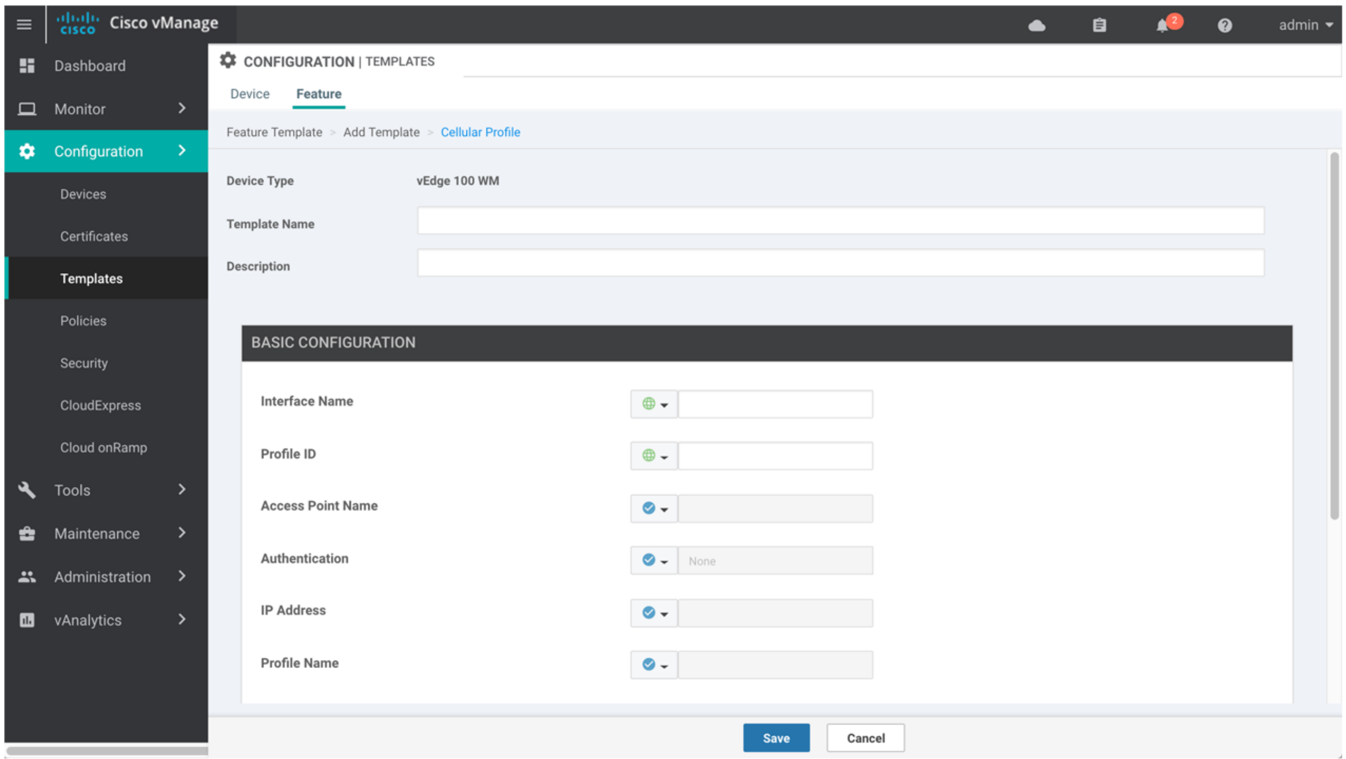
To configure a cellular profile using vManage templates:

1. Create a Cellular Profile template to configure the profiles used by the cellular modem, as described in this article.
2. Create a VPN-Interface-Cellular feature template to configure cellular module parameters. See the VPN-Interface-Cellular help topic.
3. Create a VPN feature template to configure VPN parameters. See the VPN help topic.

## 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. Click the Additional Templates tab located directly beneath the Description field, or scroll to the Additional Templates section.

6. Click the plus sign (+) next to Cellular-Profile.




7. From the Cellular-Profile drop-down, click Create Template. The Cellular-Profile template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining Cellular-Profile 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:

| 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 Viptela device to a device template** .<br><br>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 .<br><br>To change the default key, type a new string and move the cursor out of the Enter Key box.<br><br>Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID. |

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

## Configure a Cellular Profile

To configure a cellular profile, in the Basic Configuration tab, configure the following parameters. Parameters marked with an asterisk are required to configure the cellular profile.

| Parameter Name | Description |
|---|---|
| Interface name* | Enter the name of the cellular interface, which must be cellular0. |
| Profile ID* | Enter the identification number of the profile to use on the router. You use this profile identification number when you configure for the cellular interface in the VPN-Interface-Cellular template.<br>*Range:* 1 through 15 |
| Access Point Name | Enter the name of the gateway between the service provider network and the public Internet. It can be up to 32 characters long. |
| Authentication | Select the authentication method used for the connection to the cellular network. It can be CHAP, None, PAP, or PAP/CHAP. |
| IP Address (on vEdge routers) | Enter the static IP address assigned to the cellular interface. This field is used when the service provider requires that a static IP address be preconfigured before attaching to the network. |
| Profile Name (on vEdge routers) | Enter a name to identify the cellular profile. It can be up to 14 characters long. |
| Packet Data Network Type | Select the packet data network (PDN) type of the cellular network. It can be IPv4, IPv6, or IPv46. |
| Profile Username | Enter the username to use when making cellular connections for web services. It can be 1 to 32 characters. It can contain any alphanumeric characters, including spaces. |
| Profile Password | Enter the user password to use when making cellular connections for web services. The password is case-sensitive and can be clear text, or an AES encrypted key. |
| Primary DNS Address (on vEdge routers) | Enter the IP addresses of the primary DNS servers in the service provider network, in decimal four-part dotted notation. |
| Overwrite (on IOS XE routers) | Click On to overwrite the profile on the cellular modem. |

To save the feature template, click Save.

*CLI equivalent:*

```
cellular cellular0
  profile number
    apn name
    auth auth-method
    ip-addr ip-address
    name profile-name
    pdn-type type
    primary-dns ip-address
    secondary-dns ip-address
    user-name user-name
    user-pass password
```

## Release Information

Introduced in vManage NMS in Release 16.1.

## DHCP Server

Use the DHCP-Server template for all vEdge Cloud and vEdge router devices.

You enable DHCP server functionality on a vEdge router interface so it can assign IP addresses to hosts in the service-side network.

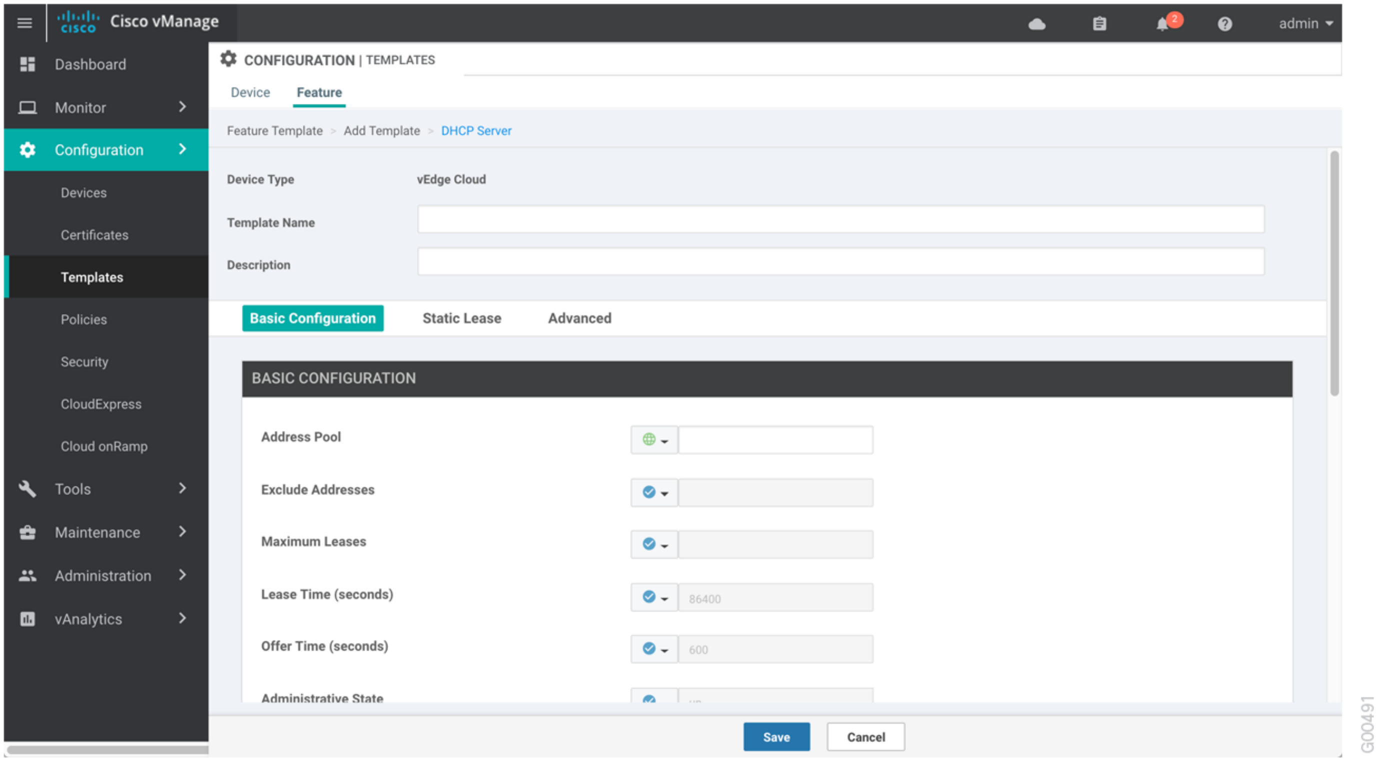
To configure a vEdge router to act as a DHCP server using vManage templates:

1. Create a DHCP-Server feature template to configure DHCP server parameters, as described in this article.
2. Create one or more interface feature templates, as described in the VPN-Interface-Ethernet and the **VPN-Interface-PPP-Ethernet** help topics.
3. Create a VPN feature template to configure VPN parameters. See the VPN help topic.

To configure a vEdge router interface to be a DHCP helper so that it forwards broadcast DHCP requests that it receives from DHCP servers, in the DHCP Helper field of the applicable interfaces template, enter the addresses of the DHCP servers.

## 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. Click the Service VPN tab located directly beneath the Description field, or scroll to the Service VPN section.
6. Click the Service VPN drop-down.
7. Under Additional VPN Templates, located to the right of the screen, click VPN Interface.
8. From the Sub-Templates drop-down, select DHCP Server.
9. From the DHCP Server drop-down, click Create Template. The DHCP-Server template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining DHCP Server parameters.




10. 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.

11. 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:

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

## Minimum DHCP Server Configuration

To configure DHCP server functionality, select the Basic Configuration tab and configure the following parameters. Parameters marked with an asterisk as required to configure DHCP servers.

| Parameter Name | Description |
|---|---|
| Address Pool* | Enter the IPv4 prefix range, in the format *prefix/length* , for the pool of addresses in the service-side network for which the vEdge router interface acts as DHCP server. |
| Exclude Addresses | Enter one or more IP addresses to exclude from the DHCP address pool. To specify multiple individual addresses, list them separated by a comma (for example, 1.1.1.1, 2.2.2.2, 3.3.3.3). To specify a range of addresses, separate them with a hyphen (for example, 1.1.1.1-1.1.1.10). |
| Maximum Leases | Specify the number of IP addresses that can be assigned on this interface.<br>*Range:* 0 through 4294967295 |
| Lease Time | Specify how long a DHCP-assigned IP address is valid.<br>*Range:* 0 through 4294967295 seconds |
| Offer Time | Specify how long the IP address offered to a DHCP client is reserved for that client. By default, an offered IP address is reserved indefinitely, until the DHCP server runs out of addresses. At that point, the address is offered to another client.<br>*Range:* 0 through 4294967295 seconds<br>*Default:* 600 seconds |
| Administrative State | Select Up to enable or Down to disable the DHCP functionality on the interface. By default, DHCP server functionality is disabled on a vEdge router interface. |

To save the feature template, click Save.

*CLI equivalent:*

```
vpn vpn-id
  interface geslot/port
    dhcp-server
      address-pool prefix/length
      admin-state (down | up)
      exclude ip-address
      lease-time seconds
      max-leases number
      offer-time minutes
```

## Configure Static Leases

To configure a static lease to assign a static IP address to a client device on the service-side network, click the Static Lease tab. Then click Add New Static Lease and configure the following parameters:

| Parameter Name | Description |
|---|---|
| MAC Address | Enter the MAC address of the client to which the static IP address is being assigned. |
| IP Address | Enter the static IP address to assign to the client. |
| Hostname | Enter the hostname of the client device. |

To edit a static lease, click the pencil icon to the right of the entry.

To remove a static lease, click the trash icon to the right of the entry.

To save the feature template, click Save.

*CLI equivalent:*

```
vpn vpn-id
  interface geslot/port
    dhcp-server
      static-lease mac-address ip ip-address host-name hostname
```

## Configure Advanced Options

To configure a advanced DHCP server options, click the Advanced tab and then configure the following parameters:

| Parameter Name | Description |
|---|---|
| Interface MTU | Specify the maximum MTU size of packets on the interface.<br>*Range:* 68 to 65535 bytes |
| Domain Name | Specify the domain name that the DHCP client uses to resolve hostnames. |
| Default Gateway | Enter the IP address of a default gateway in the service-side network. |
| DNS Servers | Enter one or more IP address for a DNS server in the service-side network. Separate multiple entries with a comma. You can specify up to eight addresses. |
| TFTP Servers | Enter the IP address of a TFTP server in the service-side network. You can specify one or two addresses. If two, separate them with a comma. |

To save the feature template, click Save.

*CLI equivalent:*

```
vpn vpn-id
  interface geslot/port
    dhcp-server
      options
        default-gateway ip-address
        dns-servers ip-address
        domain-name domain-name
        interface-mtu mtu
        tftp-servers ip-address
```

## Release Information

Introduced in vManage NMS in Release 15.2.

## GPS

Use the GPS template for all Cisco cellular routers running Viptela software.

For Cisco devices running Viptela 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 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 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 one of the following:

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

## 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.

| Parameter Name | Description |
|---|---|
| GPS | Click On to enable the GPS feature on the router. |
| GPS Mode | Select the GPS mode:<br><br>• 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.<br><br>• 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 vManage NMS Release 18.1.1.

# IGMP

Use the IGMP temlate for all vEdge Cloud and vEdge router devices.

Internet Group Management Protocol (IGMP) allows vEdge routers to join multicast groups within a particular VPN.

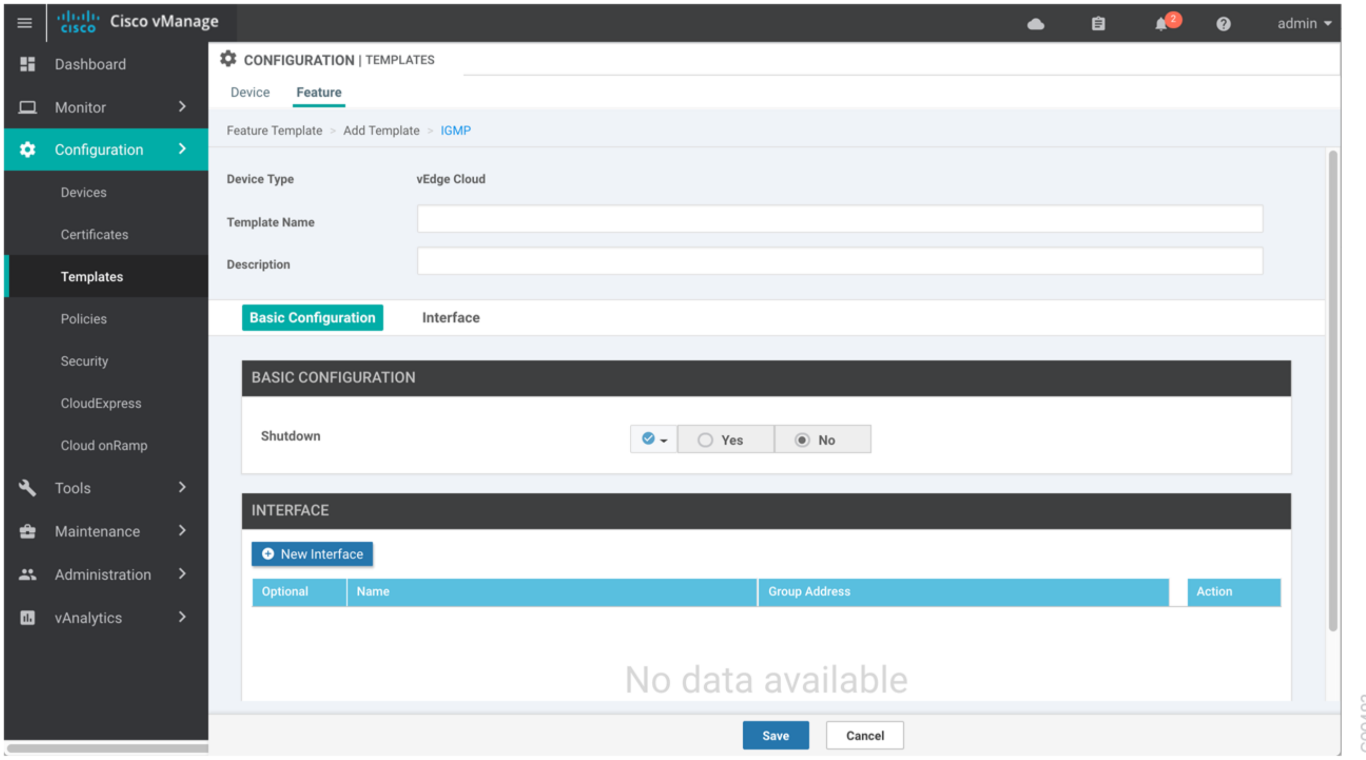
To configure IGMP using vManage templates:

1. Create an IGMP feature template to configure IGMP parameters, as described in this article.
2. Create the interface in the VPN to use for IGMP. See the VPN-Interface-Ethernet help topic.
3. Create a VPN feature template to configure VPN parameters. See the VPN help topic.

## 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. Click the Service VPN tab located directly beneath the Description field, or scroll to the Service VPN section.

6. Click the Service VPN drop-down.




7. Under Additional VPN Templates, located to the right of the screen, click IGMP.

8. From the IGMP drop-down, click Create Template. The IGMP template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining IGMP parameters.

9. In the Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

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

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

| 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 Viptela device to a device template** .<br><br>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 .<br><br>To change the default key, type a new string and move the cursor out of the Enter Key box.<br><br>Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID. |

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

## Configure IGMP

To configure IGMP, select the Basic Configuration tab to enable IGMP. Then, select the Interface tab and click Add New Interface to configure IGMP interfaces. All parameters listed below are required to configure IGMP.

| Parameter Name | Description |
|---|---|
| Shutdown | nsure that No is selected to enable IGMP. |
| Interface Name | Enter the name of the interface to use for IGMP.<br><br>To add another interface, click the plus sign (+). To delete an interface, click the trash icon to the right of the entry. |
| Join Group Address | Click Add Join Group Address, and enter the address of a multicast group for the interface to join.<br><br>Click Add to add the new interface |

To save the feature template, click Save.

*CLI equivalent:*

```
vpn vpn-id
  router
    igmp
      interface interface-name
        join-group group-address
      [no] shutdown
```

## Release Information

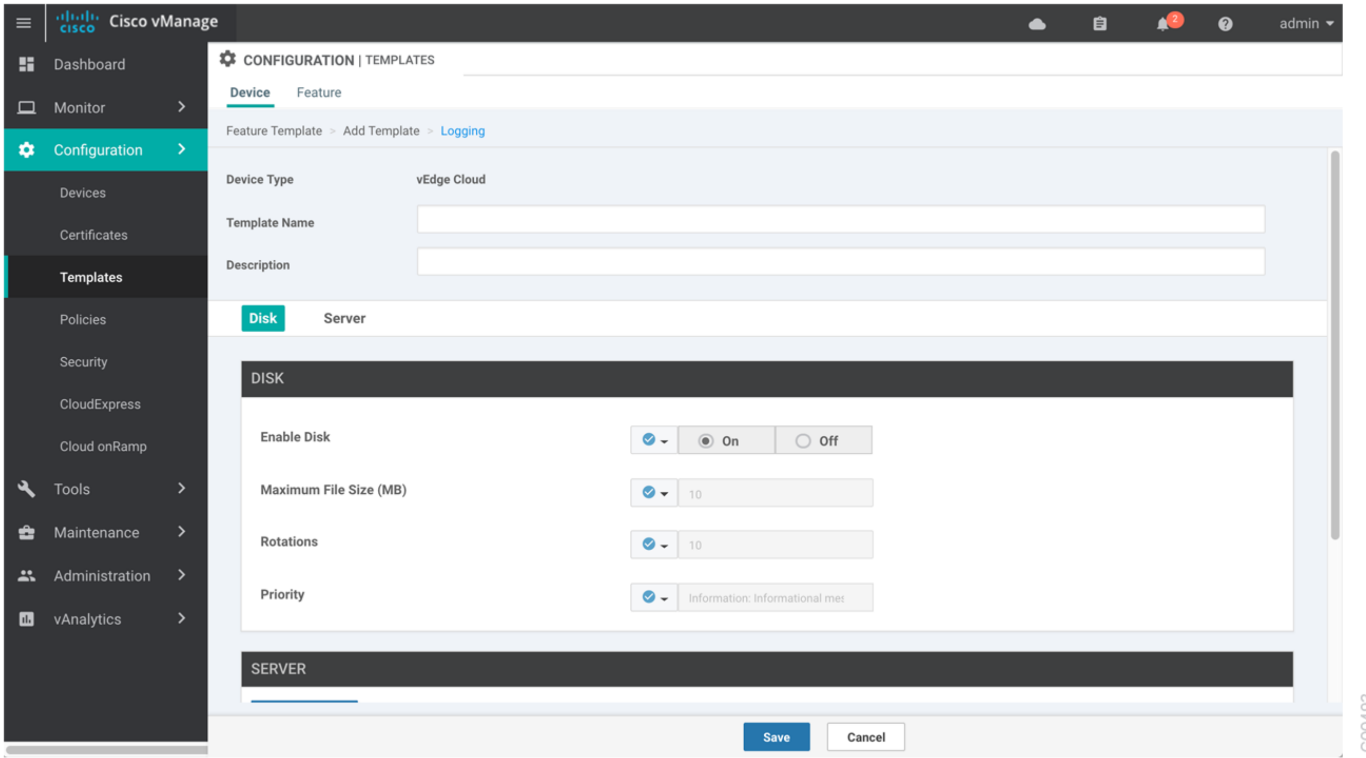
Introduced in vManage NMS in Release 15.2.

## Logging

Use the Logging template for all Viptela devices 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.




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:

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

## Minimum Logging Configuration

The following logging parameters are configured by default on all Viptela devices:

- 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:

| 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. |
| 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.<br>*Range:* 1 through 20 MB<br>*Default:* 10 MB |
| Rotations | Enter the number of syslog files to create before discarding the oldest files.<br>*Range:* 1 through 10<br>*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.<br>The priority level can be one of the following (in order of decreasing severity):<br>• Emergency—System is unusable (corresponds to syslog severity 0).<br>• Alert— Action must be taken immediately (corresponds to syslog severity 1).<br>• Critical—Critical: A serious condition (corresponds to syslog severity 2).<br>• Error—An error condition that does not fully impair system usability (corresponds to syslog severity 3).<br>• Warning—A minor error condition (corresponds to syslog severity 4).<br>• Notice—A normal, but significant condition (corresponds to syslog severity 5).<br>• 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 number
        size 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:

| Parameter Name | Description |
|---|---|
| Hostname/IP Address | Enter the DNS name, hostname, or IP address of the system on which to store syslog messages.<br><br>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.<br>*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. |
| 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:<br>• Emergency—System is unusable (corresponds to syslog severity 0).<br>• Alert— Action must be taken immediately (corresponds to syslog severity 1).<br>• Critical—Critical: A serious condition (corresponds to syslog severity 2).<br>• Error—An error condition that does not fully impair system usability (corresponds to syslog severity 3).<br>• Warning—A minor error condition (corresponds to syslog severity 4).<br>• Notice—A normal, but significant condition (corresponds to syslog severity 5).<br>• Informational—Routine condition (the default) (corresponds to syslog severity 6).<br><br>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 vManage NMS in Release 15.2.

## Multicast

Use the Multicast template for all vEdge Cloud and vEdge router devices.

To configure a vEdge router to be a multicast replicator using vManage templates:

1. Create a mulitcast feature template to configure multicast replicator parameters, as described in this article.
2. Create a PIM feature template to enable PIM on each VPN that participates in a multicast domain. See the PIM help topic.
3. Create a VPN feature template to configure parameters for the VPN that is running PIM. See the VPN help topic.

## Navigate to the Template Screen and Name the Template

1. In vManage NMS, select the Configuration ► Templates screen.

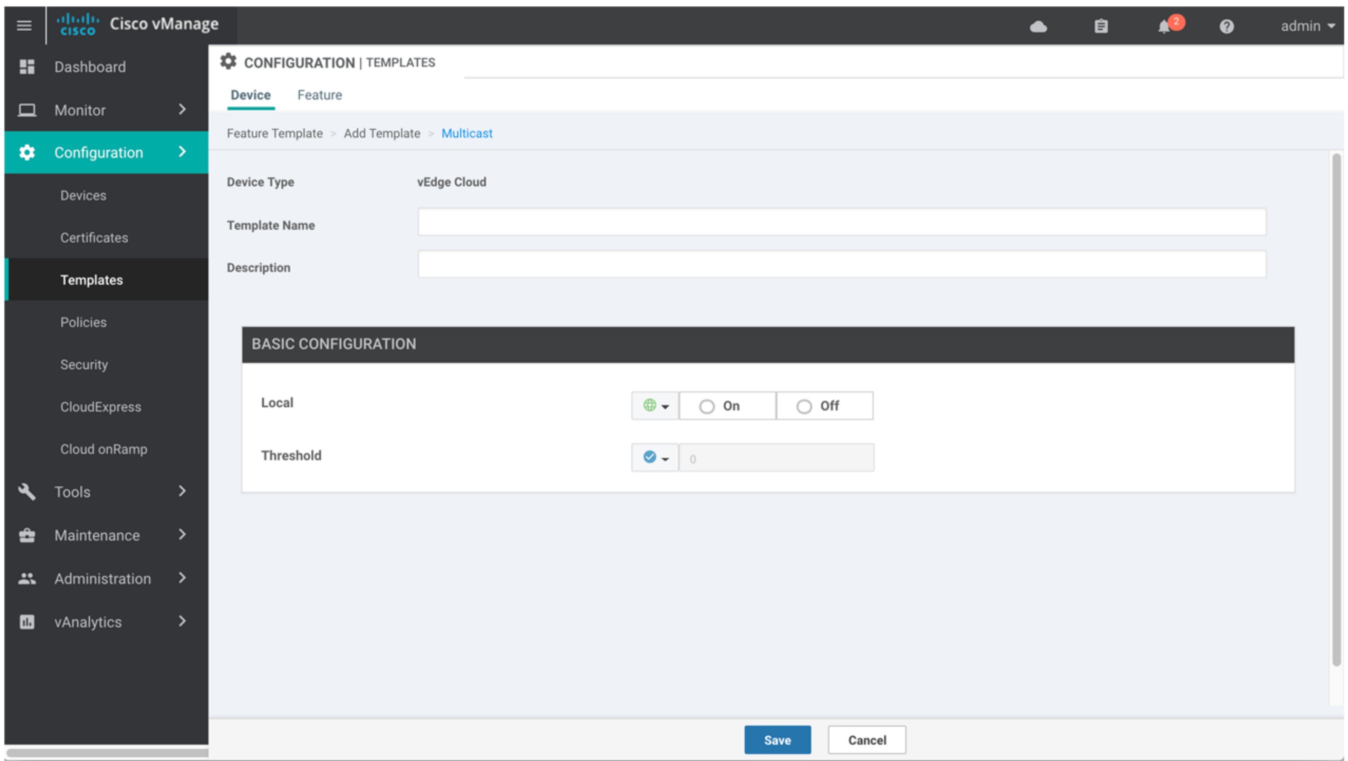
2. In the Device tab, click Create Template.

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. Click the Service VPN tab located directly beneath the Description field, or scroll to the Service VPN section.

6. Click the Service VPN drop-down.




G00494

7. Under Additional VPN Templates, located to the right of the screen, click Multicast.

8. From the Multicast drop-down, click Create Template. The Multicast template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining Multicast parameters.

9. In the Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

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

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

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

## Configure a Multicast Replicator

To configure a vEdge router to be a multicast replicator, in the Basic Configuration tab, configure the following parameters:

| Parameter Name | Description |
|---|---|
| Local | Click On to configure the local router as a multicast replicator. |
| Threshold | Specify the number of joins per group that the router can accept. For each join, the router can accept 256 outgoing tunnel interfaces (OILs).<br>*Range:* 0 through 1000<br>*Default:* 0. A value of 0 means that the router can accept any number of (*,G) and (S,G) joins. |

To save the feature template, click Save.

*CLI equivalent:*

```
vpn vpn-id
  router
    multicast-replicator local [threshold number]
```

## Release Information

Introduced in vManage NMS in Release 15.2.

## NTP

Use the NTP template for all Viptela devices.

Configure network time protocol (NTP) servers on your Viptela devices in order to synchronize time across all devices in the Viptela 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 Viptela device for the time, but no devices are allowed to use the Viptela device as an NTP server.

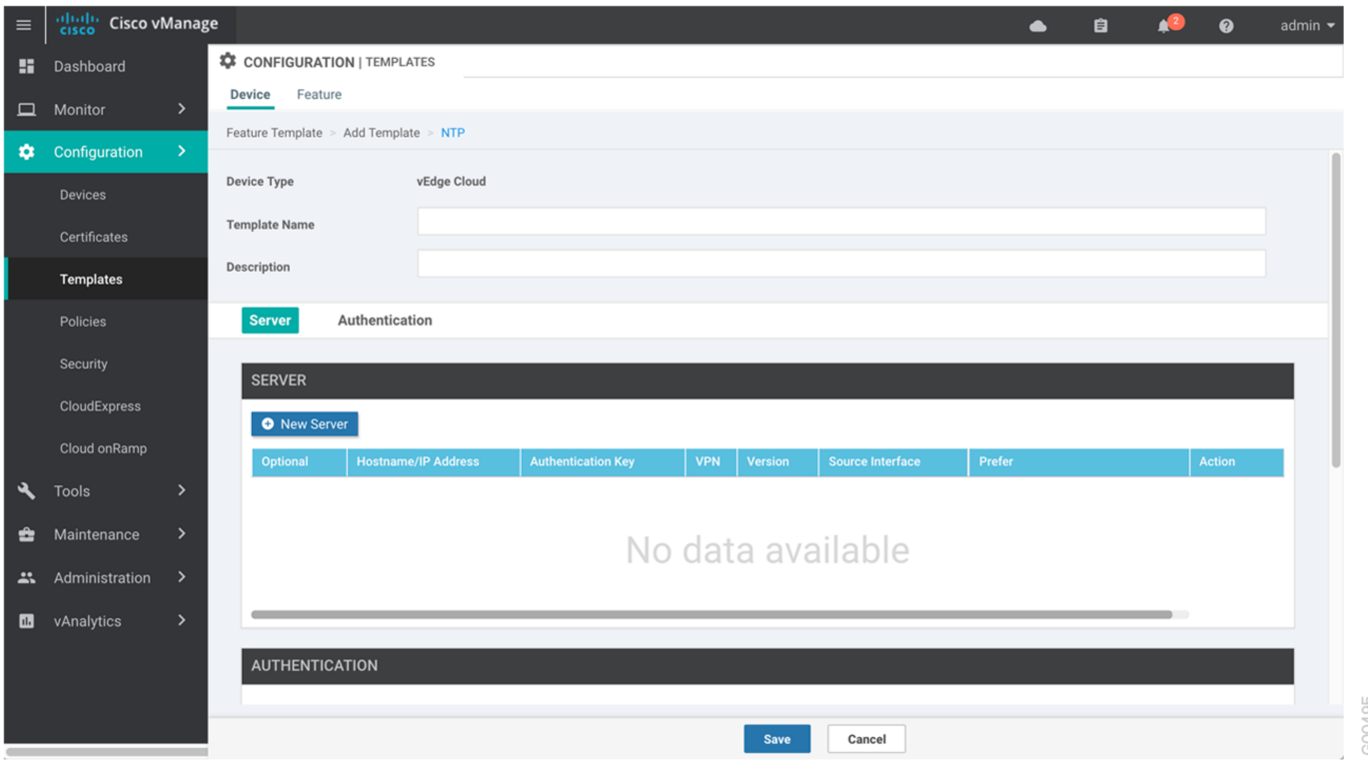
To configure NTP using vManage templates:

1. Create an NTP feature template to configure NTP parameters, as described in this article.

2. Configure the timezone in the System template. See the System help topic.

## 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. 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:

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

## 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.

| 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.<br><br>*Range:* 0 through 65530 |
| Version* | Enter the version number of the NTP protocol software.<br>*Range:* 1 through 4<br>*Default:* 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 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 Viptela 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

To configure authentication keys used to authenticate NTP servers, in the Authentication tab, xlixk 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.

| Parameter Name | Description |
|---|---|
| Authentication Key* | Select the following values:<br>• Authentication Key—Enter an MD5 key ID. It can be a number from 1 through 65535.<br>• 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;

| 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. |

*CLI equivalent:*

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

## Release Information

Introduced in vManage NMS in Release 15.2.

## OMP

Use the OMP template to configure OMP parameters for all vEdge Cloud and vEdge router devices, and for vSmart controllers.

The Viptela Overlay Management Protocol (OMP) establishes and maintains the Viptela control plane.

OMP is enabled by default on all vEdge routers, vManage NMSs, and vSmart controllers, so there is no need to explicitly configure or enable OMP. OMP must be operational for the Viptela overlay network to function. If you disable it, you disable the overlay network.

## Navigate to the Template Screen and Name the Template

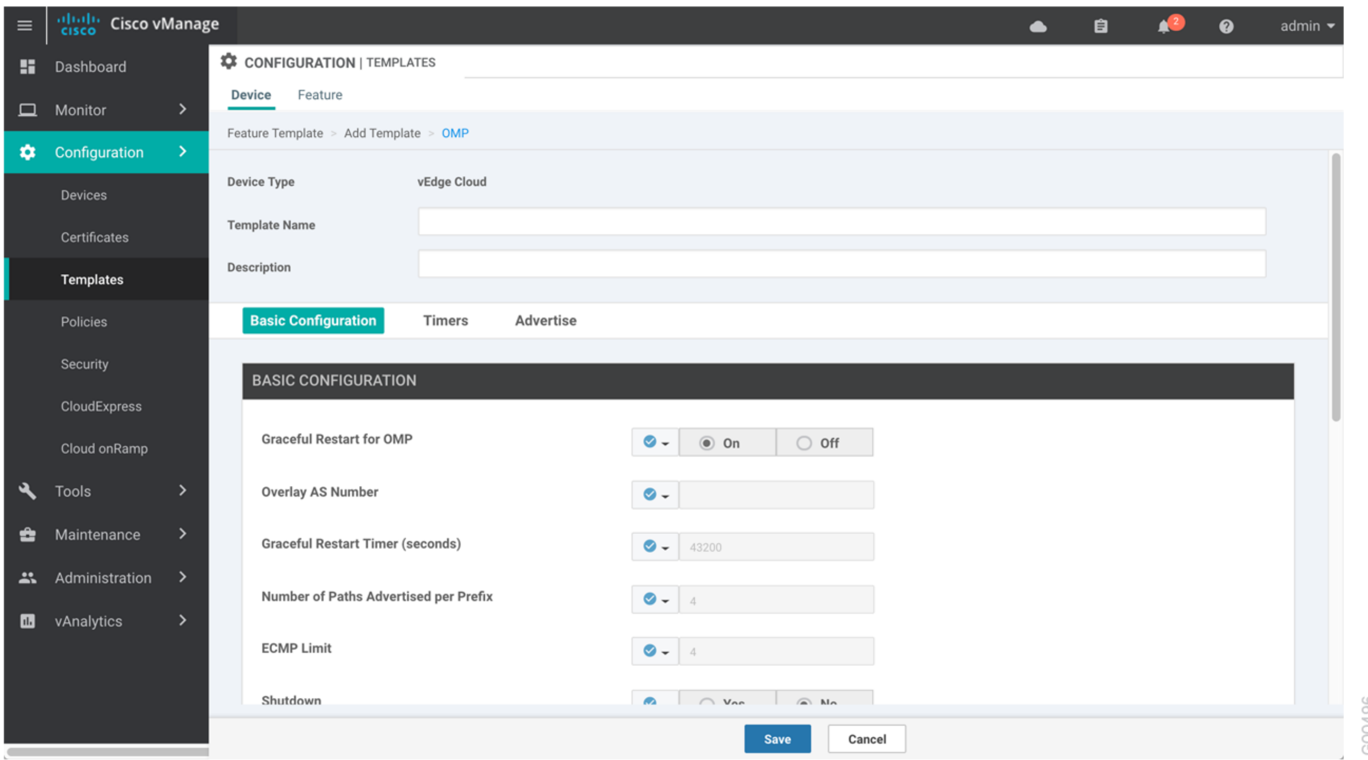
1. In vManage NMS, select the Configuration ► Templates screen.
2. In the Device tab, click Create Template.

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 OMP, select the Factory_Default_OMP_Template and click Create Template. The OMP template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining OMP parameters. You may need to click a tab or the plus sign (+) to display additional fields.

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:

| 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 Viptela device to a device template** .<br><br>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 .<br><br>To change the default key, type a new string and move the cursor out of the Enter Key box.<br><br>Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID. |

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

## Configure Basic OMP Options

To configure basic OMP options, select the Basic Configuration tab and configure the following parameters. All parameters are optional.

| Parameter Name | Description |
|---|---|
| Graceful Restart for OMP | Ensure that Yes is selected to enable graceful restart. By default, graceful restart for OMP is enabled. |
| Overlay AS Number (on vEdge routers only) | Specify a BGP AS number that OMOP advertises to the router's BGP neighbors. |
| Graceful Restart Timer | Specify how often the OMP information cache is flushed and refreshed. A timer value of 0 disables OMP graceful restart.<br>*Range:* 0 through 604800 seconds (168 hours, or 7 days)<br>*Default:* 43200 seconds (12 hours) |
| Number of Paths Advertised per Prefix | Specify the maximum number of equal-cost routes to advertise per prefix. vEdge routers advertise routes to vSmart controllers, and the controllers redistributes the learned routes, advertising each route-TLOC tuple. A vEdge router can have up to four TLOCs, and by default advertises each route-TLOC tuple to the vSmart controller. If a local site has two vEdge routers, a vSmart controller could potentially learn eight route-TLOC tuples for the same route. If the configured limit is lower than the number of route-TLOC tuples, the best route or routes are advertised.<br>*Range:* 1 through 16<br>*Default:* 4 |
| ECMP Limit (on vEdge routers only) | Specify the maximum number of OMP paths received from the vSmart controller that can be installed in the vEdge router's local route table. By default, a vEdge router installs a maximum of four unique OMP paths into its route table.<br>*Range:* 1 through 32<br>*Default:* 4 |
| Send Backup Paths (on vSmart Controllers only) | Click On to have OMP advertise backup routes to vEdge routers. By default, OMP advertises only the best route or routes. If you configure to send backup paths, OMP also advertises the first non-best route in addition to the best route or routes. |
| Shutdown | Ensure that No is selected, to enable to Viptela overlay network. Click Yes to disable OMP and disable the Viptela overlay network. OMP is enabled by default. |
| Discard rejected (on vSmart controllers only) | Click Yes to have OMP discard routes that have been rejected on the basis of policy. By default, rejected routes are not discarded. |

To save the feature template, click Save.

*CLI equivalent:*

```
omp
  discard-rejected (on vSmart controllers only)
  ecmp-limit number (on vEdge routers only)
  graceful-restart
  overlay-as as-number (on vEdge routers only)
  send-backup-paths (on vSmart controllers only)
  send-path-limit number
  [no] shutdown
```

## Configure OMP Timers

To configure OMP timers, select the Timers tab and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Advertisement Interval | Specify the time between OMP Update packets.<br><br>*Range:* 0 through 65535 seconds<br>*Default:* 1 second |
| Hold Time | Specify how long to wait before closing the OMP connection to a peer. If the peer does not receive three consecutive keepalive messages within the hold time, the OMP connection to the peer is closed.<br>*Range:* 0 through 65535 seconds<br>*Default:* 60 seconds |
| EOR Timer | Specify how long to wait after an OMP session has gone down and then come back up to send an end-of-RIB (EOR) marker. After this marker is sent, any routes that were not refreshed after the OMP session came back up are considered to be stale and are deleted from the route table.<br>*Range:* 1 through 3600 seconds (1 hour)<br>*Default:* 300 seconds (5 minutes) |

To save the feature template, click Save.

*CLI equivalent:*

```
omp
  timers
    advertisement-interval seconds
    graceful-restart-timer seconds
    holdtime seconds
```

## Configure OMP Advertisements

To advertise routes learned locally by the vEdge router to OMP, select the Advertise tab and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Advertise (on vEdge routers only) | Click On or Off to enable or disable the vEdge router advertising to OMP the routes that it learns locally:<br><br>• BGP—Click On to advertise BGP routes to OMP. By default, BGP routes are not advertised to OMP.<br><br>• Connected—Click Off to disable advertising connected routes to OMP. By default, connected routes are advertised to OMP.<br><br>• OSPF—Click On and click On again in the External field that appears to advertise external OSPF routes to OMP. OSPF inter-area and intra-area routes are always advertised to OMP. By default, external OSPF routes are not advertised to OMP.<br><br>• Static—Click Off to disable advertising static routes to OMP. By default static routes are advertised to OMP.<br><br>To configure per-VPN route advertisements to OMP, use the VPN feature template . |

To save the feature template, click Save.

*CLI equivalent:*

```
omp
  advertise (bgp | connected | ospf | static) (on vEdge routers only)
```

## Release Information

Introduced in vManage NMS in Release 15.2.
In Release 17.1, add Overlay AS Number field.

## OSPF

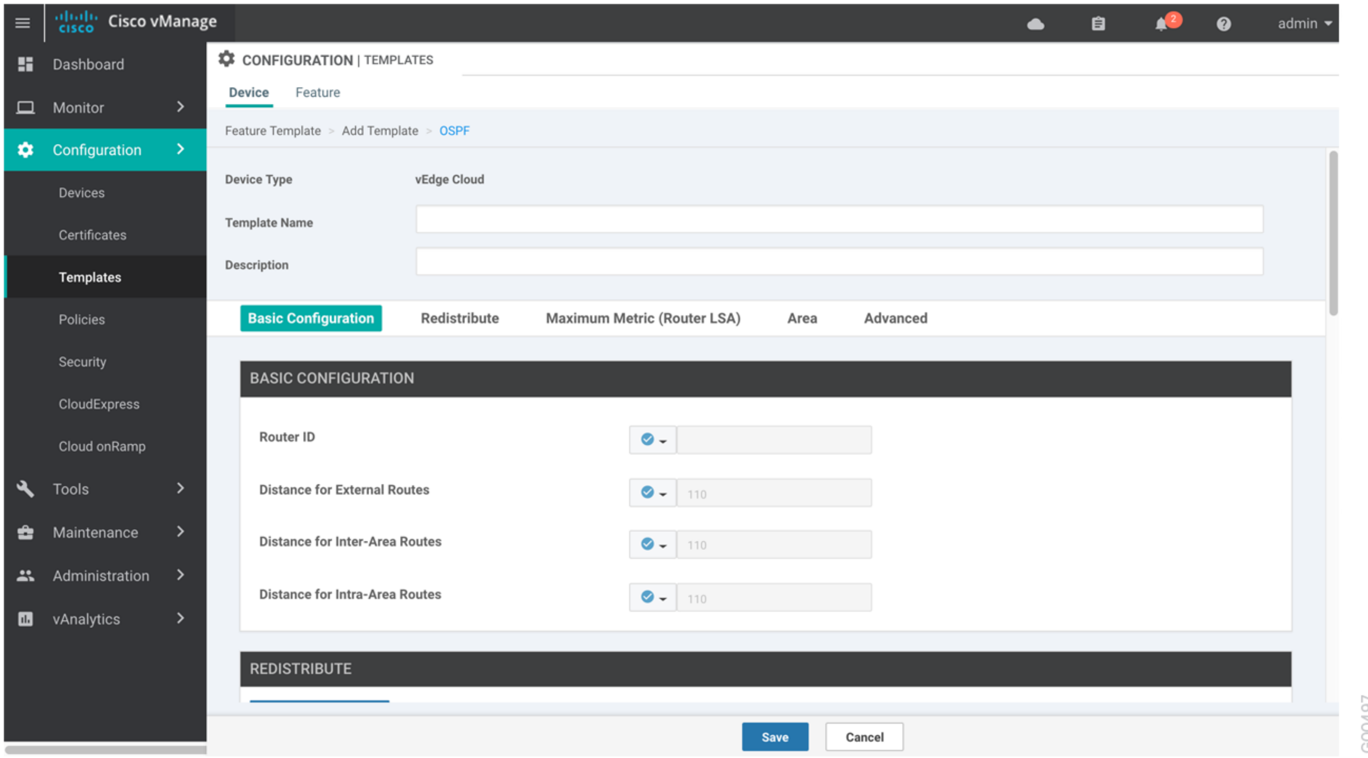
Use the OSPF template for all vEdge Cloud and vEdge router devices.

To configure OSPF on vEdge routers using vManage templates:

1. Create an OSPF feature template to configure OSPF parameters, as described in this article. OSPF can be used for service-side routing, to provide reachability to networks at the local site, and it can be used for transport-side routing, to enable communication between the vEdge router and other Viptela devices when the router is not directly connected to the WAN cloud. Create separate OSPF templates for the two OSPF routing types.
2. Create a VPN feature template to configure VPN parameters for either service-side OSPF routing (in any VPN other than VPN 0 or VPN 512) or transport-side OSPF routing (in VPN 0). See the VPN help topic.

## 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 template for VPN 0 or VPN 512:
    a. Click the Transport & Management VPN tab located directly beneath the Description field, or scroll to the Transport & Management VPN section.
    b. Under Additional VPN 0 Templates, located to the right of the screen, click OSPF.
    c. From the OSPF drop-down, click Create Template. The OSPF template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining OSPF parameters.
6. To create a template for VPNs 1 through 511, and 513 through 65530:
    a. Click the Service VPN tab located directly beneath the Description field, or scroll to the Service VPN section.
    b. Click the Service VPN drop-down.
    c. Under Additional VPN Templates, located to the right of the screen, click OSPF.
    d. From the OSPF drop-down, click Create Template. The OSPF template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining OSPF 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 and select one of the following:

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

## Configure Basic OSPF

To configure basic OSPF, select the Basic Configuration tab and then configure the following parameters. All these parameters are optional. For OSPF to function, you must configure area 0, as described below.

| Parameter Name | Description |
|---|---|
| Router ID | Enter the OSPF router ID, in decimal four-part dotted notation. This is the IP address associated with the router for OSPF adjacencies. |
| Distance for External Routes | Specify the OSPF route administration distance for routes learned from other domains.<br><br>*Range:* 0 through 255<br>*Default:* 110 |
| Distance for Inter-Area Routes | Specify the OSPF route administration distance for routes coming from one area into another.<br><br>*Range:* 0 through 255<br>*Default:* 110 |
| Distance for intra-Area routes | Specify the OSPF route administration distance for routes within an area.<br><br>*Range:* 0 through 255<br>*Default:* 110 |

To save the feature template, click Save.

*CLI equivalent:*

```
vpn vpn-id
  router
    distance
      external number
      inter-area number
      intra-area number
    router-id
```

## Redistribute Routes into OSPF

To redistribute routes learned from other protocols into OSPF on vEdge routers, select the Redistribute tab. Click Add New Redistribute and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Protocol | Select the protocol from which to redistribute routes into OSPF. Select from BGP, Connected, NAT, OMP, and Static. |
| Route Policy | Enter the name of a localized control policy to apply to routes before they are redistributed into OSPF. |

To add another OSPF route redistribution policy, click the plus sign (+).

To remove an OSPF route redistribution policy from the template configuration, click the trash icon to the right of the entry.

To save the feature template, click Save.

*CLI equivalent:*

```
vpn vpn-id
  router
    ospf
      redistribute (bgp | connected | nat | omp | static) route-policy policy-name
```

## Configure OSPF To Advertise a Maximum Metric

To configure OSPF to advertise a maximum metric so that other routers do not prefer this vEdge router as an intermediate hop in their Shortest Path First (SPF) calculation, select the Maximum Metric (Router LSA) tab. Then click Add New Router LSA and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Type | Select a type:<br>• Administrative—Force the maximum metric to take effect immediately, through operator intervention.<br>• On-Startup—Advertise the maximum metric for the specified time. |
| Advertisement Time | If you selected On-Startup, specify the number of seconds to advertise the maximum metric after the router starts up.<br>*Range:* 0, 5 through 86400 seconds<br>*Default:* 0 seconds (the maximum metric is advertised immediately when the router starts up) |

To save the feature template, click Save.

*CLI equivalent:*

```
vpn vpn-id
  router
    ospf
      max-metric
        router-lsa (administrative | on-startup seconds)
```

## Configure OSPF Areas

To configure an OSPF area within a VPN on a vEdge router, select the Area tab and click Add New Area. For OSPF to function, you must configure area 0.

| Parameter Name | Description |
|---|---|
| Area Number | Enter the number of the OSPF area.<br>*Range:* 32-bit number |
| Set the Area Type | Select the type of OSPF area, Stub or NSSA. |
| No Summary | Select On to not inject OSPF summary routes into the area. |
| Translate | If you configured the area type as NSSA, select when to allow vEdge routers that are ABRs (area border routers) to translate Type 7 LSAs to Type 5 LSAs:<br>always—Router always acts as the translator for Type 7 LSAs. That is, no other router, even if it is an ABR, can be the translator. If two ABRs are configured to always be the translator, only one of them actually ends up doing the translation.<br>candidate—Router offers translation services, but does not insist on being the translator.<br>never—Translate no Type 7 LSAs |

To save the new area, click Add.

To save the feature template, click Save.

*CLI equivalent:*

```
vpn vpn-id
  router
    ospf
```

```
area number
  nssa
    no-summary
    translate (always | candidate | never)
  stub
    no-summary
```

## Configure Interfaces in an OSPF Area

To configure the properties of an interface in an OSPF area, select the Area tab and click Add New Area. Then, in Interface, click Add Interface. In the Add Interface popup, configure the following parameters:

| Parameter Name | Description |
|---|---|
| Interface Name | Enter the name of the interface, in the format **ge** *slot* / *port* or **loopback** *number* . |
| Hello Interval | Specify how often the router sends OSPF hello packets.<br><br>*Range:* 1 through 65535 seconds<br>*Default:* 10 seconds |
| Dead Interval | Specify how often the vEdge router must receive an OSPF hello packet from its neighbor. If no packet is received, the vEdge router assumes that the neighbor is down.<br><br>*Range:* 1 through 65535 seconds<br>*Default:* 40 seconds (4 times the default hello interval) |
| LSA Retransmission Interval | Specify how often the OSPF protocol retransmits LSAs to its neighbors.<br><br>*Range:* 1 through 65535 seconds<br>*Default:* 5 seconds |
| Interface Cost | Specify the cost of the OSPF interface.<br><br>*Range:* 1 through 65535 |

To configure advanced options for an interface in an OSPF area, in the Add Interface popup, click Advanced Options and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Designated Router Priority | Set the priority of the router to be elected as the designated router (DR). The router with the highest priority becomes the DR. If the priorities are equal, the node with the highest router ID becomes the DR or the backup DR.<br>*Range:* 0 through 255<br>*Default:* 1 |
| OSPF Network Type | Select the OSPF network type to which the interface is to connect:<br><br>• Broadcast network—WAN or similar network.<br><br>• Point-to-point network—Interface connects to a single remote OSPF router.<br><br>*Default:* Broadcast |
| Passive Interface | Select On or Off to specify whether to set the OSPF interface to be passive. A passive interface advertises its address, but does not actively run the OSPF protocol.<br>*Default:* Off |
| Authentication | Specify the authentication and authentication key on the interface, to allow OSPF to exchange routing update information securely: |

| | |
|---|---|
| • Authentication Type | Select the authentication type:<br>• Simple authentication—Password is sent in clear text.<br>• Message-digest authentication—MD5 algorithm generates the password. |
| • Authentication Key | Enter the authentication key. Plain text authentication is used when devices within an area cannot support the more secure MD5 authentication. The key can be 1 to 32 characters. |
| Message Digest | Specify the key ID and authentication key if you are using message digest (MD5): |
| • Message Digest Key ID | Enter the key ID for message digest (MD5 authentication). It can be 1 to 32 characters. |
| • Message Digest Key | Enter the MD5 authentication key, in clear text or as an AES-encrypted key. It can be from 1 to 255 characters. |

To save the interface configuration, click Save.

To save the new area, click Add.

To save the feature template, click Save.

*CLI equivalent:*

```
vpn vpn-id
  router
    ospf
      area number
        interface interface-name
          authentication
            authentication-key key
            message-digest key
            type (message-digest | simple)
          cost number
          dead-interval seconds
          hello-interval seconds
          network (broadcast | point-to-point)
          passive-interface
          priority number
          retransmit-interval seconds
```

## Configure an Interface Range for Summary LSAs

To configure the properties of an interface in an OSPF area, select the Area tab and click Add New Area. Then, in Range, click Add Range. In the Area Range popup, click Add Area Range and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Address | Enter the IP address and subnet mask, in the format *prefix* / *length* , for the IP addresses to be consolidated and advertised. |
| Cost | Specify a number for the Type 3 summary LSA. OSPF uses this metric during its SPF calculation to determine the shortest path to a destination.<br>*Range:* 0 through 16777215 |
| No Advertise | Select On to not advertise the Type 3 summary LSAs or Off to advertise them. |

To save the area range, click Save.

To save the new area, click Add.

To save the feature template, click Save.

*CLI equivalent:*

```
vpn vpn-id
  router
    ospf
      area number
        range prefix/length
          cost number
          no-advertise
```

## Configure Other OSPF Properties

To configure other OSPF properties, select the Advanced tab and configure the following properties:

| Parameter Name | Description |
|---|---|
| Reference Bandwidth | Specify the reference bandwidth for the OSPF auto-cost calculation for the interface.<br><br>*Range:* 1 through 4294967 Mbps<br>*Default:* 100 Mbps |
| RFC 1538 Compatible | By default, the OSPF calculation is done per RFC 1583. Select Off to calculate the cost of summary routes based on RFC 2328. |
| Originate | Click On to generate a default external route into an OSPF routing domain:<br><br>• Always—Select On to always advertise the default route in an OSPF routing domain.<br><br>• Default metric—Set the metric used to generate the default route.<br>*Range:* 0 through 16777214<br>*Default:* 10<br><br>• Metric type—Select to advertise the default route as an OSPF Type 1 external route or an OSPF Type 2 external route. |
| SPF Calculation Delay | Specify the amount of time between when the first change to a topology is received until performing the SPF calculation.<br><br>*Range* : 0 through 600000 milliseconds (60 seconds)<br>*Default* : 200 milliseconds |
| Initial Hold Time | Specify the amount of time between consecutive SPF calculations.<br><br>*Range* : 0 through 600000 milliseconds (60 seconds)<br>*Default* : 1000 milliseconds |
| Maximum Hold Time | Specify the longest time between consecutive SPF calculations.<br><br>*Range* : 0 through 600000<br>*Default* : 10000 milliseconds (60 seconds) |
| Policy Name | Enter the name of a localized control policy to apply to routes coming from OSPF neighbors. |

To save the feature template, click Save.

*CLI equivalent:*

```
vpn vpn-id
  router
    ospf
```

```
auto-cost reference-bandwidth mbps
compatible rfc1583
default-information
  originate (always | metric metric | metric-type type)
route-policy policy-name in
timers
  spf delay initial-hold-time maximum-hold-time
```

## Release Information

Introduced in vManage NMS in Release 15.2.

## PIM

Use the PIM template for all vEdge Cloud and vEdge router devices.

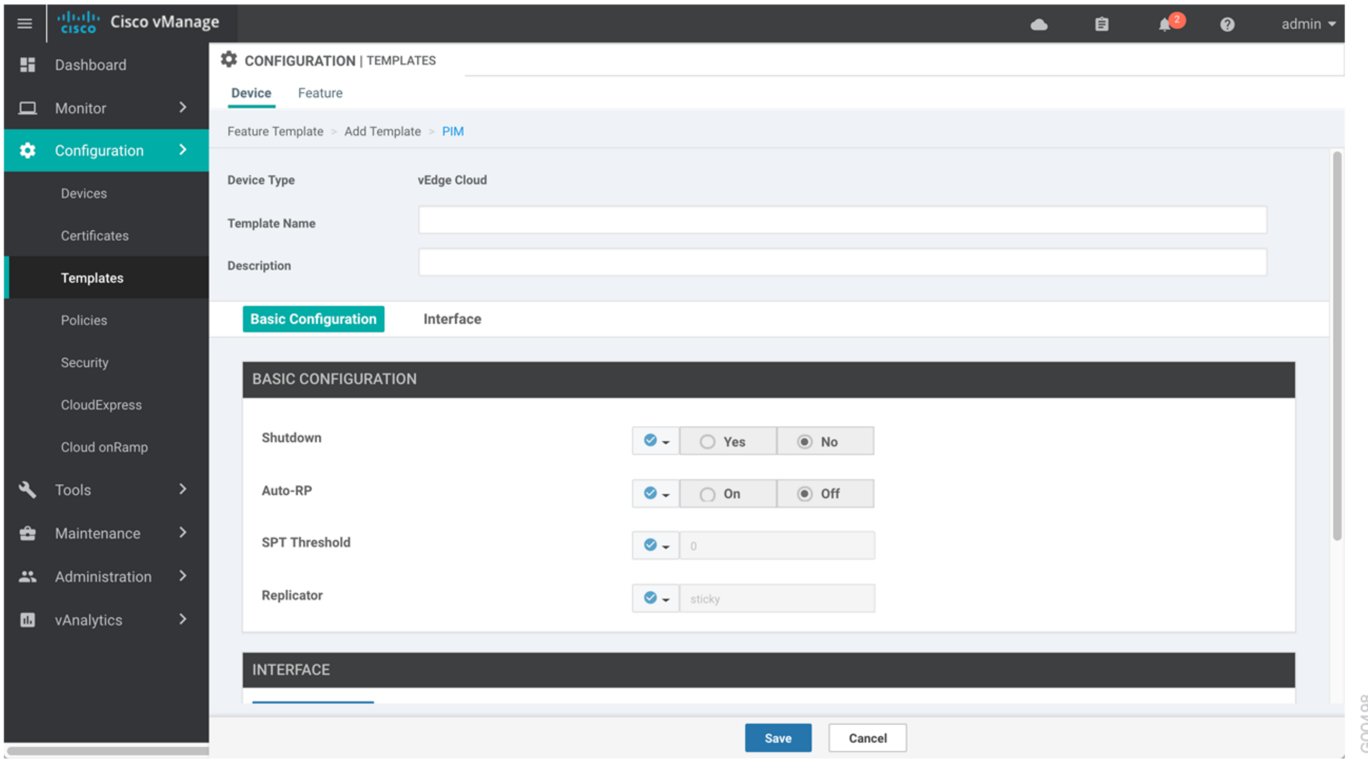
To configure the PIM Sparse Mode (PIM-SM) protocol using vManage templates so that a router can participate in the Viptela multicast overlay network:

1. Create a PIM feature template to configure PIM parameters, as described in this article.
2. Optionally, create an IGMP feature template to allow individual hosts on the service side to join multicast groups within a particular VPN. See the IGMP help topic.
3. Optionally, create a Multicast feature template to configure a vEdge router to be a multicast replicator. See the Multicast help topic.
4. Create a VPN feature template to configure parameters for the VPN that is running PIM. See the VPN help topic.

## 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. Click the Service VPN tab located directly beneath the Description field, or scroll to the Service VPN section.

6. Click the Service VPN drop-down.




7. Under Additional VPN Templates, located to the right of the screen, click PIM.

8. From the PIM drop-down, click Create Template. The PIM template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining PIM parameters.

9. In the Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

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

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

| 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 Viptela device to a device template** .<br><br>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 .<br><br>To change the default key, type a new string and move the cursor out of the Enter Key box.<br><br>Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID. |

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

## Configure Basic PIM

To configure PIM, select the Basic Configuration tab and configure the following parameters. Parameters marked with an asterisk are required to configure PIM.

| Parameter Name | Description |
|---|---|
| Shutdown* | Ensure that No is selected, to enable PIM. |
| Auto-RP | Click On to enable auto-RP to enable automatic discovery of rendezvous points (RPs) in the PIM network so that the router receivea group-to-RP mapping updates. By default, auto-RP is disabled. |
| SPT Threshold | Specify the traffic rate, in kbps, at which to switch from the shared tree to the shortest-path tree (SPT). Configuring this value forces traffic to remain on the shared tree and travel via the RP instead of via the SPT. |
| Replicator | For a topology that includes multicast replicators, determine how the replicator for a multicast group is chosen:<br><br>• Random—Choose the replicator at random.<br><br>• Sticky—Always use the same replicator. This is the default. |

To save the feature template, click Save.

*CLI equivalent:*

```
vpn vpn-id
  router
    pim
      auto-rp
      replicator-selection
      [no] shutdown
      spt-threshold kbps
```

## Configure PIM Interfaces

If the router is just a multicast replicator and is not part of a local network that contains either multicast sources or receivers, you do not need to configure any PIM interfaces. The replicator learns the locations of multicast sources and receivers from the OMP messages it exchanges with the vSmart controller. These control plane messages are exchanged in the transport VPN (VPN 0). Similarly, other vEdge routers discover replicators dynamically, through OMP messages from the vSmart controller.

To configure PIM interfaces, select the Interface tab. Then click Add New Interface and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Name | Enter the name of an interface that participates in the PIM domain, in the format **ge** *slot* /*port* . |
| Hello Interval | Specify how often the interface sends PIM hello messages. Hello messages advertise that PIM is enabled on the router.<br>*Range:* 1 through 3600 seconds<br>*Default:* 30 seconds |

| | |
|---|---|
| Join/Prune Interval | Specify how often PIM multicast traffic can join or be removed from a rendezvous point tree (RPT) or shortest-path tree (SPT). vEdge routers send join and prune messages to their upstream RPF neighbor.<br>*Range:* 10 through 600 seconds<br>*Default:* 60 seconds |

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

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

To save the feature template, click Save.

*CLI equivalent:*

```
vpn vpn-id
  router
    pim
      interface interface-name
        hello-interval seconds
        join-prune-interval seconds
```

## Release Information

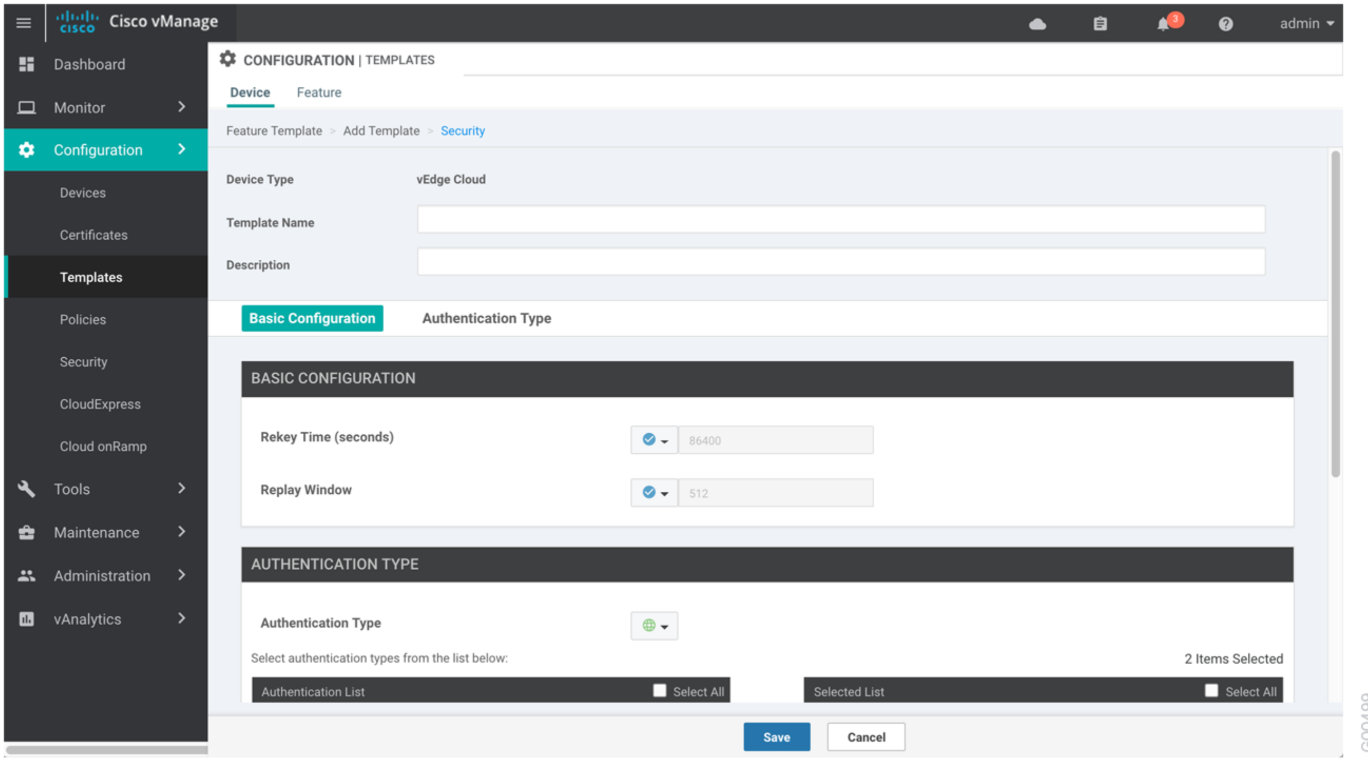
Introduced in vManage NMS in Release 15.2.

## Security

Use the Security template for all Viptela devices. On vEdge Cloud and vEdge routers and on vBond orchestrators, use this template to configure IPsec for data plane security. On vManage NMSs and vSmart controllers, use this template to configure DTLS or TLS for control plane security.

## 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 Security, select the Factory_Default_Security_Template and click Create Template. The Security template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining Security 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:

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

## Configure Control Plane Security

To configure the control plane connection protocol on a vManage NMS or a vSmart controller, select the Basic Configuration tab and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Protocol | Select the protocol to use on control plane connections to a vSmart controller:<br>• DTLS (Datagram Transport Layer Security). This is the default.<br>• TLS (Transport Layer Security) |
| Control TLS Port | If you selected TLS, configure the port number to use:<br>*Range:* 1025 through 65535<br>*Default:* 23456 |

To save the feature template, click Save

*CLI equivalent:*

```
security
  control
    protocol (dtls | tls)
    tls-port port-number
```

## Configure Data Plane Security

To configure data plane security on a vBond controller or vEdge router, select the Basic Configuration and Authentication Type tabs, and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Rekey Time | Specify how often a vEdge router changes the AES key used on its secure DTLS connection to the vSmart controller. If OMP graceful restart is enabled, the rekeying time must be at least twice the value of the OMP graceful restart timer.<br>*Range:* 10 through 1209600 seconds (14 days)<br>*Default:* 86400 seconds (24 hours) |
| Replay Window | Specify the size of the sliding replay window.<br>*Values:* 64, 128, 256, 512, 1024, 2048, 4096, 8192 packets<br>*Default:* 512 packets |
| Authentication Type | Select the authentication types from the Authentication List, and click the arrow to move them to the Selected List:<br>• ah-no-id—Enable a modified version of AH-SHA1 HMAC and ESP HMAC-SHA1 that ignores the ID field in the packet's outer IP header.<br>• ah-sha1-hmac—Enable AH-SHA1 HMAC and ESP HMAC-SHA1.<br>• none—Select no authentication.<br>• sha1-hmac—Enable ESP HMAC-SHA1. |

To save the feature template, click Save.

*CLI equivalent:*

```
security
  ipsec
    authentication-type type
```

```
rekey seconds
replay-window number
```

## Release Information

Introduced in vManage NMS in Release 15.2.

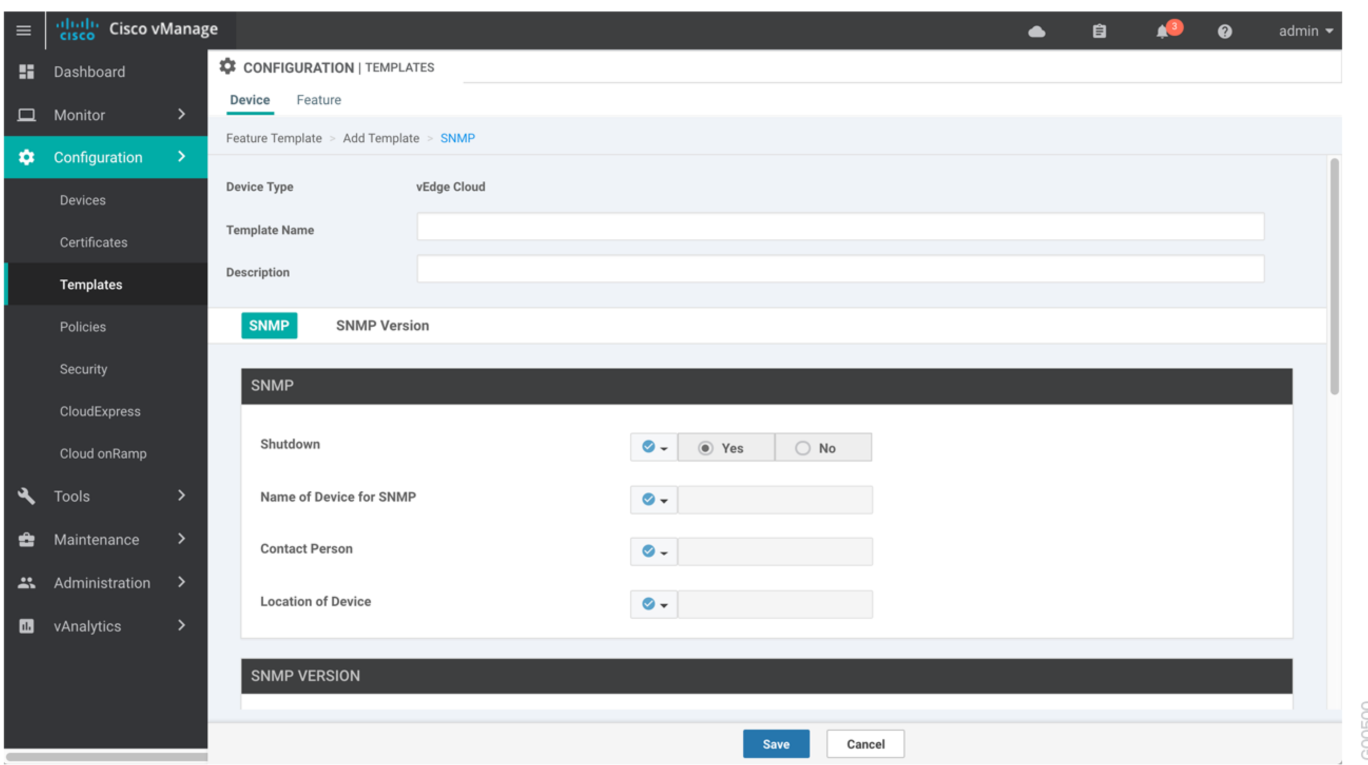
## SNMP

Use the SNMP template to configure SNMP parameters for all Viptela devices and Cisco IOS XE routers running the SD-WAN software.

Note: A single device template can contain only one SNMP feature template. So in a single device template you can configure either SNMPv2 or SNMPv3, but not both.

## 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. Click the Additional Templates tab located directly beneath the Description field, or scroll to the Additional Templates section.
6. From the SNMP drop-down, click Create Template. The SNMP template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining SNMP 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 and select one of the following:

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

## Configuring Basic SNMP

To configure basic SNMP, select the SNMP tab and configure the following parameters. All parameters are required.

| **Parameter Name** | **Description** |
|---|---|
| Shutdown | Click No to enable SNMP. By default, SNMP is disabled. |
| Name of Device for SNMP | Enter a name for the Viptela device to identify it in SNMP notifications. |
| Contact Person | Enter the name of the network management contact person in charge of managing the Viptela device. It can be a maximum of 255 characters. |
| Location of Device | Enter a description of the location of the device. It can be a maximum of 255 characters. |

To save the feature template, click Save.

*CLI equivalent:*

```
snmp
  contact string
  location string
  name string
  [no] shutdown
```

## Configure SNMPv2

To configure SNMPv2, select the SNMP Version tab and click V2. For SNMPv2, you can configure communities and trap information.

To configure SNMP views, in the View & Community section, select the View tab. Then click Add New View, and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Name | Enter a name for the view. A view specifies the MIB objects that the SNMP manager can access. The view name can be a maximum of 255 characters. You must add a view name for all views before adding a community. |
| Object Identifiers | Click Add Object Identifiers and configure the following parameters:<br>• Exclude OID—Enter the OID of the object. For example, to view the Internet portion of the SNMP MIB, enter the OID 1.3.6.1. To view the private portion of the Viptela MIB, enter the OID 1.3.6.1.4.1.41916. Use the asterisk wildcard (*) in any position of the OID subtree to match any value at that position rather than matching a specific type or name.<br>• On/Odd—Click Off to include the OID in the view or click On to exclude the OID from the view.<br>To save the object identifiers, click Save.<br>To remove an OID from the list, click the minus sign to the right of the entry. |

To add the SNMP view, click Add.

To configure the SNMP community, select the Community tab. Then click Add New Community, and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Name | Enter the name for the community. The name can be from 1 through 32 characters and can include angle brackets (< and >). |
| Authorization | Select read-only from the dropdown list. The MIBs supported by the Viptela software do not allow write operations, so you can configure only read-only authorization. |
| View | Select a view to apply to the community. The view specifies the portion of the MIB tree the community can access. |

To add the SNMP community, click Add.

To configure trap, in the Trap section, select the Trap Group tab. Then click Add New Trap Group, and configure the parameters below.

Note that an IOS XE router has no trap groups. As such, you must create a dummy trap group before you can configure the trap target server.

| Parameter Name | Description |
|---|---|
| Group Name | Enter a name for the trap group. It can be from 1 to 32 characters long. |

| | |
|---|---|
| Trap Type Modules | Click Add Trap Type Modules, and configure the following parameters:<br>In Severity Levels, select one or more severity levels for the trap—critical, major, or minor.<br>In Module Name, select the type of traps to include in the trap group:<br>• all—All trap types.<br>• app-route—Traps generated by application-aware routing.<br>• bfd—Traps generated by BFD and BFD sessions.<br>• control—Traps generated by DTLS and TLS sessions.<br>• dhcp—Traps generated by DHCP.<br>• hardware—Traps generated by Viptela hardware.<br>• omp—Traps generated by OMP.<br>• routing—Traps generated by BGP, OSPF, and PIM.<br>• security—Trap generated by certificates, vSmart and vEdge serial number files, and IPsec.<br>• system—Traps generated by system-wide functions.<br>• vpn—Traps generated by VPN-specific functions, including interfaces and VRRP. |

To save the trap type module, click Save.

To configure trap target servers, in the Trap section, select the Trap Target Server tab. Then click Add New Trap Group, and configure the parameters below.

Note that on a vEdge router, you can bind a different source interface to each trap target server. On an IOS XE router, however, the last occurrence of the source interface is chosen as the global source interface.

| Parameter Name | Description |
|---|---|
| VPN ID | Enter the number of the VPN to use to reach the trap server.<br>*Range:* 0 through 65530 |
| IP Address | Enter the IP address of the SNMP server. |
| UDP Port | Enter the UDP port number for connecting to the SNMP server.<br>*Range:* 1 though 65535 |
| Group Name | Select the name of a trap group that was configured under the Group tab. |
| Community Name | Select the name of a community that was configured under the Community tab. |
| Source Interface | Enter the interface to use to send traps to the SNMP server that is receiving the trap information. |

To save the trap target, click Add

To save the feature template, click Save.

*CLI equivalent:*

```
snmp
  community name
    authorization (read-only | read-write)
    view string
  trap
    group group-name
```

```
      trap-type
        level severity
    target vpn vpn-id ip-address udp-port
      community-name community-name
      group-name name
  view string
    oid oid-number [exclude]
```

## Configure SNMPv3

To configure SNMPv3, in SNMP Version, click V3. For SNMPv3, you can configure groups, users, and trap information. Configure groups and trap information as described above.

To confgure SNMPv3 users, in the User section, click Add New User and enter the following parameters:

| Parameter Name | Description |
|---|---|
| User | Enter a name of the SNMP user. It can be 1 to 32 alphanumeric characters. |
| Authentication Protocol | Select the authentication mechanism for the user:<br>• MD5—Use message digest 5.<br>• SHA—Use SHA-2 message digest. |
| Authentication Password | Enter the authentication password either in cleartext or as an AES-encrypted key. |
| Privacy Protocol | Select the privacy type for the user:<br>• AES-CFB-128—Use Advanced Encryption Standard cipher algorithm used in cipher feedback mode, with a 128-bit key. |
| Privacy Password | Enter the authentication password either in cleartext or as an AES-encrypted key. |
| Group | Select the name of a configure SNMPv3 group. |

To save the user, click Add.

To save the feature template, click Save.
*CLI equivalent:*

```
snmp
  group group-name authentication
    view string
  trap
    group group-name
      trap-type
        level severity
    target vpn vpn-id ip-address udp-port
      community-name community-name
      group-name name
  user username
    auth authentication
    auth-password password
    group group-name
    priv privacy
    priv-password password
```

## Release Information

Introduced in vManage NMS in Release 15.2.
In Release 16.2, add support for SNMPv3.
In Release 17.2, remove support for DES privacy for the SNMP user.

## Switch Port

Use the Switch Port template for Cisco IOS XE routers.

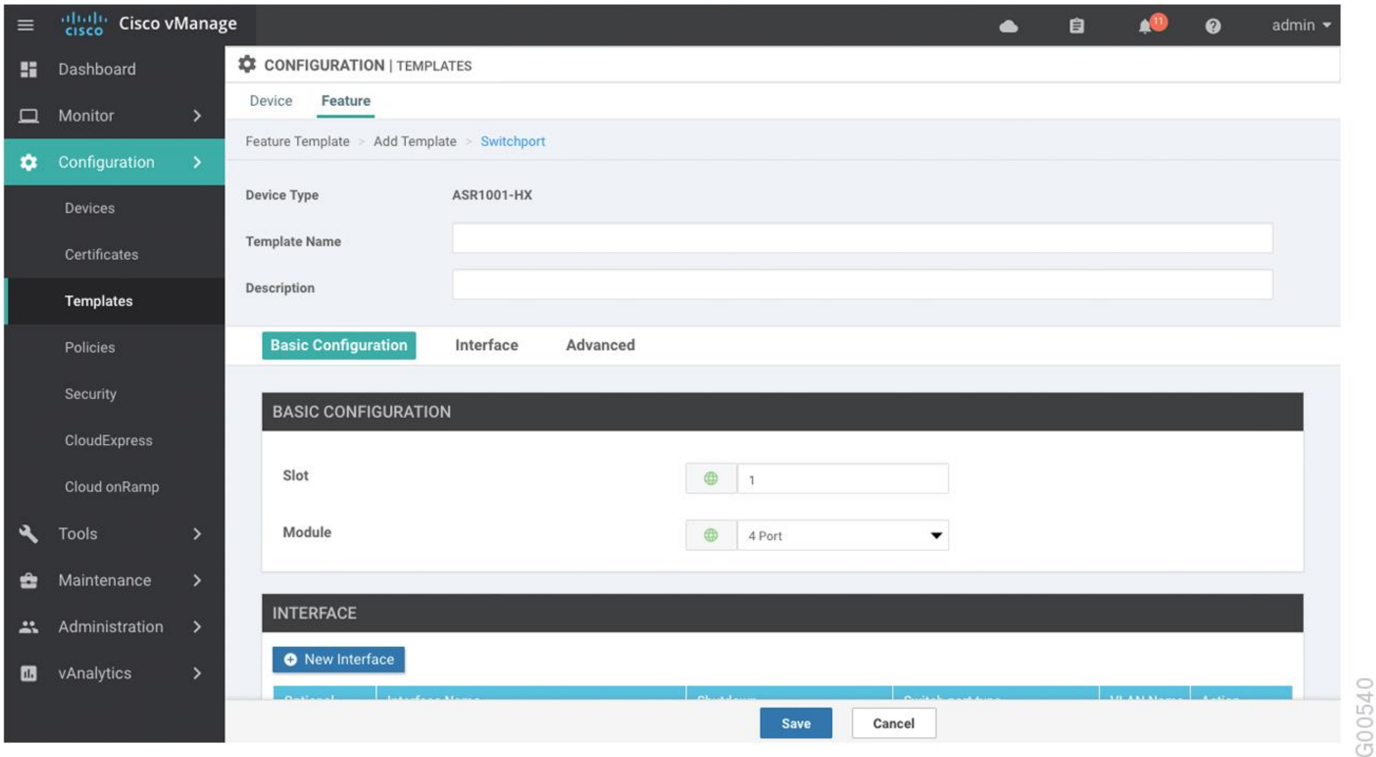
To have a vEdge router act as a transparent bridge, configure bridging domains on the router. A router can have up to 16 bridging domains.

To configure the switch ports using vManage templates:

1. Create a Switch Port feature template, as described in this article.
2. To use the switch port for routing, associate it with an SVI. See the **VPN Interface SVI** help topic.

## 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. Click the Additional Templates tab located directly beneath the Description field, or scroll to the Additional Templates section.
6. Click the plus sign (+) next to Switch Port.
7. In the Switch Port drop-down, select the port number.
8. From the lower Switch Port drop-down, click Create Template. The Switch Port template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining switch port parameters.




9. In the Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

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

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

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

## Configure Basic Switch Port Parameters

To configure basic switch port parameters, select the Basic Configuration tab and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Slot | Enter the number of the slot in which the Layer 2 switch port module is installed. |
| Module | Select the switch port module type, either 4 port or 8 port. |

To save the feature template, click Save.

## Associate Interfaces with the Switch Port

To associate an interface with the switch port, click the Interface tab and click Add New Interface.

The Wlan-GigabitEthernet0/1/8 interface applies only to C1111-8PW and C1111-8PLTExxW routers. To configure this interface, select either **C1111-8PW** or **C1111-8PLTExxW** when you create a switch port, and select **8 port** from the Module drop-down list. In addition, from the New Interface drop-down menu, make sure to select **Wlan-GigabitEthernet0/1/8** .

| Parameter Name | Description |
|---|---|
| Interface Name | Enter the name of the interface to associate with the bridging domain, in the format **ge** *slot* / *port* . |
| Shutdown | Click No to enable the interface. By default, an interface is disabled. |
| Switch Port | Select the switch port mode:<br>• Access—Configure the interface as an access port. You can configure only one VLAN on an access port, and the port can carry traffic for only one VLAN.<br>– VLAN Name—Enter a description for the VLAN.<br>– VLAN ID—Enter the VLAN number, which can be a value from 1 through 4094.<br>• Trunk—Configure the interface as a trunk port. You can configure one or more VLANs on a trunk port, and the port can carry traffic for multiple VLAN.<br>– Allowed VLANs—Enter the numbers of the VLANs for which the trunk can carry traffic.a description for the VLAN.<br>– Native VLAN ID—Enter the number of the VLAN allowed to carry untagged traffic. |

To save the feature template, click Save.

## Configure Other Interface Properties

To configure other interface properties, select the Advanced tab and configure the following properties:

| Parameter Name | Description |
|---|---|
| Age-Out Time | Enter how long an entry is in the MAC table before it ages out. Set the value to 0 to prevent entries from timing out.<br>*Range:* 0, 10 through 1000000 seconds<br>*Default:* 300 seconds |

| | |
|---|---|
| Static MAC Address | Click Add Static MAC Address to map a MAC address to a switch port. In the MAC Static Address field that appears, enter the following:<br>• MAC Address—Enter the static MAC address to map to the switch port interface.<br>• Switch Port Interface Name—Enter the name of the switch port interface.<br>• VLAN ID—Enter the number of the VLAN for the switch port.<br>Click Add to save the static MAD accress mapping. |

To save the feature template, click Save.

## Release Information

Introduced in vManage NMS in Release 18.3.

## System

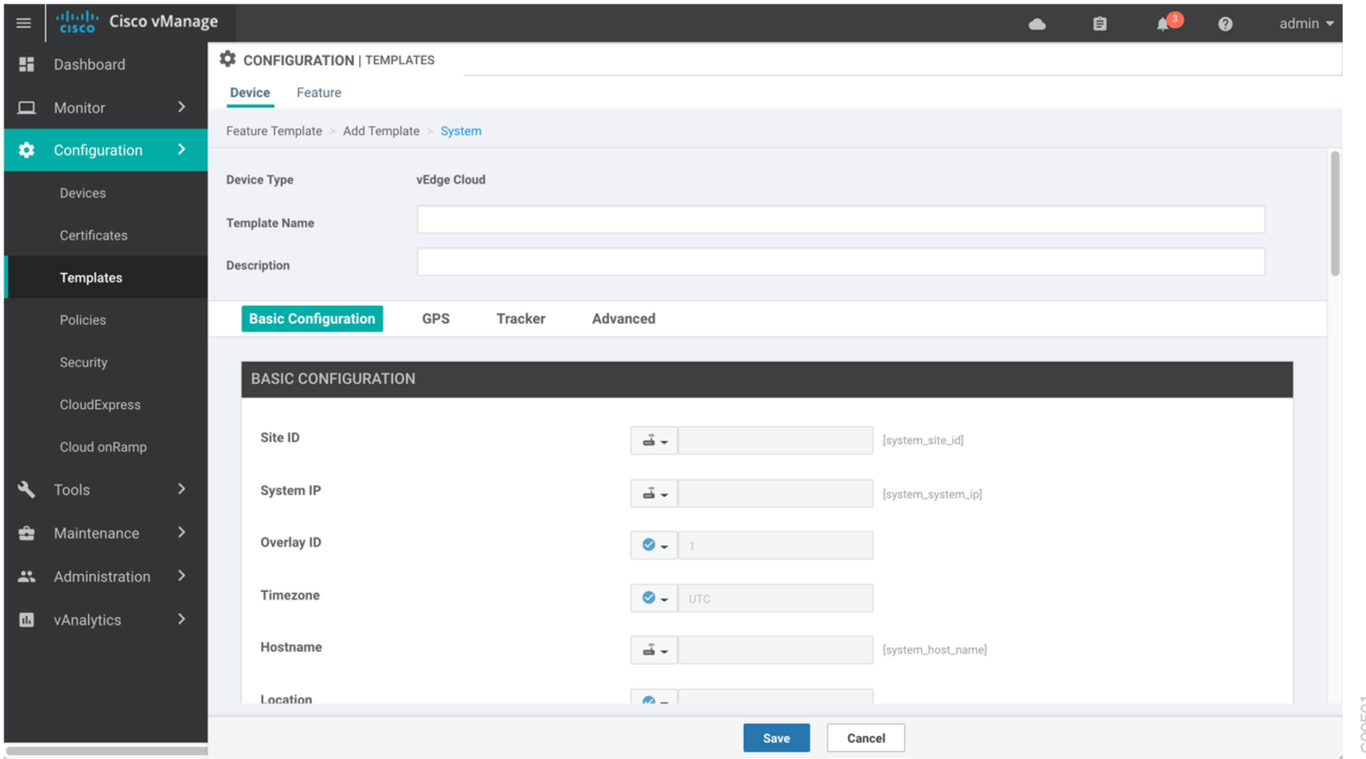
Use the System template for all Viptela devices.

To configure system-wide parameters using vManage templates:

1. Create a System feature template to configure system parameters, as described in this article.
2. Create an NTP feature template to configure NTP servers and authentication. See the NTP help topic.
3. Configure the organization name and vBond orchestrator IP address on the vManage NMS. See the Settings help topic. 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:

| 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 Viptela device to a device template** .<br><br>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 .<br><br>To change the default key, type a new string and move the cursor out of the Enter Key box.<br><br>Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID. |
| Global (indicated by a globe icon) | Enter a value for the parameter, and apply that value to all devices.<br><br>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 Viptela device, select the Basic Configuration tab and then configure the following parameters. Parameters marked with an asterisk are required.

| Parameter Field | Description |
|---|---|
| Site ID* (on vEdge routers, vManage NMSs, and vSmart controllers) | Enter the identifier of the site in the Viptela 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 Viptela devices that reside in the same site.<br>*Range:* 1 through 4294967295 ($2^{32} – 1$) |
| System IP* | Enter the system IP address for the Viptela 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 Viptela 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 (on vEdge routers only) | List the vSmart controller groups to which the vEdge router belongs. |
| Description | Enter any additional descriptive information about the device. |
| Console Baud Rate (vEdge routers only) | Select the baud rate of the console connection on the vEdge router.<br>*Values:* 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 baud or bits per second (bps)<br>*Default:* 115200 bps |
| Maximum OMP Sessions (on vEdge routers only) | Set the maximum number of OMP sessions that a vEdge router can establish to a vSmart controller.<br>*Range* : 0 through 100<br>*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 vBond orchestrator in your overlay network, go to the **Administration ► Settings** screen and click vBond.

## Configure the GPS Location

To configure a device's location, select the GPS tab and then configure the following parameters. This location is used to place the device on the vManage NMS network map. Setting the location also allows the vManage NMS to send a notification if the device is moved to another location.

| 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

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:

| 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.<br>*Range:* 100 through 1000 milliseconds<br>*Default:* 300 milliseconds |
| Interval | How often probes are sent to determine the status of the transport interface.<br>*Range:* 10 through 600 seconds<br>*Default:* 60 seconds (1 minute) |
| Multiplier | Number of times to resend probes before declaring that the transport interface is down.<br>*Range:* 1 through 10<br>*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. 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.

*CLI equivalent:*

```
system
  tracker tracker-name
    endpoint-dns-name dns-name
    endpoint-ip ip-address
    interval seconds
```

```
multiplier number
threshold milliseconds
```

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 template. You can apply only one tracker to an interface.

## Configure Advanced Options

To configure additional system parameters, click the Advanced tab:

| Parameter Name | Description |
|---|---|
| Control Session Policer Rate | Specify a maximum rate of DTLS control session traffic, to police the flow of control traffic.<br>*Range:* 1 through 65535 pps<br>*Default:* 300 pps |
| MTU of DTLS Tunnel | Specify the MTU size to use on the DTLS tunnels that send control traffic between Viptela devices.<br>*Range:* 500 through 2000 bytes<br>*Default:* 1024 bytes |
| Port Hopping | Click On to enable port hopping, or click Off to disable it. When a Viptela 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 Viptela 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.<br>*Default:* Enabled (on vEdge 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 Viptela devices are behind a single NAT device, to ensure that each device uses a unique base port for DTLS connections.<br>*Values:* 0 through 19 |
| DNS Cache Timeout | Specify when to time out the vBond orchestrator addresses that have been cached by the device.<br>*Range:* 1 through 30 minutes<br>*Default:* 30 minutes |
| 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 |
| Local vBond (only on vEdge routers acting as vBond orchestrators) | Click On to configure the vEdge router to act as a vBond orchestrator. Then specify the DNS name for the vBond orchestrator or its IP address, in decimal four-part dotted notation. |
| Track Interface (on vEdge routers only) | Set the tag string to include in routes associated with a network that is connected to a non-operational interface.<br>*Range:* 1 through 4294967295 |
| Multicast Buffer (on vEdge routers only) | Specify the percentage of interface bandwidth that multicast traffic can use.<br>*Range:* 5% through 100%<br>*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.<br>*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.<br>*Default:* Enabled |
| Host Policer Rate (on vEdge routers only) | Specify the maximum rate at which a policer delivers packets to the control plane.<br>*Range:* 1000 through 20000 pps<br>*Default:* 5000 pps |

| | |
|---|---|
| ICMP Error Rate (on vEdge routers only) | Specify how many ICMP error messages a policer can generate or receive.<br>*Range:* 1 through 200 pps<br>*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.<br>*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.<br>*Range:* 0 through 300 seconds<br>*Default:* CLI session does not time out |
| Eco-Friendly Mode (on vEdge Cloud routers only) | Click On to configure a vEdge 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 (on vEdge routers only)
  control-session-pps rate
  eco-friendly-mode (on vEdge Cloud routers only)
  host-policer-pps rate (on vEdge routers only)
  icmp-error-pps rate (on vEdge routers only)
  idle-timeout seconds
  multicast-buffer-percent percentage (on vEdge routers only)
  port-hop
  port-offset number
  route-consistency-check (on vEdge routers only)
  system-tunnel-mtu bytes
  timer
    dns-cache-timeout minutes
  track-default-gateway
  track-interface-tag number (on vEdge routers only)
  track-transport
  upgrade-confirm minutes
  [no] usb-controller (vEdge 1000 and 2000 routers only)
  vbond (dns-name | ip-address) local (on vEdge routers acting as vBond controllers)
```

## Release Information

Introduced in vManage NMS 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 ecofriendly mode.
In Release 17.2.2, add support for interface status tracking.

## T1/E1 Controller

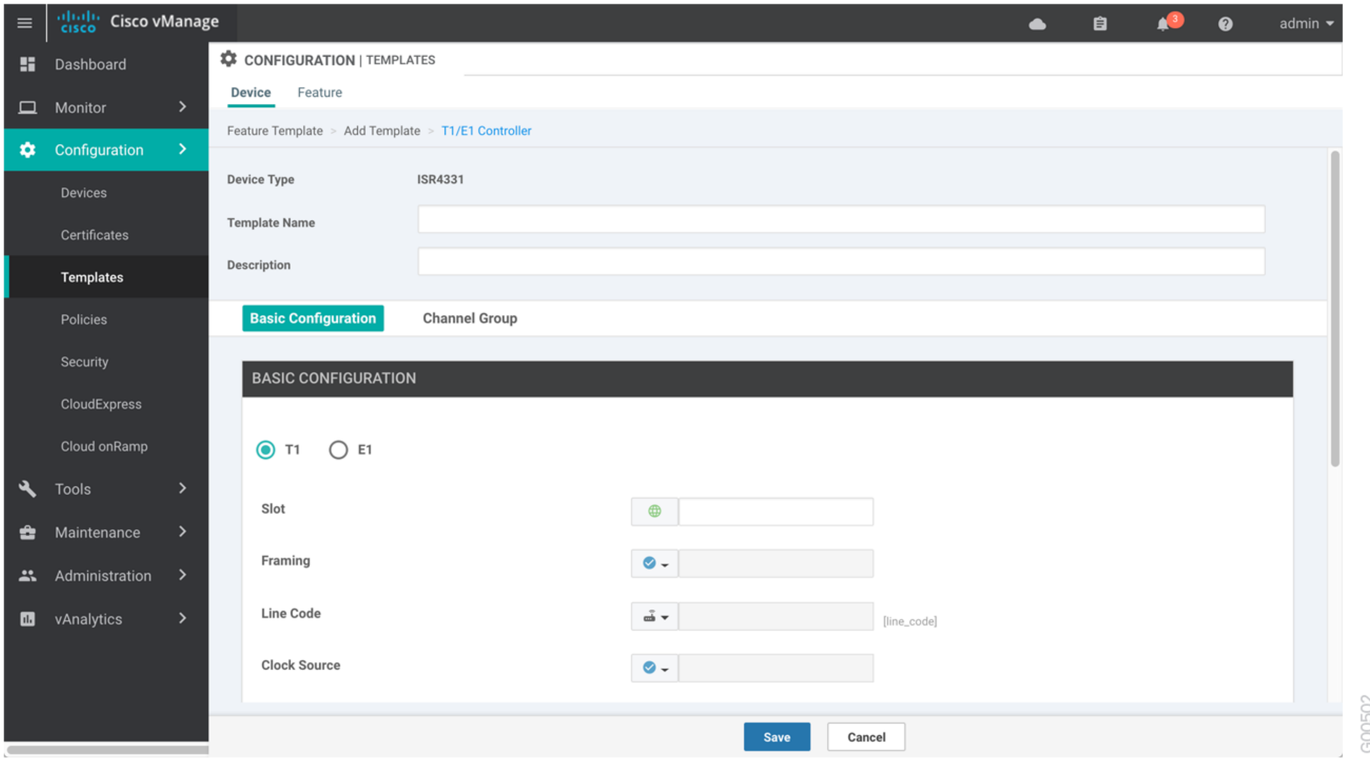
Use the T1/E1 Controller template for Cisco IOS XE routers running the SD-WAN software.

To configure the T1/E1 interfaces in a VPN using vManage templates:

1. Create a T1/E1 Controller template to configure the T1 or E1 network interface module (NIM) parameters, as described in this article.
2. Create a VPN Interface T1/E1 feature template to configure T1/E1 interface parameters. See the VPN Interface T1/E1 help topic.
3. Create a VPN feature template to configure VPN parameters. See the VPN help topic.

## 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 template for VPN 0 or VPN 512:
    a. Click the Transport & Management VPN tab located directly beneath the Description field, or scroll to the Transport & Management VPN section.
    b. Under Additional VPN 0 Templates, located to the right of the screen, click VPN Interface.
    c. From the VPN Interface drop-down, click Create Template. The VPN Interface T1/E1 template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN Interface Ethernet parameters.
6. To create a template for VPNs 1 through 511, and 513 through 65530:
    a. Click the Service VPN tab located directly beneath the Description field, or scroll to the Service VPN section.
    b. Click the Service VPN drop-down.
    c. Under Additional VPN templates, located to the right of the screen, click VPN Interface.
    d. From the VPN Interface drop-down, click Create Template. The VPN Interface Ethernet template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN Interface Ethernet 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 and select one of the following:

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

## Configure a T1 Controller

To configure a T1 controller, click the T1 radio button and configure the following parameters. Parameters marked with an asterisk are required to configure an interface.

| Parameter Name | Description |
|---|---|
| Slot* | Enter the number of the slot in which the T1 NIM is installed.<br><br>*Range:* 0 through 6 |
| Framing* | Enter the T1 frame type:<br><br>• **esf** —Send T1 frames as extended superframes. This is the default.<br><br>• **sf** —Send T1 frames as superframes. Superframing is sometimes called D4 framing. |
| Line Code | Select the line encoding to use to send T1 frames:<br><br>• ami—Use alternate mark inversion (AMI) as the linecode. AMI signaling uses frames grouped into superframes.<br><br>• b8zs—Use bipolar 8-zero substitution as the linecode. This is the default. B8ZS uses frames that are grouping into extended superframes |
| Clock Source | Select the clock source:<br><br>• internal—Use the controller framer as the reference clock.<br><br>• line—Use phase-locked loop (PLL) on the interface. This is the default. When both T1 ports use line clocking and neither port is configured as the primary, by default, port 0 is the primary clock source and port 1 is the secondary clock source. |
| Line Mode | If you choose the Line clock source, select whether the line is a primary or a secondary line. |
| Description | Enter a description for the controller. |
| Channel Group | Enter the number of the channel group. If you do so, you must enter a time slot in the Time Slot field.<br>*Range:* 0 through 30 |
| Time Slot | Enter the time slot or time slots that are part of the channel group.<br>*Range:* 1 through 24 |
| Cable Length | Select the cable length to configure the attenuation<br><br>• long—Attenuate the pulse from the transmitter using pulse equalization and line buildout. You can configure a long cable length for cables longer that 660 feet.<br><br>• short—Set the transmission attenuation for cables that are 660 feet or shorter.<br><br>There is no default length. |

| | |
|---|---|
| Length | If you specify a value in the Cable Length Field, enter the length of the cable.<br><br>For short cables, the length values can be:<br>• 110—Length from 0 through 110 feet<br>• 220—Length from 111 through 220 feet<br>• 330—Length from 221 through 330 feet<br>• 440—Length from 331 through 440 feet<br>• 550—Length from 441 through 550 feet<br>• 660—Length from 551 through 660 feet<br><br>For long cables, the length values can be:<br>• 0 dB<br>• –7.5 dB<br>• –15 dB<br>• –22.5 dB |

To save the feature template, click Save.

## Configure an E1 Controller

To configure an E1 controller, click the E1 radio button and configure the following parameters. Parameters marked with an asterisk are required to configure an interface.

| Parameter Name | Description |
|---|---|
| Slot* | Enter the number of the slot in which the E1 NIM is installed.<br><br>*Range:* 0 through 6 |
| Framing* | Enter the E1 frame type:<br>• **crc4** —Use cyclic redundancy check 4 (CRC4). This is the default.<br>• **no-crc4** —Do no use CRC4. |
| Line Code* | Select the line encoding to use to send E1 frames:<br>• ami—Use alternate mark inversion (AMI) as the linecode.<br>• hdb3—Use high-density bipolar 3 as the linecode. This is the default. |
| Clock Source | Select the clock source:<br>• internal—Use the controller framer as the reference clock.<br>• line—Use phase-locked loop (PLL) on the interface. This is the default. |
| Line Mode | If you choose the Line clock source, select whether the line is a primary or secondary line. If you configure both a primary and a secondary line, if the primary line fails, the PLL automatically switches to the secondary line. When the PLL on the primary line becomes active again, the PLL automatically switches back to the primary line. |

| | |
|---|---|
| Description | Enter a description for the controller. |
| Channel Group | To configure the serial WAN on the E1 interface, enter a channel group number.<br>*Range:* 0 through 30 |
| Time Slot | For a channel group, configure the timeslot.<br>*Range:* 1 through 31 |

To save the feature template, click Save.

## Release Information

Introduced in vManage NMS Release 18.1.1.

## VPN

Use the VPN template for all Viptela devices.

To configure VPNs for network segmentation using vManage templates:

1. Create VPN feature templates to configure VPN parameters, as described in this article. You create a separate VPN feature template for each VPN. For example, create one feature template for VPN 0, a second for VPN 1, and a third for VPN 512.
   For vManage NMSs and vSmart controllers, you can configure only VPNs 0 and 512. Create templates for these VPNs only if you want to modify the default settings for the VPN. For vEdge routers, you can create templates for these two VPNs and for additional VPN feature templates to segment service-side user networks.
   - 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.
   - VPN 512—Management VPN, which carries out-of-band network management traffic among the Viptela 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 vEdge routers except for vEdge 100. For controller devices, by default, VPN 512 is not configured.
   - VPNs 1 through 511, and 513 through 65530—VPNs on vEdge routers for service-side data traffic.
2. Create interface feature templates to configure the interfaces in the VPN. See the VPN-Interface-Ethernet help topic.
3. For vEdge routers, create interface feature templates to configure additional interfaces in the VPN. See the VPN-Interface-GRE , **VPN-Interface-PPP** , and **VPN-Interface-PPP-Ethernet** help topics.

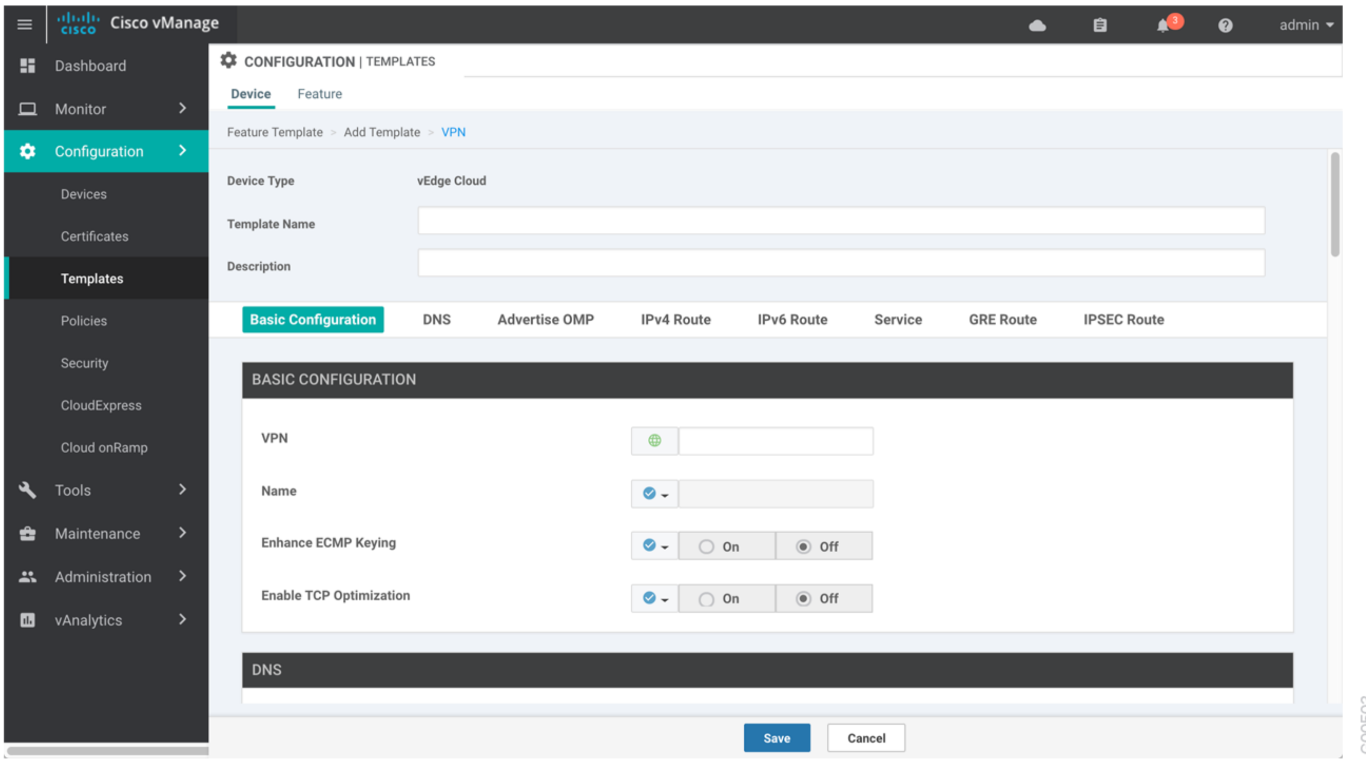
## Navigate to the Template Screen and Name the Template

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 template for VPN 0 or VPN 512:
   a. Click the Transport & Management VPN tab located directly beneath the Description field, or scroll to the Transport & Management VPN section.
   b. From the VPN 0 or VPN 512 drop-down, click Create Template. The VPN template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN parameters.
6. To create a template for VPNs 1 through 511, and 513 through 65530:

a. Click the Service VPN tab located directly beneath the Description field, or scroll to the Service VPN section.

b. Click the Service VPN drop-down.

c. From the VPN drop-down, click Create Template. The VPN template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN 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 and select one of the following:

| 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 Viptela device to a device template** .<br><br>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 .<br><br>To change the default key, type a new string and move the cursor out of the Enter Key box.<br><br>Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID. |

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

## Configure Basic VPN Parameters

To configure basic VPN parameters, select the Basic Configuration tab and then configure the following parameters. Parameters marked with an asterisk are required to configure a VPN.

| Parameter Name | Description |
|---|---|
| VPN* | Enter the numeric identifier of the VPN.<br><br>*Range for vEdge routers:* 0 through 65530<br>*Values for vSmart and vManage devices:* 0, 512 |
| Name | Enter a name for the VPN. |
| Enhance ECMP keying on vEdge routers only) | Click On to enable the use in the ECMP hash key of Layer 4 source and destination ports, in addition to the combination of the source IP address, destination IP address, protocol, and DSCP field, as the ECMP hash key. ECMP keying is Off by default. |
| Enable TCP Optimization ( on vEdge routers only) | Click On to enable TCP optimization for a service-side VPN (a VPN other than VPN 0 and VPN 512). TCP optimization fine-tunes TCP to decrease round-trip latency and improve throughput for TCP traffic. |
| Save | Click Save to save the feature template. |

To complete the configuration of the transport VPN on a vEdge router, you must configure at least one interface in VPN 0.

To save the feature template, click Save.

*CLI equivalent:*

```
vpn vpn-id
  ecmp-hash-key layer4 (on vEdge routers only)
  name text
  tcp-optimization (on vEdge routers only)
```

## Configure DNS and Static Hostname Mapping

To configure DNS addresses and static hostname mapping, select the DNS tab and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Primary DNS Address | Enter the IP address of the primary DNS server in this VPN. |
| Secondary DNS Address | Enter the IP address of a secondary DNS server in this VPN. This field appears only if you have specified a primary DNS address. |
| Hostname | Click Add New DNS, and enter the hostname of the DNS server. The name can be up to 128 characters. |
| List of IP Addresses | Enter up to eight IP addresses to associate with the hostname. Separate the entries with commas. |

To save the DNS server configuration, click Add.

To save the feature template, click Save.

*CLI equivalent:*

```
vpn vpn-id
  dns ip-address (primary | secondary)
  host hostname ip ip-address
```

## Configure Route Advertisements to OMP

To configure, for this VPN, route advertisements to OMP, select the Advertise OMP tab and configure the parameters listed below. Route advertisements that you configure here apply to the specific VPN. If you configure route advertisements to OMP for both the VPN and the entire vEdge router (using the OMP feature template ), both configurations are applied.

| Parameter Name | Description |
|---|---|
| BGP | Click On to advertise BGP routes from this VPN to OMP. |
| Static | Click On to advertise static routes from this VPN to OMP. |
| Connected | Click On to advertise connected routes from this VPN to OMP. |
| OSPF | Click On to advertise OSPF routes from this VPN to OMP. By default OSPF interarea and intra-areas routes are advertised OMP. Click On again to advertise external OSPF routes. |
| Network | Click the Network tab and click On to advertise a specific prefix to OMP. Click Add New Prefix, enter the prefix, and click Add |
| Aggregate | Click the Aggregate tab and click On to aggregate a prefix before advertising it to OMP. Click Add New Aggregate, enter the prefix, click On again to advertise only the aggregated prefix, and click Add. |

To save the route advertisement configuration, click Add.

To save the feature template, click Save.

*CLI equivalent:*

```
vpn vpn-id
  omp
    advertise (aggregate prefix [aggregate-only] | bgp | connected | network prefix | ospf type | static)
```

## Configure IPv4 Static Routes

To configure IPv4 static routes in a VPN, select the IPv4 Route tab. Then click Add New IPv4 Route, and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Prefix | Enter the IPv4 address or prefix, in decimal four-point-dotted notation, and the prefix length of the IPv4 static route to configure in the VPN. |
| Gateway | To configure the next hop to reach the static route, select one of the following:<br>• Next Hop—Specify the IPv4 address of the next-hop router to use to reach the static route.<br>• Null0—Specify that the next hop is the null interface.<br>• VPN0—Direct packets to the transport VPN.<br>Then click the plus sign (+) below the Gateway field to configure information about the next hop. |

| | |
|---|---|
| Address | If you select Next Hop as the gateway, click Add Next Hop. Then enter the IP address of the next-hop router and an administrative distance for the route. The distance can be a value from 1 through 255. The default is 1. Then click Save. |
| Enable Null0 | If you select Null0 as the gateway, in Enable Null0, click On to set the next hop to be the null interface. All packets sent to this interface are dropped without sending any ICMP messages. You can also set an administrative distance for the route. The distance can be a value from 1 through 255. The default is 1. |
| Enable VPN | If you select VPN as the gateway, in Enable VPN, click On to direct packets to the transport VPN. If NAT is enabled on the WAN interface, the packets can be forwarded to an Internet destination or other destination outside of the overlay network, effectively converting the vEdge router into a local Internet exit point. You must also enable NAT on a transport interface in VPN 0. |

To save the configured IPv4 static routes, click Add.

To save the feature template, click Save.

*CLI equivalent:*

```
vpn vpn-id
  ip route ip-address/subnet next-hop-address [administrative-distance]
```

## Configure IPv6 Static Routes

To configure IPv6 static routes in VPN 0, select the IPv6 Route tab. Then click Add New IPv6 Route, and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Prefix | Enter the IPv6 address or prefix, and the prefix length of the IPv6 static route to configure in VPN 0. |
| Gateway | To configure the next hop to reach the static route, select one of the following:<br>• Next Hop—Specify the IPv6 address of the next-hop router to use to reach the static route.<br>• Null0—Specify that the next hop is the null interface.<br>• VPN—Direct packets to the transport VPN. |
| Address | If you select Next Hop as the gateway, click Add Next Hop. Then enter the IP address of the next-hop router and an administrative distance for the route. The distance can be a value from 1 through 255. The default is 1.<br>To save the address, click Save |
| Enable Null0 | If you select Null0 as the gateway, in Enable Null0, click On to set the next hop to be the null interface. All packets sent to this interface are dropped without sending any ICMP messages. You can also set an administrative distance for the route. The distance can be a value from 1 through 255. The default is 1. |
| Enable VPN | If you select VPN as the gateway, in Enable VPN, click On to direct packets to the transport VPN. If NAT is enabled on the WAN interface, the packets can be forwarded to an Internet destination or other destination outside of the overlay network, effectively converting the vEdge router into a local Internet exit point. You must also enable NAT on a transport interface in VPN 0. |

To save the configured IPv6 static routes, click Add.

To save the feature template, click Save.

*CLI equivalent:*

```
vpn 0
  ipv6 route ip-address/subnet next-hop-address [administrative-distance]
```

## Configure Services

For a server VPN on a vEdge router (any VPN except VPN 0 and VPN 512), you can configure services that are either present on the router's local network or available on a device at a remote site that is reachable through a GRE tunnel.

To configure a service in a VPN, select the Service tab. Then click Add New Service, and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Service Type | Select the service available in the local VPN.<br>*Values:* FW, IDP, IDS, netsvc1, netsvc2, netsvc3, netsvc4, TE |
| IP Address or Interface | Enter the location of the service:<br>• If you select IP address, specify up to four IP address, separated by commas. The service is advertised to the vSmart controller only if one of the addresses can be resolved locally, at the local site, not via routes learned through OMP. You can configure up to four IP addresses.<br>• If you select Interface, specify one or two GRE interfaces. If you configure two, the first interface is the primary GRE tunnel, and the second is the backup tunnel. |

To save the service configuration, click Add.

To save the feature template, click Save.

*CLI equivalent:*

```
vpn vpn-id
  service service-name address ip-address
```

## Configure GRE-Specific Static Routes

To configure GRE-specific static routes in a service VPN (any VPN except VPN 0 and VPN 512 on a vEdge router), select the GRE Route tab. Then click Add New GRE Route, and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Prefix | Enter the IP address or prefix , in decimal four-part-dotted notation, and prefix length of the GRE-specific static route. |
| VPN ID | Enter the number of the VPN to reach the service. This must be VPN 0. |
| GRE Interface | Enter the name of one or two GRE tunnels to use to reach the service. |

To save a GRE-specific static route, click Add.

To save the feature template, click Save.

*CLI equivalent:*

```
vpn vpn-id
  ip gre-route prefix/length vpn 0 interface grenumber [grenumber2]
```

## Configure IPsec-Specific Static Routes

To configure IPsec-specific static routes in a service VPN (any VPN except VPN 0 and VPN 512 on a vEdge router), select the IPsec Route tab. Then click Add New IPsec Route, and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Prefix | Enter the IP address or prefix , in decimal four-part-dotted notation, and prefix length of the IPsec-specific static route. |
| VPN ID | Enter the number of the VPN to reach the IPsec tunnel. This must be VPN 0. |
| IPsec Interface | Enter the name of one or two IPsec tunnel interfaces. If you configure two interfaces, the first is the primary IPsec tunnel, and the second is the backup. All packets are sent only to the primary tunnel. If that tunnel fails, all packets are then sent to the secondary tunnel. If the primary tunnel comes back up, all traffic is moved back to the primary IPsec tunnel. |

To save an IPsec-specific static route, click Add.

To save the feature template, click Save.

*CLI equivalent:*

```
vpn vpn-id
  ip ipsec-route prefix/length vpn 0 interface ipsecnumber [ipsecnumber2]
```

## Release Information

Introduced in vManage NMS in Release 15.2.
In Release 15.4.3, add support for GRE tunnels.
In Release 16.3, add support for IPv6 in VPN 0.
In Release 17.2.0, add support for TE service.
In Release 18.2.0 add support for static routes to IPsec tunnels.

## VPN Interface Bridge

Use the VPN Interface Bridge template for all vEdge Cloud and vEdge router devices.

Integrated routing and bridging (IRB) allows vEdge routers in different bridge domains to communicate with each other. To enable IRB, create logical IRB interfaces to connect a bridge domain to a VPN. The VPN provides the Layer 3 routing services necessary so that traffic can be exchanged between different VLANs. Each bridge domain can have a single IRB interface and can connect to a single VPN, and a single VPN can connect to multiple bridge domains on a vEdge router.

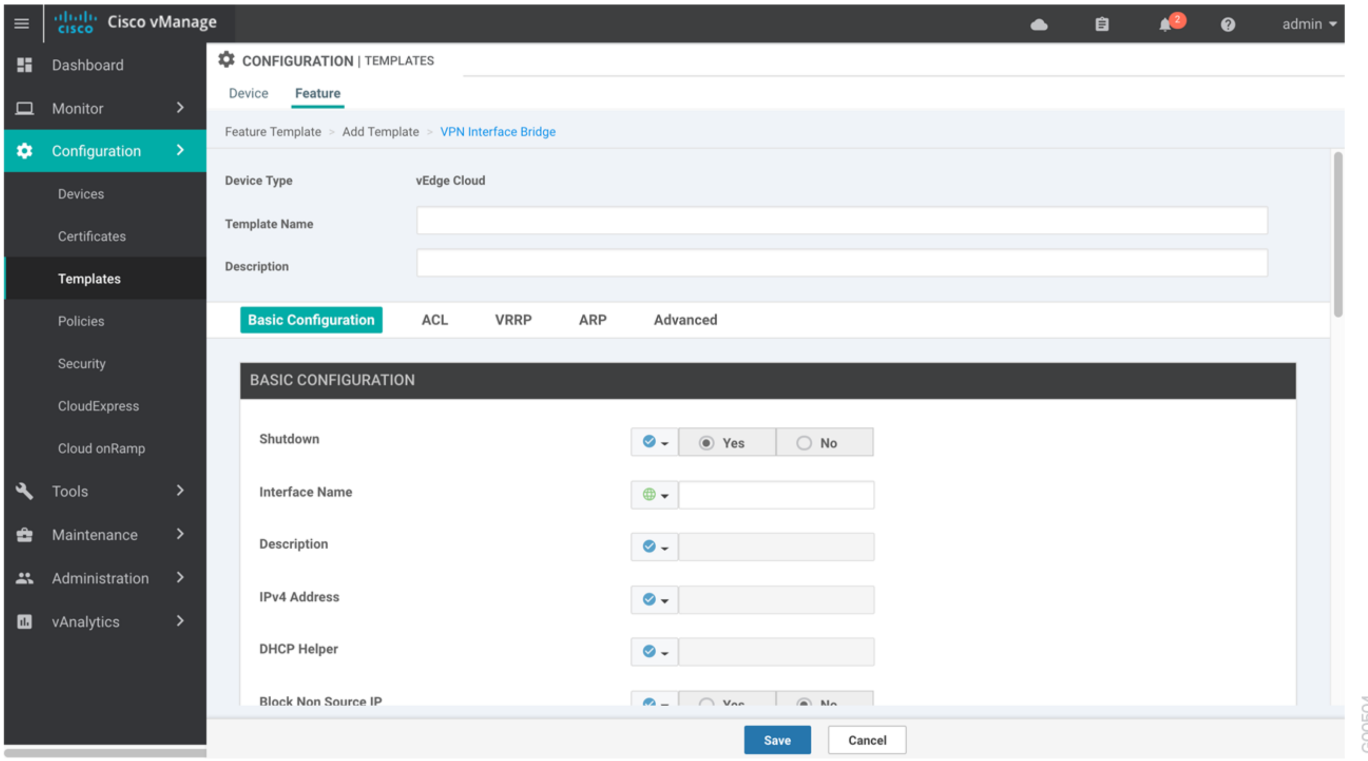
To configure a bridge interface using vManage templates:

1. Create a VPN Interface Bridge feature template to configure parameters for logical IRB interfaces, as described in this article.
2. Create a Bridge feature template for each bridging domain, to configure the bridging domain parameters. See the Bridge help topic.

## 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. Click the Service VPN tab located directly beneath the Description field, or scroll to the Service VPN section.

6. Click the Service VPN drop-down.




7. Under Additional VPN Templates, located to the right of the screen, click VPN Interface Bridge.

8. From the VPN Interface Bridge drop-down, click Create Template. The VPN Interface Bridge template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN Interface Bridge parameters.

9. In the Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

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

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

| 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 Viptela device to a device template** .<br><br>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]() .<br><br>To change the default key, type a new string and move the cursor out of the Enter Key box.<br><br>Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID. |

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

## Create a Bridging Interface

To configure an interface to use for bridging servers, select the Basic Configuration tab and click configure the following parameters. Parameters marked with an asterisk are required to configure bridging.

| Parameter Name | Description |
|---|---|
| Shutdown* | Click No to enable the interface. |
| Interface name* | Enter the name of the interface, in the format **irb** *number* . The IRB interface number can be from 1 through 63, and must be the same as the VPN identifier configured in the Bridge feature template for the bridging domain that the IRB is connected to. |
| Description | Enter a description for the interface. |
| IPv4 Address* | Enter the IPv4 address of the router. |
| DHCP Helper | Enter up to eight IP addresses for DHCP servers in the network, separated by commas, to have the interface be a DHCP helper. A DHCP helper interface forwards BOOTP (Broadcast) DHCP requests that it receives from the specified DHCP servers. |
| Block Non-Source IP | Click Yes to have the interface forward traffic only if the source IP address of the traffic matches the interface's IP prefix range. |
| Secondary IP Address (on vEdge routers) | Click Add to configure up to four secondary IPv4 addresses for a service-side interface. |

To save the template, click Save.

*CLI equivalent:*

```
vpn vpn-id
  interface irbnumber
    description "text description"
    dhcp-helper ip-addresses
    ip address prefix/length
    mac-address mac-address
    mtu bytes
    secondary-address ipv4-address
    [no] shutdown
    tcp-mss-adjust bytes
```

## Apply Access Lists

To apply access lists to IRB interfaces, select the ACL tab and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Ingress ACL – IPv4 | Click On, and specify the name of an IPv4 access list to packets being received on the interface. |
| Egress ACL– IPv4 | Click On, and specify the name of an IPv4 access list to packets being transmitted on the interface. |

To save the feature template, click Save.

*CLI equivalent:*

```
vpn vpn-id
  interface irbnumber
    access-list acl-name (in | out)
```

## Configure VRRP

To have an interface run the Virtual Router Redundancy Protocol (VRRP), which allows multiple routers to share a common virtual IP address for default gateway redundancy, select the VRRP tab. Then click Add New VRRP and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Group ID | Enter the virtual router ID, which is a numeric identifier of the virtual router. You can configure a maximum of 24 groups.<br>*Range:* 1 through 255 |
| Priority | Enter the priority level of the router. There router with the highest priority is elected as primary. If two vEdge routers have the same priority, the one with the higher IP address is elected as primary.<br>*Range:* 1 through 254<br>*Default:* 100 |
| Timer | Specify how often the VRRP primary sends VRRP advertisement messages. If subordinate routers miss three consecutive VRRP advertisements, they elect a new primary.<br>*Range:* 1 through 3600 seconds<br>*Default:* 1 second |
| Track OMP<br>Track Prefix List | By default, VRRP uses of the state of the service (LAN) interface on which it is running to determine which vEdge router is the primary virtual router. if a vEdge router loses all its WAN control connections, the LAN interface still indicates that it is up even though the router is functionally unable to participate in VRRP. To take WAN side connectivity into account for VRRP, configure one of the following:<br><br>Track OMP—Click On for VRRP to track the Overlay Management Protocol (OMP) session running on the WAN connection. If the primary VRRP router loses all its OMP sessions, VRRP elects a new default gateway from those that have at least one active OMP session.<br><br>Track Prefix List—Track both the OMP session and a list of remote prefixes, which is defined in a prefix list configured on the local router. If the primary VRRP router loses all its OMP sessions, VRRP failover occurs as described for the Track OMP option. In addition, if reachability to one of the prefixes in the list is lost, VRRP failover occurs immediately, without waiting for the OMP hold timer to expire, thus minimizing the amount of overlay traffic is dropped while the vEdge routers determine the VRRP primary. |
| IP Address | Enter the IP address of the virtual router. This address must be different from the configured interface IP addresses of both the local vEdge router and the peer running VRRP. |

To save the VRRP configuration, click Add.

To save the feature template, click Save.

*CLI equivalent:*

```
vpn vpn-id
  interface irbnumber[.subinterface]
    vrrp group-number
      ipv4 ip-address
      priority number
      timer seconds
      (track-omp | track-prefix-list list-name)
```

# Add ARP Table Entries

To configure static Address Resolution Protocol (ARP) table entries on the interface, select the ARP tab. Then click Add New ARP and configure the following parameters:

| Parameter Name | Description |
|---|---|
| IP Address | Enter the IP address for the ARP entry in dotted decimal notation or as a fully qualified host name. |
| MAC Address | Enter the MAC address in colon-separated hexadecimal notation. |

To save the ARP configuration, click Add.

To save the feature template, click Save.

*CLI equivalent:*

```
vpn vpn-id
  interface irbnumber
    arp
      ip address ip-address mac mac-address
```

# Configure Other Interface Properties

To configure other interface properties, select the Advanced tab and configure the following parameters:

| Parameter Name | Description |
|---|---|
| MAC Address | Specify a MAC address to associate with the interface, in colon-separated hexadecimal notation. |
| IP MTU | Specify the maximum MTU size of packets on the interface.<br>*Range:* 576 through 1804<br>*Default:* 1500 bytes |
| TCP MSS | Specify the maximum segment size (MSS) of TPC SYN packets passing through the vEdge router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented.<br>*Range:* 552 to 1460 bytes<br>*Default:* None |
| Clear-Dont-Fragment | Click On to clear the Don't Fragment (DF) bit in the IPv4 packet header for packets being transmitted out the interface. When the DF bit is cleared, packets larger than that interface's MTU are fragmented before being sent. |
| ARP Timeout | Specify how long it takes for a dynamically learned ARP entry to time out.<br><br>*Range:* 0 through 2678400 seconds (744 hours)<br>*Default:* 1200 seconds (20 minutes) |
| ICMP Redirect | Click Disable to disable ICMP redirect messages on the interface. By default, an interface allows ICMP redirect messages. |

To save the feature template, click Save.

*CLI equivalent:*

```
vpn vpn-id
  interface irbnumber
    arp-timeout seconds
    clear-dont-fragment
    icmp-redirect-disable
    mac-address mac-address
    mtu bytes
    tcp-mss-adjust bytes
```

## Release Information

Introduced in vManage NMS in Release 15.3.
In Release 18.2, add support for disabling ICMP redirect messages.

## VPN Interface Cellular

Use the VPN Interface Cellular feature template to configure cellular module parameters on vEdge routers and Cisco IOS XE routers running the SD-WAN software.

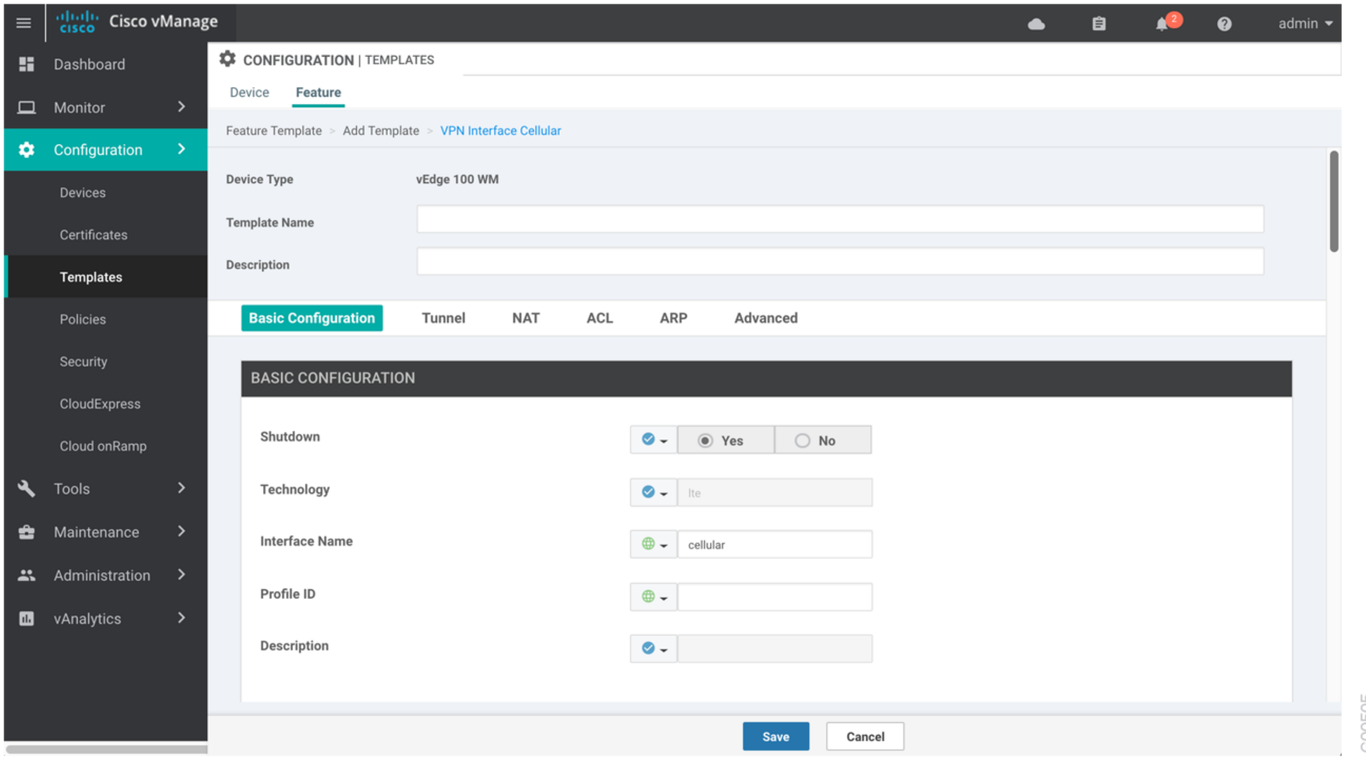
To configure cellular interfaces using vManage templates:

1. Create a VPN Interface Cellular feature template to configure cellular module parameters, as described in this article.
2. Create a Cellular Profile template to configure the profiles used by the cellular modem. See the Cellular Profile help topic.
3. Create a VPN feature template to configure VPN parameters. See the VPN help topic.

## Navigate to the Template Screen

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. Click the Transport & Management VPN tab located directly beneath the Description field, or scroll to the Transport & Management VPN section.

6. Under Additional VPN 0 Templates, located to the right of the screen, click VPN Interface Cellular.




7. From the VPN Interface Cellular drop-down, click Create Template. The VPN Interface Cellular template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN Interface Cellular 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:

| 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 Viptela device to a device template** .<br><br>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 .<br><br>To change the default key, type a new string and move the cursor out of the Enter Key box.<br><br>Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID. |

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

## Configure Basic Cellular Interface Functionality

To configure basic cellular interface functionality, select the Basic Configuration tab and configure the following parameters. Parameters marked with an asterisk are required to configure an interface. You must also configure a tunnel interface for the cellular interface.

| Parameter Name | Description |
|---|---|
| Shutdown* | Click No to enable the interface. |
| Technology | Cellular technology. The default is **lte** . Other values are **auto** and **cdma** . For ZTP to work, the technology must be **auto** . |
| Interface Name* | Enter the name of the interface. It must be **cellular0** . |
| Profile ID* | Enter the identification number of the cellular profile. This is the profile identifier that you configure in the Cellular-Profile template.<br>*Range:* 1 through 15 |
| Description | Enter a description of the cellular interface. |
| IPv4 Configuration | To configure a static address, click Static and enter an IPv4 address.<br><br>To set the interface as a DHCP client so that the interface to receive its IP address from a DHCP server, click Dynamic. You can optionally set the DHCP distance to specify the administrative distance of routes learned from a DHCP server. The default DHCP distance is 1. |
| IPv6 Configuration | To configure a static address for an interface in VPN 0, click Static and enter an IPv6 address.<br><br>To set the interface as a DHCP client so that the interface to receive its IP address from a DHCP server, click Dynamic.You can optionally set the DHCP distance to specify the administrative distance of routes learned from a DHCP server. The default DHCP distance is 1. You can optionally enable DHCP rapid commit, to speed up the assignment of IP addresses. |
| DHCP Helper | Enter up to four IP addresses for DHCP servers in the network, separated by commas, to have the interface be a DHCP helper. A DHCP helper interface forwards BOOTP (Broadcast) DHCP requests that it receives from the specified DHCP servers. |
| Block Non-Source IP | Click Yes to have the interface forward traffic only if the source IP address of the traffic matches the interface's IP prefix range. |
| Bandwidth Upstream | For transmitted traffic, set the bandwidth above which to generate notifications.<br>*Range:* 1 through ($2^{32}$ / 2) – 1 kbps |
| Bandwidth Downstream | For received traffic, set the bandwidth above which to generate notifications.<br>*Range:* 1 through ($2^{32}$ / 2) – 1 kbps |
| IP MTU* | Enter 1428 to set the MTU size, in bytes. This value must be 1428. You cannot use a different value. |

To save the feature template, click Save.

*CLI equivalent:*

```
vpn 0
  interface cellular0
    bandwidth-downstream kbps
    bandwidth-upstream kbps
```

```
block-non-source-ip
(ip address ip-address/length | ip dhcp-client [dhcp-distance number])
(ipv6 address ipv6-prefix/length | ipv6 dhcp-client [dhcp-distance number] [dhcp-rapid-comit])
mtu 1428
profile  number
no shutdown
```

## Create a Tunnel Interface

To configure an interface in VPN 0 to be a WAN transport connection, you must configure a tunnel interface on the cellular interface. The tunnel, which provides security from attacks, is used to send the phone number. At a minimum, select On and select a color for the interface, as described in the previous section. You can generally accept the system defaults for the remainder of the tunnel interface settings.

To configure a tunnel interface, select the Tunnel tab and configure the following parameters. Parameters marked with an asterisk are required to configure a cellular interface.

| Parameter Name | Description |
|---|---|
| Tunnel Interface* | Click On to create a tunnel interface. |
| Color* | Select a color for the TLOC. The color typically used for cellular interface tunnels is **lte** . |
| Control Connection | The default is On, which establishes a control connection for the TLOC. If the router has multiple TLOCs, click No to have a tunnel not establish a TLOC. |
| Maximum Control Connections | Set the maximum number of vSmart controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0.<br>*Range:* 0 through 8<br><br>*Default:* 2 |
| vBond As STUN Server | Click On to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the router is located behind a NAT. |
| Exclude Control Group List | Set the identifiers of one or more vSmart controller groups that this tunnel is not allows to establish control connections with.<br>*Range:* 0 through 100 |
| vManage Connection Preference | Set the preference for using the tunnel to exchange control traffic with the vManage NMS.<br>*Range:* 0 through 9<br>*Default:* 5 |
| Low-Bandwidth Link | Click On to set the tunnel interface as a low-bandwidth link. |
| Allow Service | Click On or Off for each service to allow or disallow the service on the cellular interface. |

To configure additional tunnel interface parameters, click Advanced Options and configure the following parameters:

| Parameter Name | Description |
|---|---|
| GRE | Use GRE encapsulation on the tunnel interface. By default, GRE is disabled.<br><br>If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation. |
| IPsec | Use IPsec encapsulation on the tunnel interface. By default, IPsec is enabled.<br><br>If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation. |

| | |
|---|---|
| IPsec Preference | Enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value.<br>*Range:* 0 through 4294967295<br>*Default:* 0 |
| IPsec Weight | Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel.<br>*Range:* 1 through 255<br>*Default:* 1 |
| Carrier | Select the carrier name or private network identifier to associate with the tunnel.<br>*Values:* carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default<br>*Default:* default |
| Bind Loopback Tunnel | Enter the name of a physical interface to bind to a loopback interface. The interface name has the format **ge** *slot* / *port* . |
| Last-Resort Circuit | Use the tunnel interface as the circuit of last resort |
| NAT Refresh Interval | Set the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection.<br>*Range:* 1 through 60 seconds<br>*Default:* 5 seconds |
| Hello Interval | Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection.<br>*Range:* 100 through 10000 milliseconds<br>*Default:* 1000 milliseconds (1 second) |
| Hello Tolerance | Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down.<br><br>*Range:* 12 through 60 seconds<br>*Default:* 12 seconds |

To save the feature template, click Save.

*CLI equivalent:*

```
vpn 0
  interface cellular0
    tunnel-interface
      allow-service service-name
      bind interface-name
      carrier carrier-name
      color color
      encapsulation (gre | ipsec)
        preference number
        weight number
      exclude-controller-group-list number
      hello-interval milliseconds
      hello-tolerance seconds
      hold-time milliseconds
      low-bandwidth-link
      max-control-connections number
      last-resort-circuit
      nat-refresh-interval seconds
      vbond-as-stun-server
      vmanage-connection-preference number
```

# Configure the Cellular Interface as a NAT Device

To configure a cellular interface to act as a NAT device for applications such as port forwarding, select the NAT tab, click On and configure the following parameters:

| Parameter Name | Description |
|---|---|
| NAT | Click On to have the interface act as a NAT device. |
| Refresh Mode | Select how NAT mappings are refreshed, either outbound or bidirectional (outbound and inbound).<br>*Default* : Outbound |
| UDP Timeout | Specify when NAT translations over UDP sessions time out.<br>*Range* : 1 through 65536 minutes<br>*Default* : 1 minutes |
| TCP Timeout | Specify when NAT translations over TCP sessions time out.<br>*Range* : 1 through 65536 minutes<br>*Default* : 60 minutes (1 hour) |
| Block ICMP | Select On to block inbound ICMP error messages. By default, a router acting as a NAT device receives these error messages.<br>*Default* : Off |
| Respond to Ping | Select On to have the router respond to ping requests to the NAT interface's IP address that are received from the public side of the connection. |

To create a port forwarding rule, click Add New Port Forwarding Rule and configure the following parameters. You can define up to 128 port-forwarding rules to allow requests from an external network to reach devices on the internal network.

| Parameter Name | Description |
|---|---|
| Port Start Range | Enter a port number to define the port or first port in the range of interest.<br>*Range:* 0 through 65535 |
| Port End Range | Enter the same port number to apply port forwarding to a single port, or enter a larger number to apply it to a range of ports.<br>*Range:* 0 through 65535 |
| Protocol | Select the protocol to which to apply the port-forwarding rule, either TCP or UDP. To match the same ports for both TCP and UDP traffic, configure two rules. |
| VPN | Specify the private VPN in which the internal server resides. This VPN is one of the VPN identifiers in the overlay network.<br>*Range:* 0 through 65530 |
| Private IP | Specify the IP address of the internal server to which to direct traffic that matches the port-forwarding rule. |

To save a port forwarding rule, click Add.

To save the feature template, click Save.

*CLI equivalent:*

```
vpn 0
  interface cellular0
    nat
      block-icmp-error
      port-forward port-start port-number1 port-end port-number2
        proto (tcp | udp) private-ip-address ip address private-vpn vpn-id
      refresh (bi-directional | outbound)
      respond-to-ping
      tcp-timeout minutes
      udp-timeout minutes
```

## Apply Access Lists

To configure a shaping rate to a cellular interface and to apply a QoS map, a rewrite rule, access lists, and policers to a router interface, select the ACL/QoS tab and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Shaping rate | Configure the aggreate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps). |
| QoS map | Specify the name of the QoS map to apply to packets being transmitted out the interface. |
| Rewrite rule | Click On, and specify the name of the rewrite rule to apply on the interface. |
| Ingress ACL – IPv4 | Click On, and specify the name of an IPv4 access list to packets being received on the interface. |
| Egress ACL– IPv4 | Click On, and specify the name of an IPv4 access list to packets being transmitted on the interface. |
| Ingress ACL – IPv6 | Click On, and specify the name of an IPv6 access list to packets being received on the interface. |
| Egress ACL– IPv6 | Click On, and specify the name of an IPv6 access list to packets being transmitted on the interface. |
| Ingress policer | Click On, and specify the name of the policer to apply to packets being received on the interface. |
| Egress policer | Click On, and specify the name of the policer to apply to packets being transmitted on the interface. |

To save the feature template, click Save.

*CLI equivalent:*

```
vpn 0
  interface cellular0
    access-list acl-name (in | out)
    ipv6 access-list acl-name (in | out)
    policer policer-name (in |out)
    qos-map name
    rewrite-rule name
    shaping-rate name
```

## Add ARP Table Entries

To configure static Address Resolution Protocol (ARP) table entries on the interface, select the ARP tab. Then click Add New ARP and configure the following parameters:

| Parameter Name | Description |
|---|---|
| IP Address | Enter the IP address for the ARP entry in dotted decimal notation or as a fully qualified host name. |
| MAC Address | Enter the MAC address in colon-separated hexadecimal notation. |

To save the ARP configuration, click Add.

To save the feature template, click Save.

*CLI equivalent:*

```
vpn vpn-id
  interface irbnumber
```

```
arp
  ip address ip-address mac mac-address
```

## Configure Other Interface Properties

To configure other interface properties, select the Advanced tab and configure the following parameters.

| Parameter Name | Description |
|---|---|
| PMTU Discovery | Click On to enable path MTU discovery on the interface, to allow the router to determine the largest MTU size supported without requiring packet fragmentation. |
| TCP MSS | Specify the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented.<br>*Range:* 552 to 1460 bytes<br>*Default:* None |
| Clear-Dont-Fragment | Click On to clear the Don't Fragment (DF) bit in the IPv4 packet header for packets being transmitted out the interface. When the DF bit is cleared, packets larger than that interface's MTU are fragmented before being sent. |
| Static Ingress QoS | Select a queue number to use for incoming traffic.<br>*Range:* 0 through 7 |
| ARP Timeout | Specify how long it takes for a dynamically learned ARP entry to time out.<br>*Range:* 0 through 2678400 seconds (744 hours)<br>*Default:* 1200 seconds (20 minutes) |
| Autonegotiate | Click Off to turn off autonegotiation. By default, an interface runs in autonegotiation mode. |
| TLOC Extension | Enter the name of a physical interface on the same router that connects to the WAN transport. This configuration then binds this service-side interface to the WAN transport. A second router at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN. |
| Tracker | Enter the name of a tracker to track the status of transport interfaces that connect to the internet. |
| ICMP Redirect | Click Disable to disable ICMP redirect messages on the interface. By default, an interface allows ICMP redirect messages. |

To save the feature template, click Save.

*CLI equivalent:*

```
vpn 0
  interface cellular0
    arp-timeout seconds
    [no] autonegotiate
    clear-dont-fragment
    icmp-redirect-disable
    mtu 1428
    pmtu
    static-ingress-qos number
    tcp-mss-adjust bytes
    tloc-extension interface-name
    tracker tracker-name
```

## Release Information

Introduced in vManage NMS in Release 16.1.
In Release 16.2, add circuit of last resort and its associated hold time.

In Release 16.3, add support for IPv6.
In Release 17.2.2, add support for tracker interface status.
In Release 18.2, add support for disabling ICMP redirect messages.

## VPN Interface DSL IPoE

Use the IPoE template for Cisco IOS XE routers.

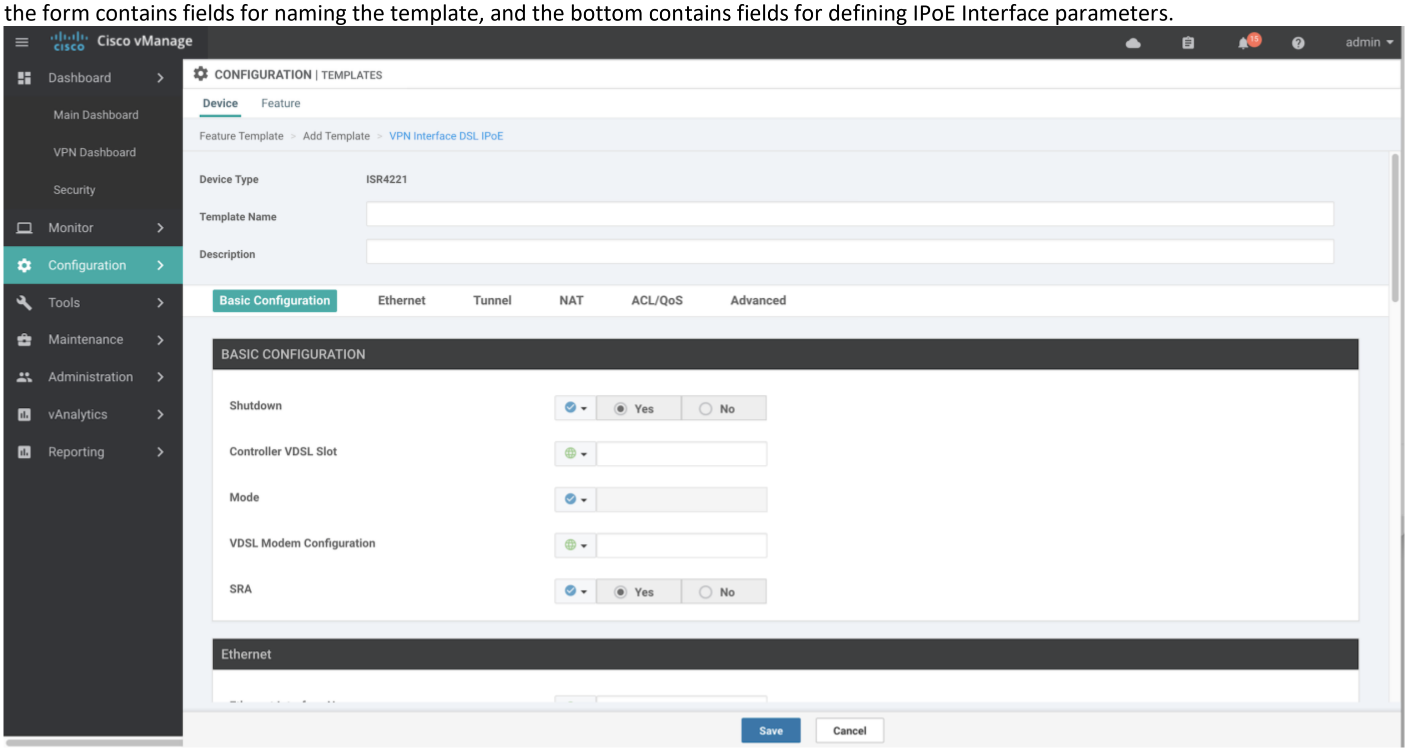
You configure IPoE on routers with DSL interfaces, to provide support for service provider digital subscriber line (DSL) functionality.

To configure DSL interfaces on Cisco routers using vManage templates:

1. Create a VPN Interface DSL IPoE feature template to configure IP-over-Ethernet interface parameters, as described in this article.
2. Create a VPN feature template to configure VPN parameters. See the VPN help topic.

## 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. Click the Transport & Management VPN tab located directly beneath the Description field, or scroll to the Transport & Management VPN section.
6. Under Additional VPN 0 Templates, located to the right of the screen, click VPN Interface DSL IPoE.
7. From the VPN Interface DSL IPoE drop-down, click Create Template. The VPN Interface DSL IPoE template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining IPoE Interface 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:

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

## Configure IPoE Functionality

To configure basic IPoE functionality, select the Basic Configuration tab and configure the following parameters. Required parameters are indicated with an asterisk.

| **Parameter Name** | **Description** |
|---|---|
| Shutdown* | Click No to enable the VDSL controller interface. |
| Controller VDSL Slot* | Enter the slot number of the controller VDSL interface, in the format *slot* / *subslot* / *port* (for example, 0/2/0). |
| Mode* | Select the operating mode of the VDSL controller from the drop-down:<br><br>• Auto—Default mode.<br><br>• ADSL1—Use ITU G.992.1 Annex A full-rate mode, which provides a downstream rate of 1.3 Mbps and an upstream rate of 1.8 Mbps.<br><br>• ADSL2—Use ITU G.992.3 Annex A, Annex L, and Annex M, which provides a downstream rate of 12 Mbps and an upstream rate of 1.3 Mbps.<br><br>• ADSL2+— Use ITU G.992.5 Annex A and Annex M, which provides a downstream rate of 24 Mbps and an upstream rate of 3.3 Mbps.<br><br>• ANSI—Operating in ADSL2/2+ mode, as defined in ITU G.991.1, G.992.3, and G992.5, Annex A and Annex M, and in VDSL2 mode, as defined in ITU-T G993.2.<br><br>• VDSL2—Operate in VDSL2 mode, as defined in ITU-T G.993.2, which uses frequencies of up to 30 MHz to provide a downstream rate of 200 Mbps and an upstream rate of 100 Mbps.. |

| | |
|---|---|
| VDSL Modem Configuration | Enter a command to send to the DSL modem in the NIM module. If the command is valid, it is executed and the results are returned to the vManage NMS. If the command is not valid, it is not executed. |
| SRA | Click Yes to enable seamless rate adaptation on the interface. SRA adjusts the line rate based on current line conditions. |

To save the feature template, click Save.

## Configure the Ethernet Interface

To configure an Ethernet interface on the VDSL controller, select the Ethernet tab and configure the following parameters. You must configure all parameters.

| Parameter Name | Description |
|---|---|
| Ethernet Interface Name | Enter a name for the Ethernet interface, in the format *subslot* / *port* (for example 2/0). You do not need to enter the slot number, because it must always be 0. |
| VLAN ID | Enter the VLAN identifier of the Ethernet interface. |
| Description | Enter a description for the interface. |
| Dynamic/Static | Assign a dynamic or static IPv4 address to the Ethernet interface. |
| IPv4 Address | Enter the static IPv4 address of the Ethernet interface. |
| DHCP Helper | Enter up to eight IP addresses for DHCP servers in the network, separated by commas, to have the interface be a DHCP helper. A DHCP helper interface forwards BOOTP (Broadcast) DHCP requests that it receives from the specified DHCP servers. |

To save the feature template, click Save.

## Create a Tunnel Interface

On IOS XE routers, you can configure up to four tunnel interfaces. This means that each router can have up to four TLOCs.

For the control plane to establish itself so that the overlay network can function, you must configure WAN transport interfaces in VPN 0.

To configure a tunnel interface for the multilink interface, select the Tunnel Interface tab and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Tunnel Interface | Click On to create a tunnel interface. |
| Color | Select a color for the TLOC. |
| Control Connection | If the router has multiple TLOCs, click No to have the tunnel not establish a TLOC. The default is On, which establishes a control connection for the TLOC. |
| Maximum Control Connections | Specify the maximum number of vSmart controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0.<br><br>*Range:* 0 through 8<br>*Default:* 2 |
| vBond As STUN Server | Click On to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the router is located behind a NAT. |

| | |
|---|---|
| Exclude Controller Group List | Set the vSmart controllers that the tunnel interface is not allowed to connect to.<br>*Range:* 0 through 100 |
| vManage Connection Preference | Set the preference for using a tunnel interface to exchange control traffic with the vManage NMS.<br>*Range:* 0 through 8<br>*Default:* 5 |
| Port Hop | Click On to enable port hopping, or click Off to disable it. When a router is behind a NAT, port hopping rotates through a pool of preselected OMP port numbers (called base ports) to establish DTLS connections with other routers 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.<br>*Default:* Enabled |
| Low-Bandwidth Link | Select to characterize the tunnel interface as a low-bandwidth link. |
| Allow Service | Select On or Off for each service to allow or disallow the service on the interface. |

To configure additional tunnel interface parameters, click Advanced Options and configure the following parameters:

| Parameter Name | Description |
|---|---|
| GRE | Use GRE encapsulation on the tunnel interface. By default, GRE is disabled.<br><br>If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation. |
| IPsec | Use IPsec encapsulation on the tunnel interface. By default, IPsec is enabled.<br><br>If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation. |
| IPsec Preference | Specify a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value.<br><br>*Range:* 0 through 4294967295<br>*Default:* 0 |
| IPsec Weight | Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel.<br><br>*Range:* 1 through 255<br>*Default:* 1 |
| Carrier | Select the carrier name or private network identifier to associate with the tunnel.<br><br>*Values:* carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default<br>*Default:* default |
| Bind Loopback Tunnel | Enter the name of a physical interface to bind to a loopback interface. |
| Last-Resort Circuit | Select to use the tunnel interface as the circuit of last resort. |
| NAT Refresh Interval | Enter the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection.<br>*Range:* 1 through 60 seconds<br>*Default:* 5 seconds |
| Hello Interval | Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection.<br>*Range:* 100 through 10000 milliseconds<br>*Default:* 1000 milliseconds (1 second) |

| | |
|---|---|
| Hello Tolerance | Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down.<br><br>*Range:* 12 through 60 seconds<br>*Default:* 12 seconds |

## Configure the Interface as a NAT Device

To configure an interface to act as a NAT device for applications such as port forwarding, select the NAT tab, click On and configure the following parameters:

| Parameter Name | Description |
|---|---|
| NAT | Click On to have the interface act as a NAT device. |
| Refresh Mode | Select how NAT mappings are refreshed, either outbound or bidirectional (outbound and inbound).<br>*Default* : Outbound |
| UDP Timeout | Specify when NAT translations over UDP sessions time out.<br>*Range* : 1 through 65536 minutes<br>*Default* : 1 minutes |
| TCP Timeout | Specify when NAT translations over TCP sessions time out.<br>*Range* : 1 through 65536 minutes<br>*Default* : 60 minutes (1 hour) |
| Block ICMP | Select On to block inbound ICMP error messages. By default, a router acting as a NAT device receives these error messages.<br>*Default* : Off |
| Respond to Ping | Select On to have the router respond to ping requests to the NAT interface's IP address that are received from the public side of the connection. |

To create a port forwarding rule, click Add New Port Forwarding Rule and configure the following parameters. You can define up to 128 port-forwarding rules to allow requests from an external network to reach devices on the internal network.

| Parameter Name | Description |
|---|---|
| Port Start Range | Enter a port number to define the port or first port in the range of interest.<br>*Range:* 0 through 65535 |
| Port End Range | Enter the same port number to apply port forwarding to a single port, or enter a larger number to apply it to a range of ports.<br>*Range:* 0 through 65535 |
| Protocol | Select the protocol to which to apply the port-forwarding rule, either TCP or UDP. To match the same ports for both TCP and UDP traffic, configure two rules. |
| VPN | Specify the private VPN in which the internal server resides. This VPN is one of the VPN identifiers in the overlay network.<br>*Range:* 0 through 65530 |
| Private IP | Specify the IP address of the internal server to which to direct traffic that matches the port-forwarding rule. |

To save a port forwarding rule, click Add.

To save the feature template, click Save.

## Apply Access Lists

To apply a rewrite rule, access lists, and policers to a router interface, select the ACL tab and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Shaping rate | Configure the aggreate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps). |
| QoS map | Specify the name of the QoS map to apply to packets being transmitted out the interface. |
| Rewrite Rule | Click On, and specify the name of the rewrite rule to apply on the interface. |
| Ingress ACL – IPv4 | Click On, and specify the name of the access list to apply to IPv4 packets being received on the interface. |
| Egress ACL – IPv4 | Click On, and specify the name of the access list to apply to IPv4 packets being transmitted on the interface. |
| Ingress ACL – IPv6 | Click On, and specify the name of the access list to apply to IPv6 packets being received on the interface. |
| Egress ACL – IPv6 | Click On, and specify the name of the access list to apply to IPv6 packets being transmitted on the interface. |
| Ingress Policer | Click On, and specify the name of the policer to apply to packets being received on the interface. |
| Egress Policer | Click On, and specify the name of the policer to apply to packets being transmitted on the interface. |

To save the feature template, click Save.

## Configure Other Interface Properties

To configure other interface properties, select the Advanced tab and configure the following properties:

| Parameter Name | Description |
|---|---|
| Bandwidth Upstream | For transmitted traffic, set the bandwidth above which to generate notifications.<br>*Range:* 1 through ($2^{32}$ / 2) – 1 kbps |
| Bandwidth Downstream | For received traffic, set the bandwidth above which to generate notifications.<br>*Range:* 1 through ($2^{32}$ / 2) – 1 kbps |
| IP MTU | Specify the maximum MTU size of packets on the interface.<br>*Range:* 576 through 1804<br>*Default:* 1500 bytes |
| TCP MSS | Specify the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented.<br>*Range:* 552 to 1460 bytes<br>*Default:* None |
| TLOC Extension | Enter the name of the physical interface on the same router that connects to the WAN transport circuit. This configuration then binds this service-side interface to the WAN transport. A second router at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN. |
| Tracker | Enter the name of a tracker to track the status of transport interfaces that connect to the internet. |
| IP Directed-Broadcast | Enables translation of a directed broadcast to physical broadcasts. An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet but which originates from a node that is not itself part of that destination subnet. |

To save the feature template, click Save.

## Release Information

Introduced in vManage NMS in Release 18.4.1.

## VPN Interface DSL PPPoA

Use the VPN Interface DSL PPPoA template for Cisco IOS XE routers.

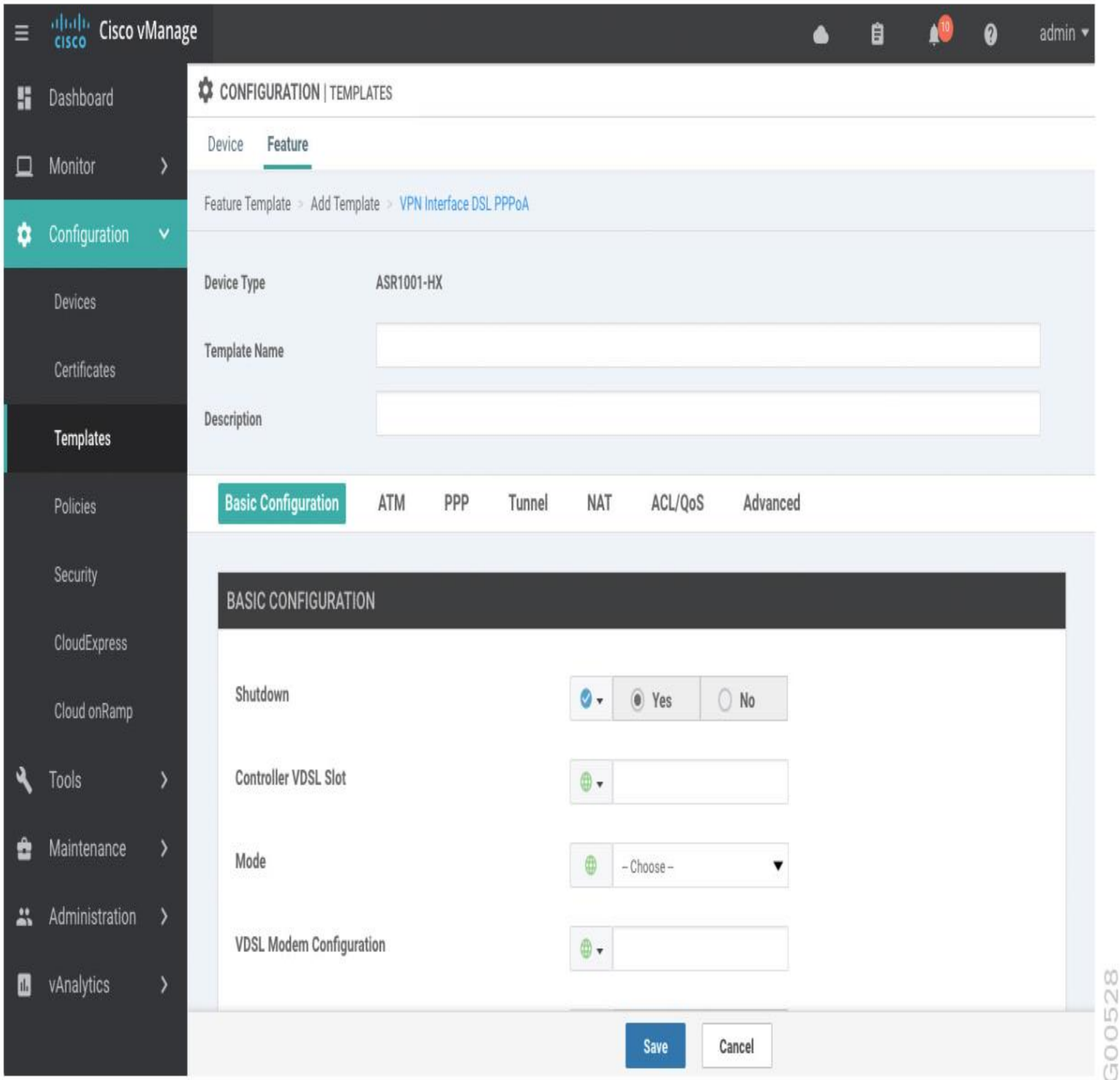
You configure PPP-over-ATM interfaces on routers with DSL NIM modules, to provide support for service provider digital subscriber line (DSL) functionality.

To configure DSL interfaces on Cisco routers using vManage templates:

1. Create a VPN Interface DSL PPPoA feature template to configure ATM interface parameters, as described in this article.
2. Create a VPN feature template to configure VPN parameters. See the VPN help topic.

## 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. Click the Transport & Management VPN tab located directly beneath the Description field, or scroll to the Transport & Management VPN section.
6. Under Additional VPN 0 Templates, located to the right of the screen, click VPN Interface DSL PPPoA.
7. From the VPN Interface DSL PPPoA drop-down, click Create Template. The VPN Interface DSL PPPoA template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN Interface PPP 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:

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

## Configure VDSL Controller Functionality

To configure basic VDSL controller functionality in a VPN, select the Basic Configuration tab and configure the following parameters. Required parameters are indicated with an asterisk.

| Parameter Name | Description |
|---|---|
| Shutdown* | Click No to enable the VDSL controller interface. |
| Controller VDSL Slot* | Enter the slot number of the controller VDSL interface, in the format *slot* / *subslot* / *port* (for example, 0/2/0). |
| Mode* | Select the operating mode of the VDSL controller from the drop-down:<br>• Auto—Default mode.<br>• ADSL1—Use ITU G.992.1 Annex A full-rate mode, which provides a downstream rate of 1.3 Mbps and an upstream rate of 1.8 Mbps.<br>• ADSL2—Use ITU G.992.3 Annex A, Annex L, and Annex M, which provides a downstream rate of 12 Mbps and an upstream rate of 1.3 Mbps.<br>• ADSL2+— Use ITU G.992.5 Annex A and Annex M, which provides a downstream rate of 24 Mbps and an upstream rate of 3.3 Mbps.<br>• ANSI—Operate in ADSL2/2+ mode, as defined in ITU G.991.1, G.992.3, and G992.5, Annex A and Annex M, and in VDSL2 mode, as defined in ITU-T G993.2.<br>• VDSL2—Operate in VDSL2 mode, as defined in ITU-T G.993.2, which uses frequencies of up to 30 MHz to provide a downstream rate of 200 Mbps and an upstream rate of 100 Mbps. |
| VDSL Modem Configuration | Enter a command to send to the DSL modem in the NIM module. If the command is valid, it is executed and the results are returned to the vManage NMS. If the command is not valid, it is not executed. |
| SRA | Enabled by default. Click No to disable seamless rate adaptation on the interface. SRA adjusts the line rate based on current line conditions. |

To save the feature template, click Save.

## Configure the ATM Interface

To configure an ATM interface on the VDSL controller, select the ATM tab and configure the following parameters. You must configure all parameters.

| Parameter Name | Description |
|---|---|
| ATM Interface Name | Enter a name for the ATM interface, in the format *subslot* / *port* (for example 2/0). You do not need to enter the slot number, because it must always be 0. |
| Description | Enter a description for the interface. |
| VPI and VCI | Create an ATM permanent virtual circuit (PVC), in the format *vpi* / *vci* , Enter values for the virtual path identifier (VPI) and the virtual channel identifier (VCI). |
| Encapsulation | Select the ATM adaptation layer (AAL) and encapsulation type to use on the ATM PVC from the drop-down:<br>• AAL5 MUX—Dedicate the PVC to a single protocol.<br>• AAL5 NLPID—Use NLPID multiplexing.<br>• AAL5 SNAP—Multiplex two or more protocols on the same PVC. |
| Dialer Pool Member | Enter the number of the dialer pool to which the interface belongs. It can be a value from 1 through 255. |
| VBR-NRT | Configure variable bit rate non-real-time parameters:<br>• Peak Cell Rate—Enter a value from 48 through 25000 Kbps.<br>• Sustainable Cell Rate—Enter the sustainable cell rate, in Kbps.<br>• Maximum Burst Size—This size can be 1 cell. |
| VBR-RT | Configure variable bit rate real-time parameters:<br>• Peak Cell Rate—Enter a value from 48 through 25000 Kbps.<br>• Average Cell Rate—Enter the average cell rate, in Kpbs.<br>• Maximum Burst Size—This size can be 1 cell. |

To save the feature template, click Save.

## Configure the PPP Authentication Protocol

To configure the PPP authentication protocol, select the PPP tab and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Authentication Protocol | Select the authentication protocol used by the MLP:<br>• CHAP—Enter the hostname and password provided by your Internet Service Provider (ISP). *hostname* can be up to 255 characters.<br>• PAP—Enter the username and password provided by your ISP. *username* can be up to 255 characters.<br>• PAP and CHAP—Configure both authentication protocols. Enter the login credentials for each protocol. To use the same username and password for both, click Same Credentials for PAP and CHAP. |

To save the feature template, click Save.

## Create a Tunnel Interface

On vEdge routers, you can configure up to four tunnel interfaces. This means that each vEdge router can have up to four TLOCs.

For the control plane to establish itself so that the overlay network can function, you must configure WAN transport interfaces in VPN 0.

To configure a tunnel interface for the multilink interface, select the Tunnel Interface tab and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Tunnel Interface | Click On to create a tunnel interface. |
| Color | Select a color for the TLOC. |
| Control Connection | If the vEdge router has multiple TLOCs, click No to have the tunnel not establish a TLOC. The default is On, which establishes a control connection for the TLOC. |
| Maximum Control Connections | Specify the maximum number of vSmart controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0.<br><br>*Range:* 0 through 8<br>*Default:* 2 |
| vBond As STUN Server | Click On to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the vEdge router is located behind a NAT. |
| Exclude Controller Group List | Set the vSmart controllers that the tunnel interface is not allowed to connect to.<br>*Range:* 0 through 100 |
| vManage Connection Preference | Set the preference for using a tunnel interface to exchange control traffic with the vManage NMS.<br>*Range:* 0 through 8<br>*Default:* 5 |
| Port Hop | Click On to enable port hopping, or click Off to disable it. When a router is behind a NAT, port hopping rotates through a pool of preselected OMP port numbers (called base ports) to establish DTLS connections with other routers 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.<br>*Default:* Enabled |
| Low-Bandwidth Link | Select to characterize the tunnel interface as a low-bandwidth link. |
| Allow Service | Select On or Off for each service to allow or disallow the service on the interface. |

To configure additional tunnel interface parameters, click Advanced Options and configure the following parameters:

| Parameter Name | Description |
|---|---|
| GRE | Use GRE encapsulation on the tunnel interface. By default, GRE is disabled.<br><br>If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation. |
| IPsec | Use IPsec encapsulation on the tunnel interface. By default, IPsec is enabled.<br><br>If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation. |

| | |
|---|---|
| IPsec Preference | Specify a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value.<br><br>*Range:* 0 through 4294967295<br>*Default:* 0 |
| IPsec Weight | Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel.<br><br>*Range:* 1 through 255<br>*Default:* 1 |
| Carrier | Select the carrier name or private network identifier to associate with the tunnel.<br><br>*Values:* carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default<br>*Default:* default |
| Bind Loopback Tunnel | Enter the name of a physical interface to bind to a loopback interface. |
| Last-Resort Circuit | Select to use the tunnel interface as the circuit of last resort. |
| NAT Refresh Interval | Enter the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection.<br>*Range:* 1 through 60 seconds<br>*Default:* 5 seconds |
| Hello Interval | Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection.<br>*Range:* 100 through 10000 milliseconds<br>*Default:* 1000 milliseconds (1 second) |
| Hello Tolerance | Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down.<br><br>*Range:* 12 through 60 seconds<br>*Default:* 12 seconds |

## Apply Access Lists

To apply a rewrite rule, access lists, and policers to a router interface, select the ACL tab and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Shaping rate | Configure the aggreate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps). |
| QoS map | Specify the name of the QoS map to apply to packets being transmitted out the interface. |
| Rewrite Rule | Click On, and specify the name of the rewrite rule to apply on the interface. |
| Ingress ACL – IPv4 | Click On, and specify the name of the access list to apply to IPv4 packets being received on the interface. |
| Egress ACL – IPv4 | Click On, and specify the name of the access list to apply to IPv4 packets being transmitted on the interface. |
| Ingress ACL – IPv6 | Click On, and specify the name of the access list to apply to IPv6 packets being received on the interface. |
| Egress ACL – IPv6 | Click On, and specify the name of the access list to apply to IPv6 packets being transmitted on the interface. |
| Ingress Policer | Click On, and specify the name of the policer to apply to packets being received on the interface. |

| | |
|---|---|
| Egress Policer | Click On, and specify the name of the policer to apply to packets being transmitted on the interface. |

To save the feature template, click Save.

## Configure Other Interface Properties

To configure other interface properties, select the Advanced tab and configure the following properties:

| Parameter Name | Description |
|---|---|
| PMTU Discovery | Click On to enable path MTU discovery on the interface, to allow the router to determine the largest MTU size supported without requiring packet fragmentation. |
| TCP MSS | Specify the maximum segment size (MSS) of TPC SYN packets passing through the vEdge router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented.<br>*Range:* 552 to 1460 bytes<br>*Default:* None |
| Clear Dont Fragment | Click On to clear the Don't Fragment bit in the IPv4 packet header for packets being transmitted out the interface. When the DF bit is cleared, packets larger than that interface's MTU are fragmented before being sent. |
| Static Ingress QoS | Select a queue number to use for incoming traffic.<br>*Range: 0 through 7* |
| Autonegotiate | Click Off to turn off autonegotiation. By default, an interface runs in autonegotiation mode. |
| TLOC Extension | Enter the name of the physical interface on the same router that connects to the WAN transport circuit. This configuration then binds this service-side interface to the WAN transport. A second vEdge router at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN. |

To save the feature template, click Save.

## Release Information

Introduced in vManage NMS in Release 18.3.

## VPN Interface DSL PPPoE

Use the VPN Interface DSL PPPoE template for Cisco IOS XE routers.

You configure PPP-over-Ethernet interfaces on routers with DSL NIM modules, to provide support for service provider digital subscriber line (DSL) functionality.

To configure DSL interfaces on Cisco routers using vManage templates:

1. Create a VPN Interface DSL PPPoE feature template to configure PPP-over-Ethernet interface parameters, as described in this article.
2. Create a VPN feature template to configure VPN parameters. See the VPN help topic.

## 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.

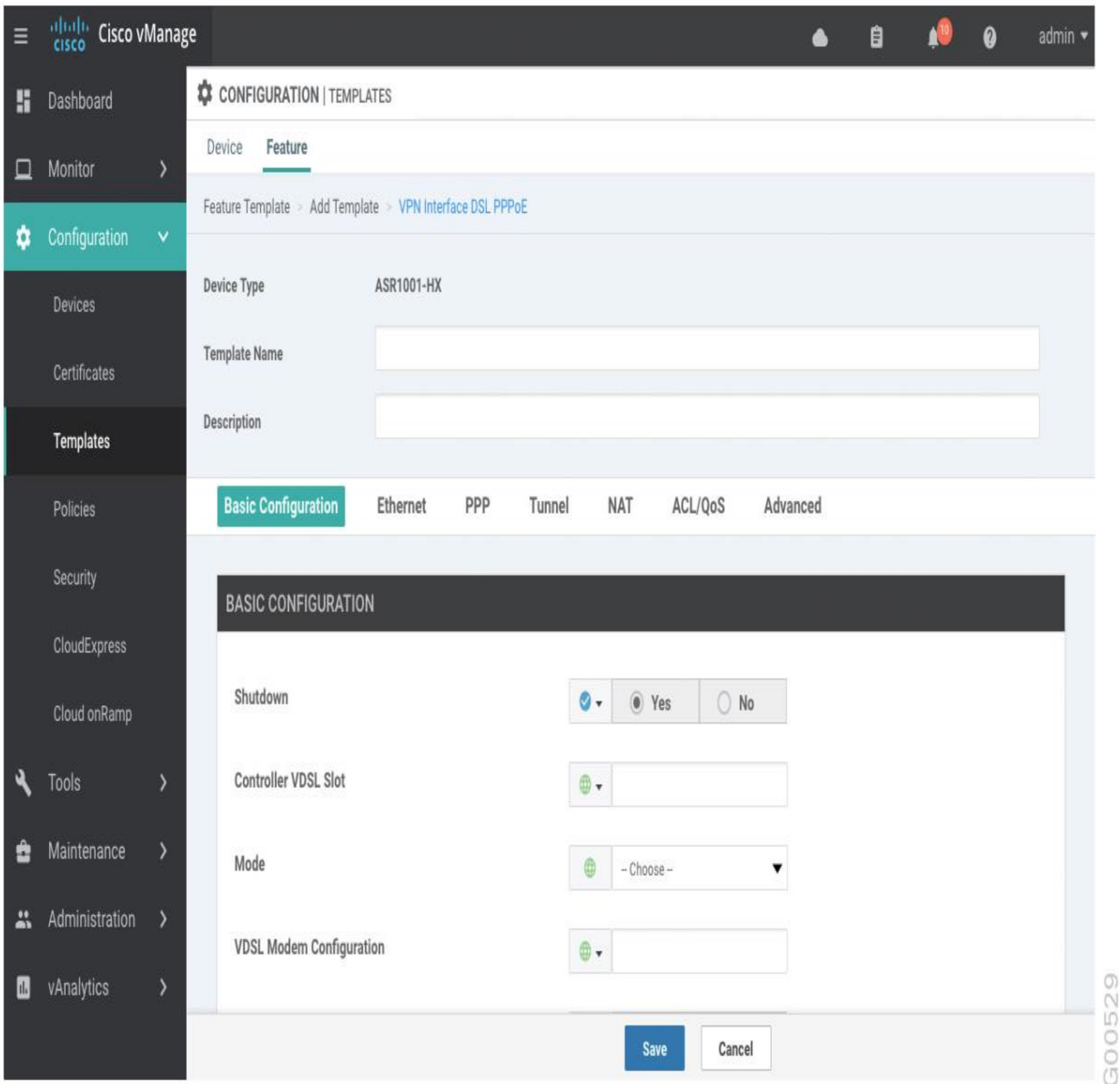
3. From the Create Template drop-down, select From Feature Template.

4. From the Device Model drop-down, select the type of device for which you are creating the template.

5. Click the Transport & Management VPN tab located directly beneath the Description field, or scroll to the Transport & Management VPN section.

6. Under Additional VPN 0 Templates, located to the right of the screen, click VPN Interface DSL PPPoE.

7. From the VPN Interface DSL PPPoE drop-down, click Create Template. The VPN Interface DSL PPPoE template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining PPPoE Interface 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:

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

## Configure VDSL Controller Functionality

To configure basic VDSL controller functionality in a VPN, select the Basic Configuration tab and configure the following parameters. Required parameters are indicated with an asterisk.

| **Parameter Name** | **Description** |
|---|---|
| Shutdown* | Click No to enable the VDSL controller interface. |
| Controller VDSL Slot* | Enter the slot number of the controller VDSL interface, in the format *slot* / *subslot* / *port* (for example, 0/2/0). |
| Mode* | Select the operating mode of the VDSL controller from the drop-down:<br><br>• Auto—Default mode.<br><br>• ADSL1—Use ITU G.992.1 Annex A full-rate mode, which provides a downstream rate of 1.3 Mbps and an upstream rate of 1.8 Mbps.<br><br>• ADSL2—Use ITU G.992.3 Annex A, Annex L, and Annex M, which provides a downstream rate of 12 Mbps and an upstream rate of 1.3 Mbps.<br><br>• ADSL2+— Use ITU G.992.5 Annex A and Annex M, which provides a downstream rate of 24 Mbps and an upstream rate of 3.3 Mbps.<br><br>• ANSI—Operating in ADSL2/2+ mode, as defined in ITU G.991.1, G.992.3, and G992.5, Annex A and Annex M, and in VDSL2 mode, as defined in ITU-T G993.2.<br><br>• VDSL2—Operate in VDSL2 mode, as defined in ITU-T G.993.2, which uses frequencies of up to 30 MHz to provide a downstream rate of 200 Mbps and an upstream rate of 100 Mbps.. |
| VDSL Modem Configuration | Enter a command to send to the DSL modem in the NIM module. If the command is valid, it is executed and the results are returned to the vManage NMS. If the command is not valid, it is not executed. |

| | |
|---|---|
| SRA | Click Yes to enable seamless rate adaptation on the interface. SRA adjusts the line rate based on current line conditions. |

To save the feature template, click Save.

## Configure the Ethernet Interface

To configure an Ethernet interface on the VDSL controller, select the Ethernet tab and configure the following parameters. You must configure all parameters.

| Parameter Name | Description |
|---|---|
| Ethernet Interface Name | Enter a name for the Ethernet interface, in the format *subslot* / *port* (for example 2/0). You do not need to enter the slot number, because it must always be 0. |
| VLAN ID | Enter the VLAN identifier of the Ethernet interface. |
| Description | Enter a description for the interface. |
| Dialer Pool Member | Enter the number of the dialer pool to which the interface belongs. It can be a value from 1 through 255. |
| PPP Max Payload | Enter the maximum receive unit (MRU) value to be negotiated during PPP Link Control Protocol (LCP) negotiation.<br>*Range:* 64 through 1792 bytes |
| Dialer IP | Configure the IP prefix of the dialer interface. This prefix is that of the node in the destination that the interface calls.<br>• Negotiated—Use the address that is obtained during IPCP negotiation. |

To save the feature template, click Save.

## Configure the PPP Authentication Protocol

To configure the PPP authentication protocol, select the PPP tab and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Authentication Protocol | Select the authentication protocol used by the MLP:<br>• CHAP—Enter the hostname and password provided by your Internet Service Provider (ISP). *hostname* can be up to 255 characters.<br>• PAP—Enter the username and password provided by your ISP. *username* can be up to 255 characters.<br>• PAP and CHAP—Configure both authentication protocols. Enter the login credentials for each protocol. To use the same username and password for both, click Same Credentials for PAP and CHAP. |

To save the feature template, click Save.

## Create a Tunnel Interface

On IOS XE routers, you can configure up to four tunnel interfaces. This means that each router can have up to four TLOCs.

For the control plane to establish itself so that the overlay network can function, you must configure WAN transport interfaces in VPN 0.

To configure a tunnel interface for the multilink interface, select the Tunnel Interface tab and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Tunnel Interface | Click On to create a tunnel interface. |

| | |
|---|---|
| Color | Select a color for the TLOC. |
| Control Connection | If the router has multiple TLOCs, click No to have the tunnel not establish a TLOC. The default is On, which establishes a control connection for the TLOC. |
| Maximum Control Connections | Specify the maximum number of vSmart controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0.<br><br>*Range:* 0 through 8<br>*Default:* 2 |
| vBond As STUN Server | Click On to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the router is located behind a NAT. |
| Exclude Controller Group List | Set the vSmart controllers that the tunnel interface is not allowed to connect to.<br>*Range:* 0 through 100 |
| vManage Connection Preference | Set the preference for using a tunnel interface to exchange control traffic with the vManage NMS.<br>*Range:* 0 through 8<br>*Default:* 5 |
| Port Hop | Click On to enable port hopping, or click Off to disable it. When a router is behind a NAT, port hopping rotates through a pool of preselected OMP port numbers (called base ports) to establish DTLS connections with other routers 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.<br>*Default:* Enabled |
| Low-Bandwidth Link | Select to characterize the tunnel interface as a low-bandwidth link. |
| Allow Service | Select On or Off for each service to allow or disallow the service on the interface. |

To configure additional tunnel interface parameters, click Advanced Options and configure the following parameters:

| Parameter Name | Description |
|---|---|
| GRE | Use GRE encapsulation on the tunnel interface. By default, GRE is disabled.<br><br>If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation. |
| IPsec | Use IPsec encapsulation on the tunnel interface. By default, IPsec is enabled.<br><br>If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation. |
| IPsec Preference | Specify a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value.<br><br>*Range:* 0 through 4294967295<br>*Default:* 0 |
| IPsec Weight | Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel.<br><br>*Range:* 1 through 255<br>*Default:* 1 |
| Carrier | Select the carrier name or private network identifier to associate with the tunnel.<br><br>*Values:* carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default<br>*Default:* default |

| | |
|---|---|
| Bind Loopback Tunnel | Enter the name of a physical interface to bind to a loopback interface. |
| Last-Resort Circuit | Select to use the tunnel interface as the circuit of last resort. |
| NAT Refresh Interval | Enter the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection.<br>*Range:* 1 through 60 seconds<br>*Default:* 5 seconds |
| Hello Interval | Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection.<br>*Range:* 100 through 10000 milliseconds<br>*Default:* 1000 milliseconds (1 second) |
| Hello Tolerance | Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down.<br><br>*Range:* 12 through 60 seconds<br>*Default:* 12 seconds |

## Configure the Interface as a NAT Device

To configure an interface to act as a NAT device for applications such as port forwarding, select the NAT tab, click On and configure the following parameters:

| Parameter Name | Description |
|---|---|
| NAT | Click On to have the interface act as a NAT device. |
| Refresh Mode | Select how NAT mappings are refreshed, either outbound or bidirectional (outbound and inbound).<br>*Default* : Outbound |
| UDP Timeout | Specify when NAT translations over UDP sessions time out.<br>*Range* : 1 through 65536 minutes<br>*Default* : 1 minutes |
| TCP Timeout | Specify when NAT translations over TCP sessions time out.<br>*Range* : 1 through 65536 minutes<br>*Default* : 60 minutes (1 hour) |
| Block ICMP | Select On to block inbound ICMP error messages. By default, a router acting as a NAT device receives these error messages.<br>*Default* : Off |
| Respond to Ping | Select On to have the router respond to ping requests to the NAT interface's IP address that are received from the public side of the connection. |

To create a port forwarding rule, click Add New Port Forwarding Rule and configure the following parameters. You can define up to 128 port-forwarding rules to allow requests from an external network to reach devices on the internal network.

| Parameter Name | Description |
|---|---|
| Port Start Range | Enter a port number to define the port or first port in the range of interest.<br>*Range:* 0 through 65535 |
| Port End Range | Enter the same port number to apply port forwarding to a single port, or enter a larger number to apply it to a range of ports.<br>*Range:* 0 through 65535 |

| | |
|---|---|
| Protocol | Select the protocol to which to apply the port-forwarding rule, either TCP or UDP. To match the same ports for both TCP and UDP traffic, configure two rules. |
| VPN | Specify the private VPN in which the internal server resides. This VPN is one of the VPN identifiers in the overlay network.<br>*Range:* 0 through 65530 |
| Private IP | Specify the IP address of the internal server to which to direct traffic that matches the port-forwarding rule. |

To save a port forwarding rule, click Add.

To save the feature template, click Save.

## Apply Access Lists

To apply a rewrite rule, access lists, and policers to a router interface, select the ACL tab and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Shaping rate | Configure the aggregate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps). |
| QoS map | Specify the name of the QoS map to apply to packets being transmitted out the interface. |
| Rewrite Rule | Click On, and specify the name of the rewrite rule to apply on the interface. |
| Ingress ACL – IPv4 | Click On, and specify the name of the access list to apply to IPv4 packets being received on the interface. |
| Egress ACL – IPv4 | Click On, and specify the name of the access list to apply to IPv4 packets being transmitted on the interface. |
| Ingress ACL – IPv6 | Click On, and specify the name of the access list to apply to IPv6 packets being received on the interface. |
| Egress ACL – IPv6 | Click On, and specify the name of the access list to apply to IPv6 packets being transmitted on the interface. |
| Ingress Policer | Click On, and specify the name of the policer to apply to packets being received on the interface. |
| Egress Policer | Click On, and specify the name of the policer to apply to packets being transmitted on the interface. |

To save the feature template, click Save.

## Configure Other Interface Properties

To configure other interface properties, select the Advanced tab and configure the following properties:

| Parameter Name | Description |
|---|---|
| Bandwidth Upstream | For transmitted traffic, set the bandwidth above which to generate notifications.<br>*Range:* 1 through $(2^{32} / 2) - 1$ kbps |
| Bandwidth Downstream | For received traffic, set the bandwidth above which to generate notifications.<br>*Range:* 1 through $(2^{32} / 2) - 1$ kbps |
| IP MTU | Specify the maximum MTU size of packets on the interface.<br>*Range:* 576 through 1804<br>*Default:* 1500 bytes |

| | |
|---|---|
| TCP MSS | Specify the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented.<br>*Range:* 552 to 1460 bytes<br>*Default:* None |
| Clear Dont Fragment | Click On to clear the Don't Fragment bit in the IPv4 packet header for packets being transmitted out the interface. When the DF bit is cleared, packets larger than that interface's MTU are fragmented before being sent. |
| TLOC Extension | Enter the name of the physical interface on the same router that connects to the WAN transport circuit. This configuration then binds this service-side interface to the WAN transport. A second router at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN. |
| Tracker | Enter the name of a tracker to track the status of transport interfaces that connect to the internet. |

To save the feature template, click Save.

## Release Information

Introduced in vManage NMS in Release 18.3.

## VPN Interface Ethernet

Use the VPN Interface Ethernet template for all Viptela devices and Cisco IOS XE routers running the SD-WAN software.

To configure the Ethernet interfaces in a VPN using vManage templates:

1. Create a VPN Interface Ethernet feature template to configure Ethernet interface parameters, as described in this article.
2. Create a VPN feature template to configure VPN parameters. See the VPN help topic.
3. Optionally, on vEdge routers, to enable DHCP server functionality on the interface, create a DHCP Server feature template. See the DHCP Server help topic.

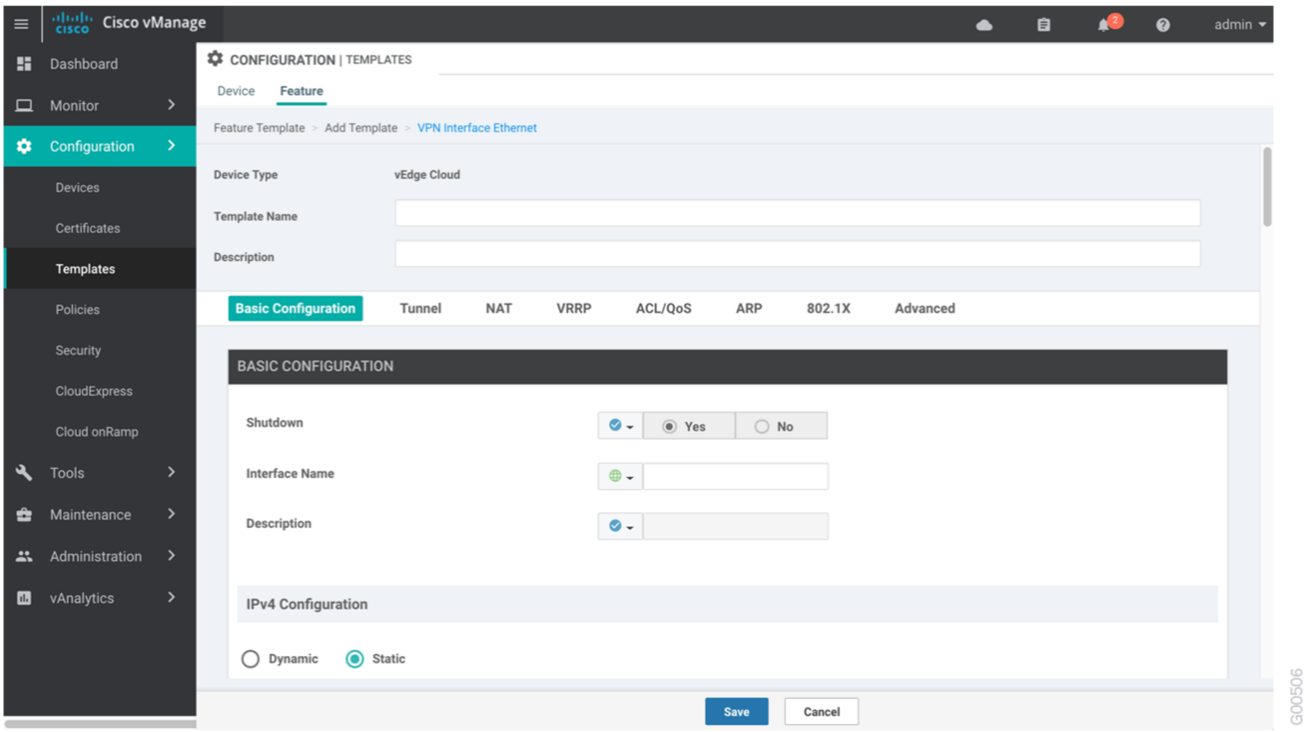
## Navigate to the Template Screen and Name the Template

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 template for VPN 0 or VPN 512:
   a. Click the Transport & Management VPN tab located directly beneath the Description field, or scroll to the Transport & Management VPN section.
   b. Under Additional VPN 0 Templates, located to the right of the screen, click VPN Interface.
   c. From the VPN Interface drop-down, click Create Template. The VPN Interface Ethernet template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN Interface Ethernet parameters.
6. To create a template for VPNs 1 through 511, and 513 through 65530:
   a. Click the Service VPN tab located directly beneath the Description field, or scroll to the Service VPN section.

b. Click the Service VPN drop-down.

c. Under Additional VPN templates, located to the right of the screen, click VPN Interface.

d. From the VPN Interface drop-down, click Create Template. The VPN Interface Ethernet template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN Interface Ethernet 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 and select one of the following:

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

## Configure Basic Interface Functionality

To configure basic interface functionality in a VPN, select the Basic Configuration tab and configure the following parameters. Parameters marked with an asterisk are required to configure an interface.

| Parameter Name | Description |
|---|---|
| Shutdown* | Click No to enable the interface. |
| Interface name* | Enter a name for the interface.<br><br>For IOS XE routers, you must spell out the interface names completely (for example, **GigabitEthernet0/0/0** ), and you must configure all the router's interfaces even if you are not using them so that they are configured in the shutdown state and so that all default values for them are configured. |
| Description | Enter a description for the interface. |
| IPv4 Configuration* | To configure a static address, click Static and enter an IPv4 address.<br><br>To set the interface as a DHCP client so that the interface to receive its IP address from a DHCP server, click Dynamic. You can optionally set the DHCP distance to specify the administrative distance of routes learned from a DHCP server. The default DHCP distance is 1. |
| IPv6 Address* | To configure a static address for an interface in VPN 0, click Static and enter an IPv6 address.<br><br>To set the interface as a DHCP client so that the interface to receive its IP address from a DHCP server, click Dynamic. You can optionally set the DHCP distance to specify the administrative distance of routes learned from a DHCP server. The default DHCP distance is 1. You can optionally enable DHCP rapid commit, to speed up the assignment of IP addresses. |
| DHCP Helper (on vEdge routers) | Enter up to eight IP addresses for DHCP servers in the network, separated by commas, to have the interface be a DHCP helper. A DHCP helper interface forwards BOOTP (Broadcast) DHCP requests that it receives from the specified DHCP servers. |
| Block Non-Source IP (on vEdge routers) | Click Yes to have the interface forward traffic only if the source IP address of the traffic matches the interface's IP prefix range. |
| Bandwidth Upstream (on vEdge routers and vManage NMSs) | For transmitted traffic, set the bandwidth above which to generate notifications.<br>*Range:* 1 through ($2^{32}$ / 2) – 1 kbps |

| | |
|---|---|
| Bandwidth Downstream (on vEdge routers and vManage NMSs) | For received traffic, set the bandwidth above which to generate notifications.<br>*Range:* 1 through ($2^{32}$ / 2) – 1 kbps |
| Secondary IP Address (on vEdge routers) | Click Add to configure up to four secondary IPv4 addresses for a service-side interface. |

To save the feature template, click Save.

*CLI equivalent:*

```
vpn vpn-id
  interface interface-name
    bandwidth-downstream kbps
    bandwidth-upstream kbps
    block-non-source-ip
    description text
    dhcp-helper ip-address (on vEdge routers only)
    (ip address ipv4-prefix/length| ip dhcp-client [dhcp-distance number])
    (ipv6 address ipv6-prefix/length | ipv6 dhcp-client [dhcp-distance number] [dhcp-rapid-commit])
    secondary-address ipv4-address
    [no] shutdown
```

## Create a Tunnel Interface

On vEdge routers, you can configure up to four tunnel interfaces. This means that each vEdge router can have up to four TLOCs.

On vSmart controllers and vManage NMSs, you can configure one tunnel interface.

For the control plane to establish itself so that the overlay network can function, you must configure WAN transport interfaces in VPN 0.

To configure a tunnel interface, select the Interface Tunnel tab and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Tunnel Interface | Click On to create a tunnel interface. |
| Color | Select a color for the TLOC. |
| Control Connection (on vEdge routers) | If the vEdge router has multiple TLOCs, click No to have the tunnel not establish a TLOC. The default is On, which establishes a control connection for the TLOC. |
| Maximum Control Connections (on vEdge routers) | Specify the maximum number of vSmart controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0.<br><br>*Range:* 0 through 8<br>*Default:* 2 |
| vBond As Stun Server (on vEdge routers) | Click On to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the vEdge router is located behind a NAT. |
| Exclude Controller Group List (on vEdge routers) | Set the vSmart controllers that the tunnel interface is not allowed to connect to.<br>*Range:* 0 through 100 |
| vManage Connection Preference (on vEdge routers) | Set the preference for using a tunnel interface to exchange control traffic with the vManage NMS.<br>*Range:* 0 through 8<br>*Default:* 5 |

| | |
|---|---|
| Port Hop | Click On to enable port hopping, or click Off to disable it. If port hopping is enabled globally, you can disable it on an individual TLOC (tunnel interface). To control port hopping on a global level, use the System configuration template.<br>*Default:* Enabled (on vEdge routers); disabled (on vManage NMSs and vSmart controllers) |
| Low-Bandwidth Link (on vEdge routers) | Select to characterize the tunnel interface as a low-bandwidth link. |
| Allow Service | Select On or Off for each service to allow or disallow the service on the interface. |

To configure additional tunnel interface parameters, click Advanced Options:

| Parameter Name | Description |
|---|---|
| GRE (on vEdge routers) | Use GRE encapsulation on the tunnel interface. By default, GRE is disabled.<br><br>If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation. |
| IPsec (on vEdge routers) | Use IPsec encapsulation on the tunnel interface. By default, IPsec is enabled.<br><br>If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation. |
| IPsec Preference (on vEdge routers) | Specify a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value.<br><br>*Range:* 0 through 4294967295<br>*Default:* 0 |
| IPsec Weight (on vEdge routers) | Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel.<br><br>*Range:* 1 through 255<br>*Default:* 1 |
| Carrier | Select the carrier name or private network identifier to associate with the tunnel.<br><br>*Values:* carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default<br>*Default:* default |
| Bind Loopback Tunnel (on vEdge routers) | Enter the name of a physical interface to bind to a loopback interface. |
| Last-Resort Circuit (on vEdge routers) | Select to use the tunnel interface as the circuit of last resort. |
| NAT Refresh Interval | Enter the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection.<br>*Range:* 1 through 60 seconds<br>*Default:* 5 seconds |
| Hello Interval | Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection.<br>*Range:* 100 through 10000 milliseconds<br>*Default:* 1000 milliseconds (1 second) |
| Hello Tolerance | Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down.<br><br>*Range:* 12 through 60 seconds<br>*Default:* 12 seconds |

To save the feature template, click Save.

*CLI equivalent:*

```
vpn 0
  interface interface-name
    tunnel-interface
      allow-service service-name
      bind interface-name (on vEdge routers only)
      carrier carrier-name
      color color
      encapsulation (gre | ipsec) (on vEdge routers only)
        preference number
        weight number
      exclude-controller-group-list number (on vEdge routers only)
      hello-interval milliseconds
      hello-tolerance seconds
      last-resort-circuit (on vEdge routers only)
      low-bandwidth-link (on vEdge routers only)
      max-control-connections number (on vEdge routers only)
      nat-refresh-interval seconds
      vbond-as-stun-server
      vmanage-connection-preference number (on vEdge routers only)
```

## Configure the Interface as a NAT Device (on vEdge Routers)

To configure an interface to act as a NAT device for applications such as port forwarding, select the NAT tab, click On and configure the following parameters:

| Parameter Name | Description |
|---|---|
| NAT | Click On to have the interface act as a NAT device. |
| Refresh Mode | Select how NAT mappings are refreshed, either outbound or bidirectional (outbound and inbound).<br>*Default* : Outbound |
| UDP Timeout | Specify when NAT translations over UDP sessions time out.<br>*Range* : 1 through 65536 minutes<br>*Default* : 1 minutes |
| TCP Timeout | Specify when NAT translations over TCP sessions time out.<br>*Range* : 1 through 65536 minutes<br>*Default* : 60 minutes (1 hour) |
| Block ICMP | Select On to block inbound ICMP error messages. By default, a vEdge router acting as a NAT device receives these error messages.<br>*Default* : Off |
| Respond to Ping | Select On to have the vEdge router respond to ping requests to the NAT interface's IP address that are received from the public side of the connection. |

To create a port forwarding rule, click Add New Port Forwarding Rule and configure the following parameters. You can define up to 128 port-forwarding rules to allow requests from an external network to reach devices on the internal network.

| Parameter Name | Description |
|---|---|
| Port Start Range | Enter a port number to define the port or first port in the range of interest.<br>*Range:* 0 through 65535 |
| Port End Range | Enter the same port number to apply port forwarding to a single port, or enter a larger number to apply it to a range of ports.<br>*Range:* 0 through 65535 |

| | |
|---|---|
| Protocol | Select the protocol to which to apply the port-forwarding rule, either TCP or UDP. To match the same ports for both TCP and UDP traffic, configure two rules. |
| VPN | Specify the private VPN in which the internal server resides. This VPN is one of the VPN identifiers in the overlay network.<br>*Range:* 0 through 65530 |
| Private IP | Specify the IP address of the internal server to which to direct traffic that matches the port-forwarding rule. |

To save a port forwarding rule, click Add.

To save the feature template, click Save.

*CLI equivalent:*

```
vpn vpn-id
  interface interface-name
    nat
      block-icmp-error
      port-forward port-start port-number1 port-end port-number2 proto (tcp | udp)
        private-ip-address ip-address private-vpn vpn-id
      refresh (bi-directional | outbound)
      respond-to-ping
      tcp-timeout minutes
      udp-timeout minutes
```

## Configure VRRP (on vEdge Routers)

To have an interface run the Virtual Router Redundancy Protocol (VRRP), which allows multiple routers to share a common virtual IP address for default gateway redundancy, select the VRRP tab. Then click Add New VRRP and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Group ID | Enter the virtual router ID, which is a numeric identifier of the virtual router. You can configure a maximum of 24 groups.<br>*Range:* 1 through 255 |
| Priority | Enter the priority level of the router. There router with the highest priority is elected as primary. If two vEdge routers have the same priority, the one with the higher IP address is elected as primary.<br>*Range:* 1 through 254<br>*Default:* 100 |
| Timer | Specify how often the VRRP primary sends VRRP advertisement messages. If subordinate routers miss three consecutive VRRP advertisements, they elect a new primary.<br>*Range:* 1 through 3600 seconds<br>*Default:* 1 second |
| Track OMP<br>Track Prefix List | By default, VRRP uses of the state of the service (LAN) interface on which it is running to determine which vEdge router is the primary virtual router. if a vEdge router loses all its WAN control connections, the LAN interface still indicates that it is up even though the router is functionally unable to participate in VRRP. To take WAN side connectivity into account for VRRP, configure one of the following:<br><br>Track OMP—Click On for VRRP to track the Overlay Management Protocol (OMP) session running on the WAN connection. If the primary VRRP router loses all its OMP sessions, VRRP elects a new default gateway from those that have at least one active OMP session.<br><br>Track Prefix List—Track both the OMP session and a list of remote prefixes, which is defined in a prefix list configured on the local router. If the primary VRRP router loses all its OMP sessions, VRRP failover occurs as described for the Track OMP option. In addition, if reachability to one of the prefixes in the list is lost, VRRP failover occurs immediately, without waiting for the OMP hold timer to expire, thus minimizing the amount of overlay traffic is dropped while the vEdge routers determine the VRRP primary. |

| | |
|---|---|
| IP Address | Enter the IP address of the virtual router. This address must be different from the configured interface IP addresses of both the local vEdge router and the peer running VRRP. |

*CLI equivalent:*

```
vpn vpn-id
  interface geslot/port[.subinterface]
    vrrp group-number
      ipv4 ip-address
      priority number
      timer seconds
      (track-omp | track-prefix-list list-name)
```

## Apply Access Lists and QoS Parameters (on vEdge Routers)

To configure a shaping rate to a router interface and to apply a QoS map, a rewrite rule, access lists, and policers to a router interface, select the ACL/QoS tab and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Shaping rate | Configure the aggregate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps). |
| QoS Map | Specify the name of the QoS map to apply to packets being transmitted out the interface. |
| Rewrite Rule | Click On, and specify the name of the rewrite rule to apply on the interface. |
| Ingress ACL – IPv4 | Click On, and specify the name of the access list to apply to IPv4 packets being received on the interface. |
| Egress ACL – IPv4 | Click On, and specify the name of the access list to apply to IPv4 packets being transmitted on the interface. |
| Ingress ACL – IPv6 | Click On, and specify the name of the access list to apply to IPv6 packets being received on the interface. |
| Egress ACL – IPv6 | Click On, and specify the name of the access list to apply to IPv6 packets being transmitted on the interface. |
| Ingress Policer | Click On, and specify the name of the policer to apply to packets received on the interface. |
| Egress Policer | Click On, and specify the name of the policer to apply to packets being transmitted on the interface. |

To save the feature template, click Save.

*CLI equivalent:*

```
vpn vpn-id
  interface interface-name
    access-list acl-list (in | out)
    policer policer-name (in |out)
    qos-map name
    rewrite-rule name
    shaping-rate name
```

## Add ARP Table Entries

To configure static Address Resolution Protocol (ARP) table entries on the interface, select the ARP tab. Then click Add New ARP and configure the following parameters:

| Parameter Name | Description |
|---|---|

| | |
|---|---|
| IP Address | Enter the IP address for the ARP entry in dotted decimal notation or as a fully qualified host name. |
| MAC Address | Enter the MAC address in colon-separated hexadecimal notation. |

To save the ARP configuration, click Add.

To save the feature template, click Save.

*CLI equivalent:*

```
vpn vpn-id
  interface interface-name
    arp
      ip ip-address mac mac-address
```

## Configure IEEE 802.1X Authentication for WANs

To configure IEEE 802.1X authentication for WANs on the interface, select the 802.1X tab, and click On:

| Parameter Name | Description |
|---|---|
| 802.1X | Click On to enable IEEE 802.1X on the interface. |
| RADIUS Server | Enter the tag of the RADIUS server to use for 802.1X authentication. It can be from 4 through 16 characters long. You configure the tag in the AAA feature template . |
| Account Interim Interval | Enter how often to send 802.1X interim accounting updates to the RADIUS server.<br>*Range:* 0 through 7200 seconds<br>*Default:* 0 (no interim accounting updates are sent) |
| NAS Identifier | Enter the NAS identifier of the local router. It can be a string from 1 to 255 characters long. This identifier is sent to the RADIUS server. |
| NAS IP | Enter the NAS IP address of the local router. This address is sent to the RADIUS server. |
| Wake On LAN | Enable a client to be powered up when the router receives an Ethernet magic packet frame. |
| Control Direction | Select how an 802.1X interface that is using wake on LAN handles packets from unauthorized clients:<br>• In and Out—Send and receive packets with unauthorized clients. This is the default<br>• In Only—Send but do not receive packets with unauthorized clients. |
| Reauthentication | Enter how often to reauthenticate 802.1X clients. By default, no reauthentication attempts are made after the initial LAN access request.<br>*Range:* 0 through 1440 minutes |
| Inactivity | Enter how long to wait before revoking an 802.1X client's network access.<br>*Range:* 0 through 1440 minutes (24 hours)<br>*Default:* 60 minutes (1 hour) |
| Host Mode | Select whether an 802.1X interface grants access to a single client or to multiple clients:<br>• Multi Auth—Grant access to one client on a voice VLAN and multiple clients on data VLANs.<br>• Multi Host—Grant access to multiple clients<br>• Single Host—Grant access only to the first authenticated client. This is the default. |

To configure other IEEE 802.1X authentication properties, click Advanced Options and configure the following parameters:

Parameter Name

Description

Authentication Order

Set the order of authentication methods to use when authenticating devices for connection to the 802.1X WAN. The default authentication order is RADIUS, then MAC authentication bypass (MAB).

**VLAN**

Authentication Fail VLAN

Configure network access when RADIUS authentication or the RADIUS server fails. An authentication-fail VLAN is similar to a critical VLAN.

Guest VLAN

Configure a guest VLAN to provide limited services 50 802.1X–compliant clients.

Authentication Reject VLAN

Configure limited services to 802.1X–compliant clients that failed RADIUS authentication. An authentication-reject VLAN is similar to a restricted VLAN.

Default VLAN

Configure network access for 802.1X–compliant clients that are successfully authenticated by the RADIUS server. If you do not configure a default VLAN on the router, successfully authenticated clients are placed into VLAN 0, which is the VLAN associated with an untagged bridge.

**Dynamic Authentication Server**

DAS Port

Configure the UDP port number to listen for CoA requests from the RADIUS server.
*Range:* 1 through 65535
*Default:* 3799

Client

Set the IP address of the RADIUS or other authentication server from which to accept CoA requests.

Secret Key

Set the password that the RADIUS or other authentication server uses to access the router's 802.1X interface.

Time Window

Set how long a CoA request is valid.
*Range:* 0 through 1000 seconds
*Default:* 300 seconds (5 minutes)

Require Timestamp

Enable to require the DAS client to timestamp CoA messages.

VPN

Set the VPN through which the RADIUS or other authentication server is reachable.

**MAC Authentication Bypass**

Server

Select to enable MAC authentication bypass (MAB) on the RADIUS server and to authentication non-802.1X–compliant clients using a RADIUS server.

Allow

Specify the MAC addresses of one or more devices so that authentication checks for these devices are performed using the RADIUS server.

**Request Attributes**

Authentication

Click Authentication, then click Add New Authentication Entry to configure RADIUS authentication attribute–value (AV) pairs to send to the RADIUS server during an 802.1X session.

To save the entry, click Add.

Accounting

Click Accounting, then click Add New Accounting Entry to configure RADIUS accounting attribute–value (AV) pairs to send to the RADIUS server during an 802.1X session.

To save the entry, click Add.

To save the feature template, click Save.

*CLI equivalent:*

```
vpn 0
  interface interface-name
    dot1x
      accounting-interval minutes
      acct-req-attr attribute-number (integer integer | octet octet | string string)
      auth-fail-vlan vlan-id
      auth-order (mab | radius)
      auth-reject-vlan vlan-id
      auth-req-attr attribute-number (integer integer | octet octet | string string)
      control-direction direction
      das
        client ip-address
        port port-number
        require-timestamp
        secret-key password
        time-window seconds
        vpn vpn-id
      default-vlan vlan-id
      guest-vlan vlan-id
      host-mode (multi-auth | multi-host | single-host)
      mac-authentication-bypass
        allow mac-addresses
        server
      nas-identifier string
      nas-ip-address ip-address
      radius-servers tag
      reauthentication minutes
      timeout
        inactivity minutes
      wake-on-lan
```

## Configure Other Interface Properties

To configure other interface properties, select the Advanced tab and configure the following parameters:

| Parameter Name | Description |
|---|---|

| | |
|---|---|
| Duplex | Choose full or half to specify whether the interface runs in full-duplex or half-duplex mode.<br>*Default:* full |
| MAC Address | Specify a MAC address to associate with the interface, in colon-separated hexadecimal notation. |
| IP MTU | Specify the maximum MTU size of packets on the interface.<br>*Range:* 576 through 1804<br>*Default:* 1500 bytes |
| PMTU Discovery | Click On to enable path MTU discovery on the interface. PMTU determines the largest MTU size that the interface supports so that packet fragmentation does not occur. |
| Flow Control | Select a setting for bidirectional flow control, which is a mechanism for temporarily stopping the transmission of data on the interface.<br>*Values:* autonet, both, egress, ingress, none<br>*Default:* autoneg |
| TCP MSS | Specify the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented.<br>*Range:* 552 to 1460 bytes<br>*Default:* None |
| Speed | Specify the speed of the interface, for use when the remote end of the connection does not support autonegotiation.<br>*Values:* 10, 100, or 1000 Mbps<br>*Default:* Autonegotiate (10/100/1000 Mbps) |
| Clear-Dont-Fragment | Click On to clear the Don't Fragment (DF) bit in the IPv4 packet header for packets being transmitted out the interface. When the DF bit is cleared, packets larger than that interface's MTU are fragmented before being sent. |
| Static Ingress QoS (on vEdge routers) | Specify a queue number to use for incoming traffic.<br>*Range:* 0 through 7 |
| ARP Timeout (on vEdge routers) | Specify how long it takes for a dynamically learned ARP entry to time out.<br>*Range:* 0 through 2678400 seconds (744 hours)<br>*Default:* 1200 (20 minutes) |
| Autonegotiation | Click Off to turn off autonegotiation. By default, an interface runs in autonegotiation mode. |
| TLOC Extension | Enter the name of a physical interface on the same router that connects to the WAN transport. This configuration then binds this service-side interface to the WAN transport. A second router at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN.<br><br>Note that TLOC extension over L3 is only supported for Cisco IOS XE routers. If configuring TLOC extension over L3 for a Cisco IOS XE router, enter the IP address of the L3 interface. |
| Power over Ethernet (on vEdge 100m and vEdge 100wm routers) | Click On to enable PoE on the interface. |
| Tracker (on vEdge routers) | Enter the name of a tracker to track the status of transport interfaces that connect to the internet. |
| ICMP Redirect (on vEdge routers) | Click Disable to disable ICMP redirect messages on the interface. By default, an interface allows ICMP redirect messages. |
| GRE Tunnel Source IP (on IOS XE routers) | Enter the IP address of the extended WAN interface. |

| | |
|---|---|
| Xconnect (on IOS XE routers) | Enter the name of a physical interface on the same router that connects to the WAN transport. |

*CLI equivalent:*

```
vpn vpn-id
  interface interface-name
    arp-timeout seconds (on vEdge routers only)
    [no] autonegotiate
    clear-dont-fragment
    duplex (full | half)
    flow-control control
    icmp-redirect-disable (on vEdge routers only)
    mac-address mac-address
    mtu bytes
    pmtu
    pppoe-client (on vEdge 100m and vEdge 100wm routers only)
      ppp-interface pppnumber
    speed speed
    static-ingress-qos number (on vEdge routers only)
    tcp-mss-adjust bytes
    tloc-extension interface-name (on vEdge routers only)
    tracker tracker-name (on vEdge routers only)
```

## Release Information

Introduced in vManage NMS Release 15.2.
In Release 17.2.2, add support for tracker interface status.
In Release 18.2, add support for disabling ICMP redirect messages.

## VPN Interface Ethernet PPPoE

Use the PPPoE template for Cisco IOS XE routers.

You configure PPPoE over GigabitEthernet interfaces on Cisco IOS XE routers, to provide PPPoE client support.

To configure interfaces on Cisco routers using vManage templates:

1. Create a VPN Interface Ethernet PPPoE feature template to configure Ethernet PPPoE interface parameters, as described in this article.

2. Create a VPN feature template to configure VPN parameters. See the VPN help topic.

## 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.

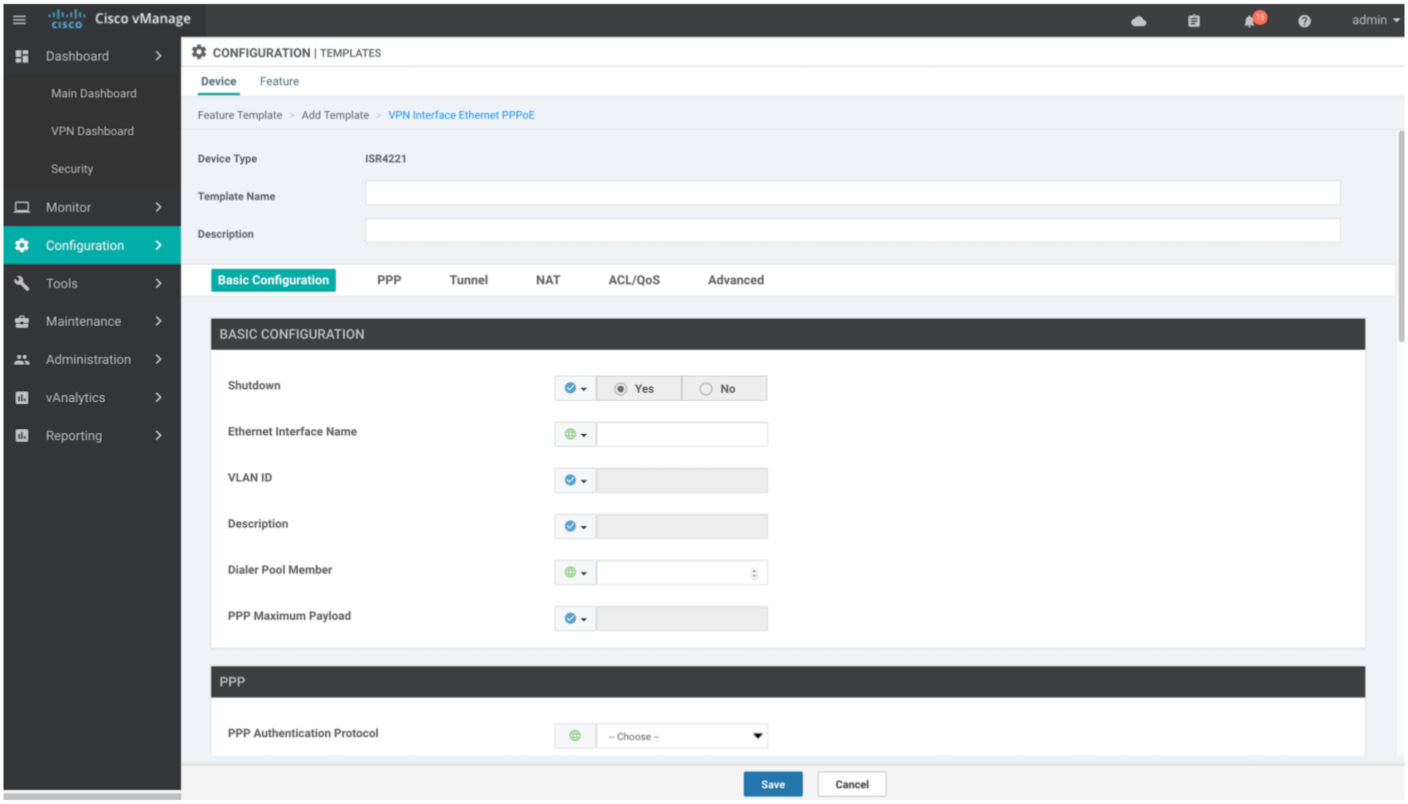
3. From the Create Template drop-down, select "From Feature Template."

4. From the Device Model drop-down, select the type of device for which you are creating the template.

5. Click the Transport & Management VPN tab located directly beneath the Description field, or scroll to the Transport & Management VPN section.

6. Under Additional VPN 0 Templates, located to the right of the screen, click VPN Interface Ethernet PPPoE.

7. From the VPN Interface Ethernet PPPoE drop-down, click Create Template. The VPN Interface Ethernet PPPoE template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining Ethernet PPPoE 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:

| 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 Viptela device to a device template** .<br><br>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](#) .<br><br>To change the default key, type a new string and move the cursor out of the Enter Key box.<br><br>Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID. |

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

## Configure PPPoE Functionality

To configure basic PPPoE functionality, select the Basic Configuration tab and configure the following parameters. Required parameters are indicated with an asterisk.

| **Parameter Name** | **Description** |
|---|---|
| Shutdown* | Click No to enable the GigabitEthernet interface. |
| Ethernet Interface Name | Enter the name of a GigabitEthernet interface.<br><br>For IOS XE routers, you must spell out the interface names completely (for example, **GigabitEthernet0/0/0** ). |
| VLAN ID | VLAN tag of the sub-interface. |
| Description | Enter a description of the Ethernet-PPPoE-enabled interface. |
| Dialer Pool Member | Enter the number of the dialer pool to which the interface belongs.<br><br>*Range* : 100 to 255. |
| PPP Maximum Payload | Enter the maximum receive unit (MRU) value to be negotiated during PPP Link Control Protocol (LCP) negotiation.<br>*Range* : 64 through 1792 bytes |

To save the feature template, click Save.

## Configure the PPP Authentication Protocol

To configure the PPP Authentication Protocol, select the PPP tab and configure the following parameters. Required parameters are indicated with an asterisk.

| Parameter Name | Description |
|---|---|
| PPP Authentication Protocol | Select the authentication protocol used by the MLP:<br><br>• CHAP—Enter the hostname and password provided by your Internet Service Provider (ISP). *hostname* can be up to 255 characters.<br><br>• PAP—Enter the username and password provided by your ISP. *username* can be up to 255 characters.<br><br>• PAP and CHAP—Configure both authentication protocols. Enter the login credentials for each protocol. To use the same username and password for both, click Same Credentials for PAP and CHAP. |

To save the feature template, click Save.

## Create a Tunnel Interface

On IOS XE routers, you can configure up to four tunnel interfaces. This means that each router can have up to four TLOCs.

For the control plane to establish itself so that the overlay network can function, you must configure WAN transport interfaces in VPN 0.

To configure a tunnel interface for the multilink interface, select the Tunnel Interface tab and configure the following parameters:

| Parameter Name | Description |
|---|---|

| | |
|---|---|
| Tunnel Interface | Click On to create a tunnel interface. |
| Color | Select a color for the TLOC. |
| Control Connection | If the router has multiple TLOCs, click No to have the tunnel not establish a TLOC. The default is On, which establishes a control connection for the TLOC. |
| Maximum Control Connections | Specify the maximum number of vSmart controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0.<br><br>*Range:* 0 through 8<br>*Default:* 2 |
| vBond As STUN Server | Click On to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the router is located behind a NAT. |
| Exclude Controller Group List | Set the vSmart controllers that the tunnel interface is not allowed to connect to.<br>*Range:* 0 through 100 |
| vManage Connection Preference | Set the preference for using a tunnel interface to exchange control traffic with the vManage NMS.<br>*Range:* 0 through 8<br>*Default:* 5 |
| Port Hop | Click On to enable port hopping, or click Off to disable it. When a router is behind a NAT, port hopping rotates through a pool of preselected OMP port numbers (called base ports) to establish DTLS connections with other routers 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.<br>*Default:* Enabled |
| Low-Bandwidth Link | Select to characterize the tunnel interface as a low-bandwidth link. |
| Allow Service | Select On or Off for each service to allow or disallow the service on the interface. |

To configure additional tunnel interface parameters, click Advanced Options and configure the following parameters:

| Parameter Name | Description |
|---|---|
| GRE | Use GRE encapsulation on the tunnel interface. By default, GRE is disabled.<br><br>If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation. |
| IPsec | Use IPsec encapsulation on the tunnel interface. By default, IPsec is enabled.<br><br>If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation. |
| IPsec Preference | Specify a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value.<br><br>*Range:* 0 through 4294967295<br>*Default:* 0 |
| IPsec Weight | Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel.<br><br>*Range:* 1 through 255<br>*Default:* 1 |

| | |
|---|---|
| Carrier | Select the carrier name or private network identifier to associate with the tunnel.<br><br>*Values:* carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default<br>*Default:* default |
| Bind Loopback Tunnel | Enter the name of a physical interface to bind to a loopback interface. |
| Last-Resort Circuit | Select to use the tunnel interface as the circuit of last resort. |
| NAT Refresh Interval | Enter the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection.<br>*Range:* 1 through 60 seconds<br>*Default:* 5 seconds |
| Hello Interval | Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection.<br>*Range:* 100 through 10000 milliseconds<br>*Default:* 1000 milliseconds (1 second) |
| Hello Tolerance | Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down.<br><br>*Range:* 12 through 60 seconds<br>*Default:* 12 seconds |

## Configure the Interface as a NAT Device

To configure an interface to act as a NAT device for applications such as port forwarding, select the NAT tab, click On and configure the following parameters:

| Parameter Name | Description |
|---|---|
| NAT | Click On to have the interface act as a NAT device. |
| Refresh Mode | Select how NAT mappings are refreshed, either outbound or bidirectional (outbound and inbound).<br>*Default* : Outbound |
| UDP Timeout | Specify when NAT translations over UDP sessions time out.<br>*Range* : 1 through 65536 minutes<br>*Default* : 1 minutes |
| TCP Timeout | Specify when NAT translations over TCP sessions time out.<br>*Range* : 1 through 65536 minutes<br>*Default* : 60 minutes (1 hour) |
| Block ICMP | Select On to block inbound ICMP error messages. By default, a router acting as a NAT device receives these error messages.<br>*Default* : Off |
| Respond to Ping | Select On to have the router respond to ping requests to the NAT interface's IP address that are received from the public side of the connection. |

To create a port forwarding rule, click Add New Port Forwarding Rule and configure the following parameters. You can define up to 128 port-forwarding rules to allow requests from an external network to reach devices on the internal network.

| Parameter Name | Description |
|---|---|
| Port Start Range | Enter a port number to define the port or first port in the range of interest.<br>*Range:* 0 through 65535 |

| | |
|---|---|
| Port End Range | Enter the same port number to apply port forwarding to a single port, or enter a larger number to apply it to a range of ports.<br>*Range:* 0 through 65535 |
| Protocol | Select the protocol to which to apply the port-forwarding rule, either TCP or UDP. To match the same ports for both TCP and UDP traffic, configure two rules. |
| VPN | Specify the private VPN in which the internal server resides. This VPN is one of the VPN identifiers in the overlay network.<br>*Range:* 0 through 65530 |
| Private IP | Specify the IP address of the internal server to which to direct traffic that matches the port-forwarding rule. |

To save a port forwarding rule, click Add.

To save the feature template, click Save.

## Apply Access Lists

To apply a rewrite rule, access lists, and policers to a router interface, select the ACL tab and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Shaping rate | Configure the aggregate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps). |
| QoS map | Specify the name of the QoS map to apply to packets being transmitted out the interface. |
| Rewrite Rule | Click On, and specify the name of the rewrite rule to apply on the interface. |
| Ingress ACL – IPv4 | Click On, and specify the name of the access list to apply to IPv4 packets being received on the interface. |
| Egress ACL – IPv4 | Click On, and specify the name of the access list to apply to IPv4 packets being transmitted on the interface. |
| Ingress ACL – IPv6 | Click On, and specify the name of the access list to apply to IPv6 packets being received on the interface. |
| Egress ACL – IPv6 | Click On, and specify the name of the access list to apply to IPv6 packets being transmitted on the interface. |
| Ingress Policer | Click On, and specify the name of the policer to apply to packets being received on the interface. |
| Egress Policer | Click On, and specify the name of the policer to apply to packets being transmitted on the interface. |

To save the feature template, click Save.

## Configure Other Interface Properties

To configure other interface properties, select the Advanced tab and configure the following properties:

| Parameter Name | Description |
|---|---|
| Bandwidth Upstream | For transmitted traffic, set the bandwidth above which to generate notifications.<br>*Range:* 1 through ($2^{32}$ / 2) – 1 kbps |
| Bandwidth Downstream | For received traffic, set the bandwidth above which to generate notifications.<br>*Range:* 1 through ($2^{32}$ / 2) – 1 kbps |

| | |
|---|---|
| IP MTU | Specify the maximum MTU size of packets on the interface.<br>*Range:* 576 through 1804<br>*Default:* 1500 bytes |
| TCP MSS | Specify the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented.<br>*Range:* 552 to 1460 bytes<br>*Default:* None |
| TLOC Extension | Enter the name of the physical interface on the same router that connects to the WAN transport circuit. This configuration then binds this service-side interface to the WAN transport. A second router at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN. |
| Tracker | Enter the name of a tracker to track the status of transport interfaces that connect to the internet. |
| IP Directed-Broadcast | Enables translation of a directed broadcast to physical broadcasts. An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet but which originates from a node that is not itself part of that destination subnet. |

To save the feature template, click Save.

## Release Information

Introduced in vManage NMS in Release 18.4.1.

## VPN Interface GRE

Use the VPN Interface GRE template for all vEdge Cloud and vEdge router devices.

When a service, such as a firewall, is available on a device that supports only GRE tunnels, you can configure a GRE tunnel on the vEdge router to connect to the remote device by configuring a logical GRE interface. You then advertise that the service is available via a GRE tunnel, and you create data policies to direct the appropriate traffic to the tunnel. GRE interfaces come up as soon as they are configured, and they stay up as long as the physical tunnel interface is up.

To configure GRE interfaces using vManage templates:

1. Create a VPN Interface GRE feature template to configure a GRE interface, as described in this article.
2. Create a VPN feature template to advertise a service that is reachable via a GRE tunnel, to configure GRE-specific static routes, and to configure other VPN parameters. See the VPN help topic.
3. Create a data policy on the vSmart controller that applies to the service VPN, including a **set service** *service-name* **local** command. See the Policies help topic.

## 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 template for VPN 0 or VPN 512:
    a. Click the Transport & Management VPN tab located directly beneath the Description field, or scroll to the Transport & Management VPN section.

b. Under Additional VPN 0 Templates, located to the right of the screen, click VPN Interface GRE.

c. From the VPN Interface GRE drop-down, click Create Template. The VPN Interface GRE template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN Interface GRE parameters.

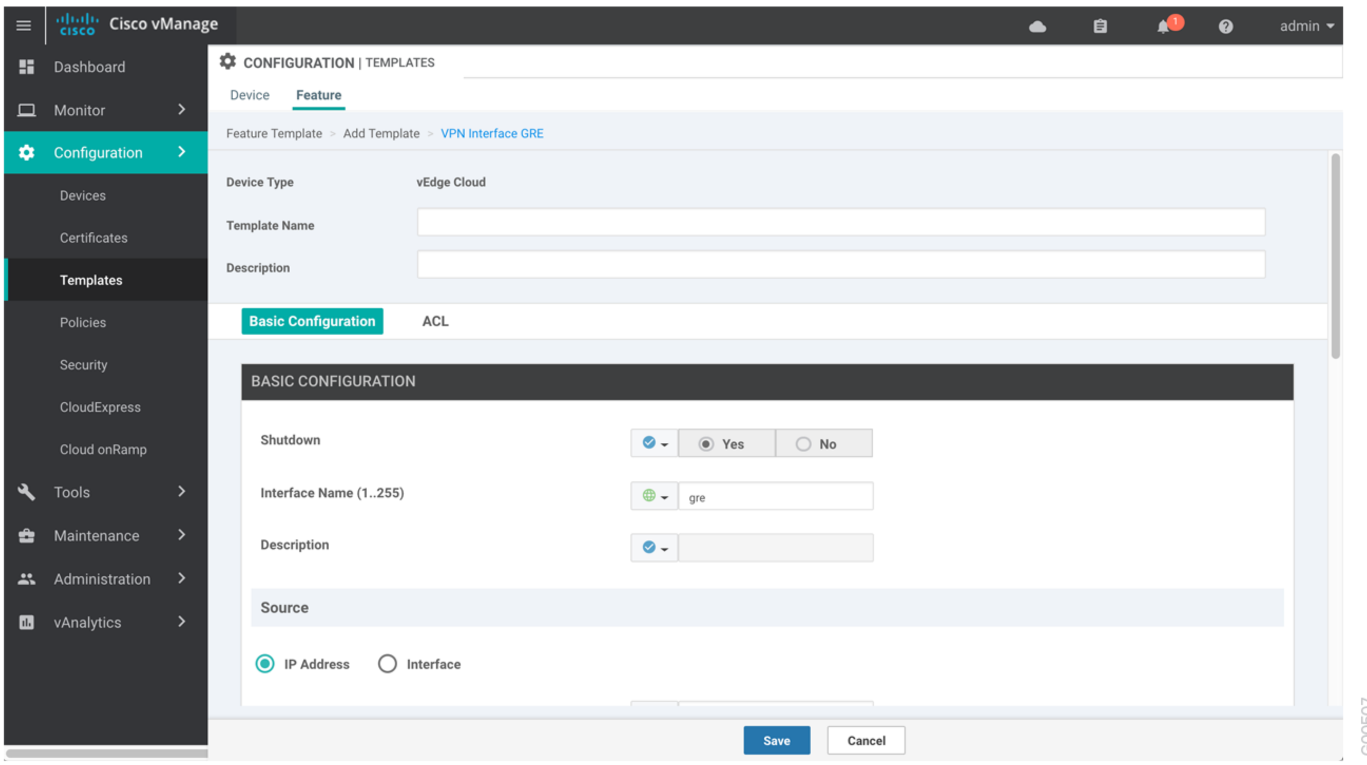
6. To create a template for VPNs 1 through 511, and 513 through 65530:

   a. Click the Service VPN tab located directly beneath the Description field, or scroll to the Service VPN section.

   b. Click the Service VPN drop-down.

   c. Under Additional VPN templates, located to the right of the screen, click VPN Interface GRE.

   d. From the VPN Interface GRE drop-down, click Create Template. The VPN Interface GRE template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN Interface GRE 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 and select one of the following:

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

## Configuring a Basic GRE Interface

To configure a basic GRE interface, select the Basic Configuration and then configure the following parameters. Parameters marked with an asterisk are required to configure a GRE interface.

| Parameter Name | Description |
|---|---|
| Shutdown* | Click Off to enable the interface. |
| Interface Name* | Enter the name of the GRE interface, in the format **gre** *number* . *number* can be from 1 through 255. |
| Description | Enter a description of the GRE interface. |
| Source* | Enter the source of the GRE interface:<br>• GRE Source IP Address—Enter the source IP address of the GRE tunnel interface. This address is on the local router.<br>• Tunnel Source Interface—Enter the physical interface that is the source of the GRE tunnel. |
| Destination* | Enter the destination IP address of the GRE tunnel interface. This address is on a remote device |
| GRE Destination IP Address* | Enter the destination IP address of the GRE tunnel interface. This address is on a remote device |
| IPv4 Address | Enter an IPv4 address for the GRE tunnel. |
| IP MTU | Specify the maximum MTU size of packets on the interface.<br>*Range:* 576 through 1804<br>*Default:* 1500 bytes |
| Clear-Dont-Fragment | Click On to clear the Don't Fragment bit in the IPv4 packet header for packets being transmitted out the interface. |
| TCP MSS | Specify the maximum segment size (MSS) of TPC SYN packets passing through the vEdge router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented.<br>*Range:* 552 to 1460 bytes<br>*Default:* None |

| | |
|---|---|
| Keepalive Interval | Specify how often the GRE interface sends keepalive packets on the GRE tunnel. Because GRE tunnels are stateless, sending of keepalive packets is the only way to determine whether the remote end of the tunnel is up. The keepalive packets are looped back to the sender. Receipt of these packets by the sender indicates that the remote end of the GRE tunnel is up.<br>*Range:* 0 through 65535 seconds<br>*Default:* 10 seconds |
| Keepalive Retries | Specify how many times the GRE interface tries to resend keepalive packets before declaring the remote end of the GRE tunnel to be down.<br>*Range:* 0 through 255<br>*Default:* 3 |

To save the feature template, click Save.

*CLI equivalent:*

```
vpn vpn-id
  interface grenumber
    clear-dont-fragment
    description text
    ip address ipv4-prefix/length
    keepalive seconds retries
    mtu bytes
    policer policer-name (in |out)
    qos-map name
    rewrite-rule name
    shaping-rate name
    [no] shutdown
    tcp-mss-adjust bytes
    tunnel-destination ip-address
    (tunnel-source ip-address | tunnel-source-interface interface-name)
```

## Configure Interface Access Lists

To configure access lists on a GRE interface, select the ACL tab and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Rewrite Rule | Click On, and specify the name of the rewrite rule to apply on the interface. |
| Ingress ACL – IPv4 | Click On, and specify the name of the access list to apply to IPv4 packets being received on the interface. |
| Egress ACL – IPv4 | Click On, and specify the name of the access list to apply to IPv4 packets being transmitted on the interface. |
| Ingress Policer | Click On, and specify the name of the policer to apply to packets being received on the interface. |
| Egress Policer | Click On, and specify the name of the policer to apply to packets being transmitted on the interface. |

*CLI equivalent:*

```
vpn vpn-id
  interface grenumber
    access-list acl-list (in | out)
    policer policer-name (in |out)
    qos-map name
    rewrite-rule name
    shaping-rate name
```

## Release Information

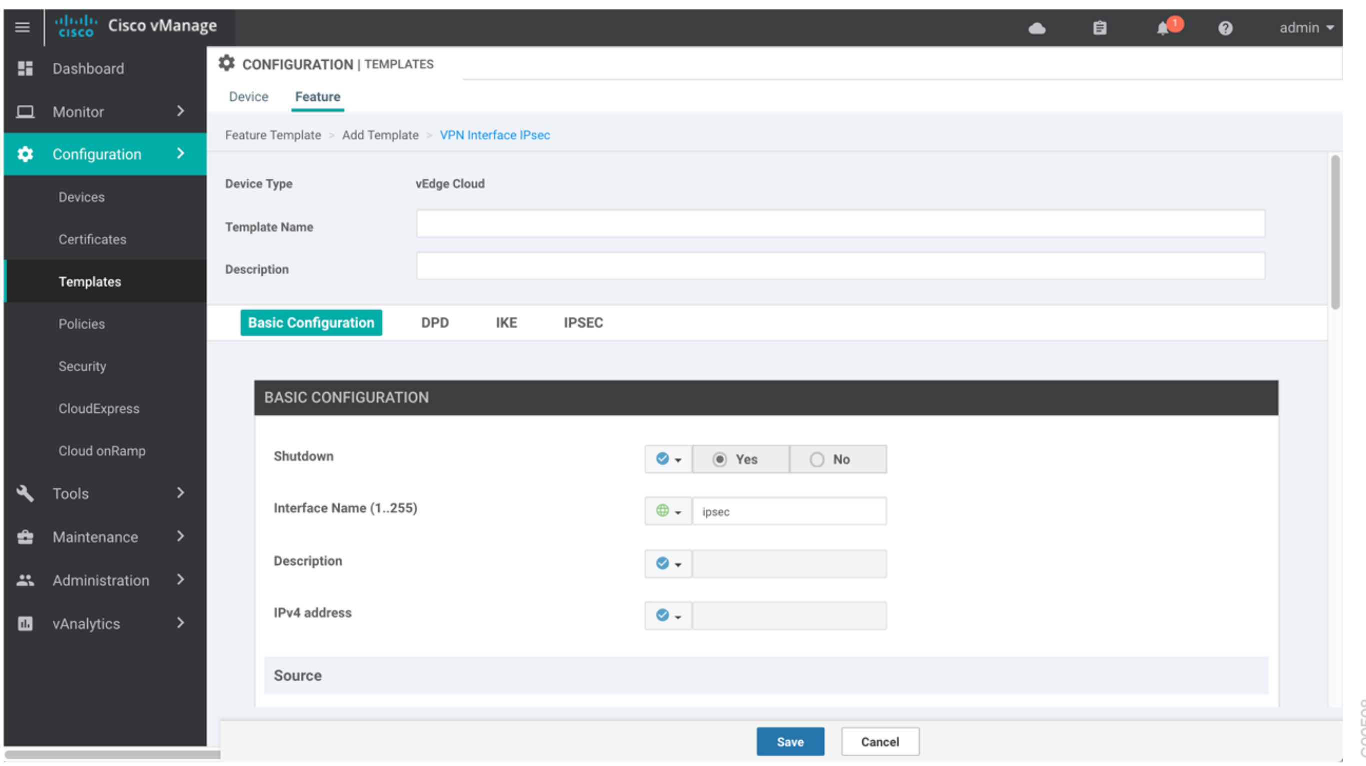
Introduced in vManage NMS Release 15.4.1.

## VPN Interface IPsec

Use the VPN Interface IPsec feature template to configure IPsec tunnels on vEdge routers that are being used for Internet Key Exchange (IKE) sessions. You can configure IPsec on tunnels in the transport VPN (VPN 0) and in service VPNs (VPN 1 through 65530, except for 512).

## 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. Click the Service VPN tab located directly beneath the Description field, or scroll to the Service VPN section.
6. Click the Service VPN drop-down.




7. Under Additional VPN Templates, located to the right of the screen, click VPN Interface IPsec.
8. From the VPN Interface IPsec drop-down, click Create Template. The VPN Interface IPsec template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN Interface IPsec parameters.
9. In the Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

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

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

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

## Configure a Basic IPsec Tunnel Interface

To configure an IPsec tunnel to use for IKE sessions, select the Basic Configuration tab and configure the following parameters. Parameters marked with an asterisk are required to configure an IPsec tunnel.

| Parameter Name | Description |
| --- | --- |
| Shutdown* | Click No to enable the interface. |
| Interface Name* | Enter the name of the IPsec interface, in the format **ipsec** *number* . *number* can be from 1 through 256. |
| Description | Enter a description of the IPsec interface. |
| IPv4 Address* | Enter the IPv4 address of the IPsec interface, in the format *ipv4-prefix* / *length* . The address must be a /30. |
| Source* | Set the source of the IPsec tunnel that is being used for IKE key exchange:<br><br>• Click IP Address—Enter the IPv4 address that is the source tunnel interface. This address must be configured in VPN 0.<br><br>• Click Interface—Enter the name of the physical interface that is the source of the IPsec tunnel. This interface must be configured in VPN 0. |
| Destination: IPsec Destination IP Address/FQDN* | Set the destination of the IPsec tunnel that is being used for IKE key exchange. Enter either an IPv4 address or the fully qualified DNS name that points to the destination. |
| TCP MSS | Specify the maximum segment size (MSS) of TPC SYN packets passing through the vEdge router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented.<br>*Range:* 552 to 1460 bytes<br>*Default:* None |

| | |
|---|---|
| IP MTU | Specify the maximum MTU size of packets on the interface.<br>*Range:* 576 through 1804<br>*Default:* 1500 bytes |

To save the feature template, click Save.

*CLI equivalent:*

```
vpn vpn-id
  interface ipsecnumber
    ip address ipv4-prefix/length
    mtu bytes
    no shutdown
    tcp-mss-adjust bytes
    tunnel-destination ipv4-address
    (tunnel-source ip-address | tunnel-source-interface interface-name)
```

## Configure Dead-Peer Detection

To configure IKE dead-peer detection to determine whether the connection to an IKE peer is functional and reachable, select the DPD tab and configure the following parameters:

| Parameter Name | Description |
|---|---|
| DPD Interval | Specify the interval for IKE to send Hello packets on the connection.<br>*Range:* 0 through 65535 seconds (1 hour through 14 days)<br>*Default:* 10 seconds |
| DPD Retries | Specify how many unacknowledged packets to accept before declaring an IKE peer to be dead and then tearing down the tunnel to the peer.<br>*Range:* 0 through 255<br>*Default:* 3 |

To save the feature template, click Save.

*CLI equivalent:*

```
vpn vpn-id
  interface ipsecnumber
    dead-peer-detection seconds retries number
```

## Configure IKE

To configure IKE, select the IKE tab and configure the parameters discussed below.

When you create an IPsec tunnel on a vEdge router, IKE Version 1 is enabled by default on the tunnel interface. The following properties are also enabled by default for IKEv1:

- Authentication and encryption—AES-256 advanced encryption standard CBC encryption with the HMAC-SHA1 keyed-hash message authentication code algorithm for integrity
- Diffie-Hellman group number—16
- Rekeying time interval—4 hours
- SA establishment mode—Main

To modify IKEv1 parameters, configure the following:

| Parameter Name | Description |
|---|---|

| | |
|---|---|
| IKE Version | Enter 1 to select IKEv1. |
| IKE Mode | Specify the IKE SA establishment mode.<br>*Values:* Aggressive mode, Main mode<br>*Default:* Main mode |
| IPsec Rekey Interval | Specify the interval for refreshing IKE keys.<br>*Range:* 3600 through 1209600 seconds (1 hour through 14 days)<br>*Default:* 14400 seconds (4 hours) |
| IKE Cipher Suite | Specify the type of authentication and encryption to use during IKE key exchange.<br>*Values:* aes128-cbc-sha1, aes256-cbc-sha1<br>*Default:* aes256-cbc-sha1 |
| IKE Diffie-Hellman Group | Specify the Diffie-Hellman group to use in IKE key exchange.<br>*Values:* 1024-bit modulus, 2048-bit modulus, 3072-bit modulus, 4096-bit modulus<br>*Default:* 4096-bit modulus |
| IKE Authentication: Preshared Key | To use preshared key (PSK) authentication, enter the password to use with the preshared key. |
| IKE ID for Local End Point | If the remote IKE peer requires a local end point identifier, specify it.<br>*Range: Default:* Tunnel's source IP address |
| IKE ID for Remote End Point | If the remote IKE peer requires a remote end point identifier, specify it.<br>*Range:* 1 through 64 characters<br>*Default:* Tunnel's destination IP address |

To save the feature template, click Save.

*CLI equivalent:*

```
vpn vpn-id
  interface ipsecnumber
    ike
      authentication-type type
        local-id id
        pre-shared-secret password
        remote-id id
      cipher-suite suite
      group number
      mode mode
      rekey-interval seconds
      version 1
```

To configure IKEv2, configure the following parameters:

| Parameter Name | Description |
|---|---|
| IKE Version | Enter 2 to select IKEv2. |
| IPsec Rekey Interval | Specify the interval for refreshing IKE keys.<br>*Range:* 3600 through 1209600 seconds (1 hour through 14 days)<br>*Default:* 14400 seconds (4 hours) |
| IKE Cipher Suite | Specify the type of authentication and encryption to use during IKE key exchange.<br>*Values:* aes128-cbc-sha1, aes256-cbc-sha1<br>*Default:* aes256-cbc-sha1 |
| IKE Diffie-Hellman Group | Specify the Diffie-Hellman group to use in IKE key exchange.<br>*Values:* 1024-bit modulus, 2048-bit modulus, 3072-bit modulus, 4096-bit modulus<br>*Default:* 4096-bit modulus |

| | |
|---|---|
| IKE Authentication: Preshared Key | To use preshared key (PSK) authentication, enter the password to use with the preshared key. |
| IKE ID for Local End Point | If the remote IKE peer requires a local end point identifier, specify it.<br>*Range: Default:* Tunnel's source IP address |
| IKE ID for Remote End Point | If the remote IKE peer requires a remote end point identifier, specify it.<br>*Range:* 1 through 64 characters<br>*Default:* Tunnel's destination IP address |

To save the feature template, click Save.

*CLI equivalent:*

```
vpn vpn-id
  interface ipsecnumber
    ike
      authentication-type type
        local-id id
        pre-shared-secret password
        remote-id id
      cipher-suite suite
      group number
      rekey-interval seconds
      version 2
```

## Configure IPsec Tunnel Parameters

To configure the IPsec tunnel that carries IKE traffic, select the IPsec tab and configure the following parameters:

| Parameter Name | Description |
|---|---|
| IPsec Rekey Interval | Specify the interval for refreshing IKE keys.<br>*Range:* 3600 through 1209600 seconds (1 hour through 14 days)<br>*Default:* 14400 seconds (4 hours) |
| IKE Replay Window | Specify the replay window size for the IPsec tunnel.<br>*Values:* 64, 128, 256, 512, 1024, 2048, 4096, 8192 bytes<br>*Default:* 32 bytes |
| IPsec Cipher Suite | Specify the authentication and encryption to use on the IPsec tunnel.<br>*Values:* **aes256-cbc-sha1** , **aes256-gcm** , **null-sha1**<br>*Default:* **aes256-gcm** |
| Perfect Forward Secrecy | Specify the PFS settings to use on the IPsec tunnel.<br>*Values:*<br>• **group-2** —Use the 1024-bit Diffie-Hellman prime modulus group.<br>• **group-14** —Use the 2048-bit Diffie-Hellman prime modulus group.<br>• **group-15** —Use the 3072-bit Diffie-Hellman prime modulus group.<br>• **group-16** —Use the 4096-bit Diffie-Hellman prime modulus group.<br>• **none** —Disable PFS.<br>*Default:* **group-16** |

To save the feature template, click Save.

*CLI equivalent:*

```
vpn vpn-id
  interface ipsecnumber
    ipsec
      cipher-suite suite
      perfect-forward-secrecy pfs-setting
```

```
rekey-interval seconds
replay-window number
```

## Release Information

Introduced in vManage NMS in Release 17.2.
In Release 17.2.3, add support for PFS.
In Release 18.2, support support for IPsec tunnels in VPN 0.
In Release 18.4, standard IPsec support for IOS XE routers.

## VPN Interface Multilink

Use the VPN Interface Multilink template for Cisco IOS XE routers running the SD-WAN software.

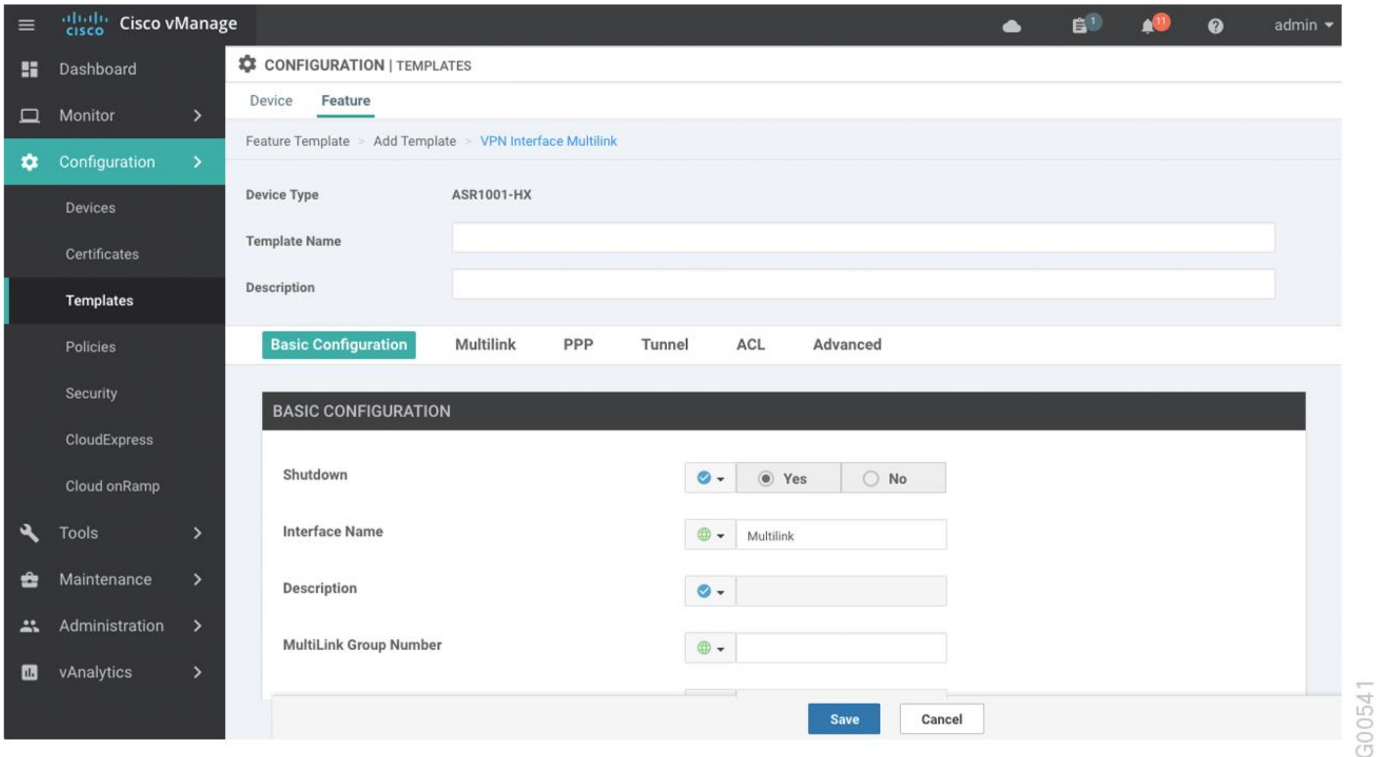
Multilink Point-to-Point Protocol (MLP) is used to combine multiple physical links into a single logical connection, called an MLP bundle.

To configure multilink on IOS XE routers using vManage templates:

1. Create a VPN Interface Multilink feature template to configure multilink interface properties.
2. Optionally, create a VPN feature template to modify the default configuration of VPN 0. See the VPN help topic.

## 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. If you are configuring the multilink interface in the transport VPN (VPN 0):
    a. Click the Transport & Management VPN tab located directly beneath the Description field, or scroll to the Transport & Management VPN section.
    b. Under Additional VPN 0 Templates, located to the right of the screen, click VPN Interface Multilink Controller.
6. If you are configuring the multilink interface in a service VPN (VPNs other than VPN 0):
    a. Click the Service VPN tab located directly beneath the Description field, or scroll to the Service VPN section.
    b. In the Service VPN drop-down, enter the number of the service VPN.
    c. Under Additional VPN Templates, located to the right of the screen, click VPN Interface Multilink Controller.
7. From the VPN Interface Multilink Controller drop-down, click Create Template. The VPN Multilink template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining multilink Interface 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:

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

## Configure a Multilink Interface

To configure a multilink interface, select the Basic Configuration tab and configure the following parameters. Parameters marked with an asterisk are required to configure the interface.

Note, if you are creating a VPN Interface Multilink template, you do not need to create a T1/E1 Controller template or a VPN Interface T1/E1 template.

| Parameter Name | Description |
|---|---|
| Shutdown* | Click No to enable the multilink interface. |
| Multilink Interface Name* | Enter the number of the MLP interface. It can be a number from 1 through 65,535. |
| Description | Enter a description for the multilink interface. |
| Multilink Group Number* | Enter the number of the multilink group. It can be a number from 1 through 65,535 but it must be the same as the number you enter in the Multilink Interface Name parameter. |
| IPv4 Address* | To configure a static address, click Static and enter an IPv4 address.<br><br>To set the interface as a DHCP client so that the interface to receive its IP address from a DHCP server, click Dynamic. You can optionally set the DHCP distance to specify the administrative distance of routes learned from a DHCP server. The default DHCP distance is 1. |
| IPv6 Address* | To configure a static address for an interface in VPN 0, click Static and enter an IPv6 address.<br><br>To set the interface as a DHCP client so that the interface to receive its IP address from a DHCP server, click Dynamic. You can optionally set the DHCP distance to specify the administrative distance of routes learned from a DHCP server. The default DHCP distance is 1. You can optionally enable DHCP rapid commit, to speed up the assignment of IP addresses. |
| Bandwidth Upstream | For transmitted traffic, set the bandwidth above which to generate notifications.<br>*Range:* 1 through ($2^{32}$ / 2) – 1 kbps |
| Bandwidth Downstream | For received traffic, set the bandwidth above which to generate notifications.<br>*Range:* 1 through ($2^{32}$ / 2) – 1 kbps |
| IP MTU | Specify the maximum MTU size of packets on the interface. MLP encapsulation adds 6 extra bytes (4 header, 2 checksum) to each outbound packet. These overhead bytes reduce the effective bandwidth on the connection; therefore, the throughput for an MLP bundle is slightly less than an equivalent bandwidth connection that is not using MLP.<br>*Range:* 576 through 1804<br>*Default:* 1500 bytes |

To save the feature template, click Save.

## Configure the PPP Authentication Protocol

To configure the PPP authentication protocol, select the PPP tab and configure the following parameters:

| Parameter Name | Description |
|---|---|

| | |
|---|---|
| Authentication Protocol | Select the authentication protocol used by the MLP:<br>• CHAP—Enter the hostname and password provided by your Internet Service Provider (ISP). *hostname* can be up to 255 characters.<br>• PAP—Enter the username and password provided by your ISP. *username* can be up to 255 characters.<br>• PAP and CHAP—Configure both authentication protocols. Enter the login credentials for each protocol. To use the same username and password for both, click Same Credentials for PAP and CHAP. |

To save the feature template, click Save.

## Create a Tunnel Interface

On vEdge routers, you can configure up to four tunnel interfaces. This means that each vEdge router can have up to four TLOCs.

For the control plane to establish itself so that the overlay network can function, you must configure WAN transport interfaces in VPN 0.

To configure a tunnel interface for the multilink interface, select the Tunnel Interface tab and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Tunnel Interface | Click On to create a tunnel interface. |
| Color | Select a color for the TLOC. |
| Control Connection | If the vEdge router has multiple TLOCs, click No to have the tunnel not establish a TLOC. The default is On, which establishes a control connection for the TLOC. |
| Maximum Control Connections | Specify the maximum number of vSmart controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0.<br>*Range:* 0 through 8<br>*Default:* 2 |
| vBond As STUN Server | Click On to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the vEdge router is located behind a NAT. |
| Exclude Controller Group List | Set the vSmart controllers that the tunnel interface is not allowed to connect to.<br>*Range:* 0 through 100 |
| vManage Connection Preference | Set the preference for using a tunnel interface to exchange control traffic with the vManage NMS.<br>*Range:* 0 through 8<br>*Default:* 5 |
| Port Hop | Click On to enable port hopping, or click Off to disable it. When a router is behind a NAT, port hopping rotates through a pool of preselected OMP port numbers (called base ports) to establish DTLS connections with other routers 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.<br>*Default:* Enabled |
| Low-Bandwidth Link | Select to characterize the tunnel interface as a low-bandwidth link. |
| Allow Service | Select On or Off for each service to allow or disallow the service on the interface. |

To configure additional tunnel interface parameters, click Advanced Options and configure the following parameters:

| Parameter Name | Description |
|---|---|

| | |
|---|---|
| GRE | Use GRE encapsulation on the tunnel interface. By default, GRE is disabled.<br><br>If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation. |
| IPsec | Use IPsec encapsulation on the tunnel interface. By default, IPsec is enabled.<br><br>If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation. |
| IPsec Preference | Specify a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value.<br><br>*Range:* 0 through 4294967295<br>*Default:* 0 |
| IPsec Weight | Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel.<br><br>*Range:* 1 through 255<br>*Default:* 1 |
| Carrier | Select the carrier name or private network identifier to associate with the tunnel.<br><br>*Values:* carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default<br>*Default:* default |
| Bind Loopback Tunnel | Enter the name of a physical interface to bind to a loopback interface. |
| Last-Resort Circuit | Select to use the tunnel interface as the circuit of last resort. |
| NAT Refresh Interval | Enter the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection.<br>*Range:* 1 through 60 seconds<br>*Default:* 5 seconds |
| Hello Interval | Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection.<br>*Range:* 100 through 10000 milliseconds<br>*Default:* 1000 milliseconds (1 second) |
| Hello Tolerance | Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down.<br><br>*Range:* 12 through 60 seconds<br>*Default:* 12 seconds |

## Apply Access Lists

To apply a rewrite rule, access lists, and policers to a router interface, select the ACL tab and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Shaping rate | Configure the aggregate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps). |
| QoS map | Specify the name of the QoS map to apply to packets being transmitted out the interface. |
| Rewrite Rule | Click On, and specify the name of the rewrite rule to apply on the interface. |

| | |
|---|---|
| Ingress ACL – IPv4 | Click On, and specify the name of the access list to apply to IPv4 packets being received on the interface. |
| Egress ACL – IPv4 | Click On, and specify the name of the access list to apply to IPv4 packets being transmitted on the interface. |
| Ingress ACL – IPv6 | Click On, and specify the name of the access list to apply to IPv6 packets being received on the interface. |
| Egress ACL – IPv6 | Click On, and specify the name of the access list to apply to IPv6 packets being transmitted on the interface. |
| Ingress Policer | Click On, and specify the name of the policer to apply to packets being received on the interface. |
| Egress Policer | Click On, and specify the name of the policer to apply to packets being transmitted on the interface. |

To save the feature template, click Save.

## Configure Other Interface Properties

To configure other interface properties, select the Advanced tab and configure the following properties:

| Parameter Name | Description |
|---|---|
| PMTU Discovery | Click On to enable path MTU discovery on the interface, to allow the router to determine the largest MTU size supported without requiring packet fragmentation. |
| TCP MSS | Specify the maximum segment size (MSS) of TPC SYN packets passing through the vEdge router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented.<br>*Range:* 552 to 1460 bytes<br>*Default:* None |
| Clear Dont Fragment | Click On to clear the Don't Fragment bit in the IPv4 packet header for packets being transmitted out the interface. When the DF bit is cleared, packets larger than that interface's MTU are fragmented before being sent. |
| Static Ingress QoS | Select a queue number to use for incoming traffic.<br>*Range: 0 through 7* |
| Autonegotiate | Click Off to turn off autonegotiation. By default, an interface runs in autonegotiation mode. |
| TLOC Extension | Enter the name of the physical interface on the same router that connects to the WAN transport circuit. This configuration then binds this service-side interface to the WAN transport. A second vEdge router at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN. |

To save the feature template, click Save.

## Release Information

Introduced in vManage NMS in Release 18.3.

## VPN Interface NAT Pool

## Create NAT Pool Interfaces in a VPN

Use the VPN Interface NAT Pool template for all vEdge routers, to create Network Address Translation (NAT) pools of IP addresses in virtual private networks (VPNs).
To configure NAT pool interfaces in a VPN using vManage templates:

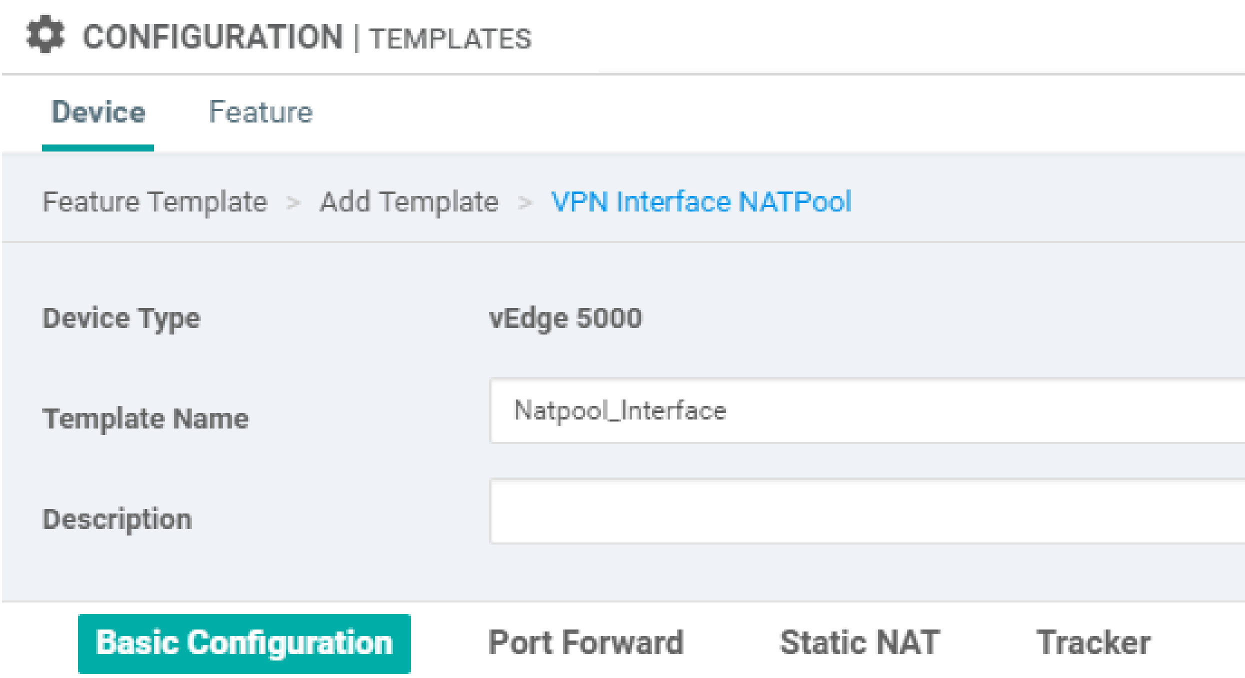
1. Create a VPN Interface NAT Pool template to configure Ethernet interface parameters, as described in this article.
2. Create a VPN feature template to configure parameters for a service-side VPN. See the VPN help topic.
3. Optionally, create a data policy to direct data traffic to a service-side NAT. See Create a Device Template.

## Create and Name a VPN Interface NAT Pool Template

You can open a new VPN Interface NAT Pool template from the Service VPN section of a device template.

1. From the vManage menu, select Configuration > Templates.
2. Click **Feature** .
3. Click **Add Template** .
4. Select a vEdge device from the list.
5. From the VPN section, click **VPN Interface NATPool** .

The VPN Interface NATPool template form displays. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN Interface NAT Pool parameters.

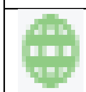



6. In the required Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
7. In the optional Template Description field, enter a description of the template. The description can be up to 2048 characters and can contain only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

### Parameter Menus and Options

Parameter Menus and Options

When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a ), 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:

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

## Configure a NAT Pool Interface

To configure a NAT pool interface, configure the following parameters. Parameters marked with an asterisk are required to configure the interface.

### Basic Configuration

Enter the following basic configuration parameters:

**Parameter Name**

**Values**

**Description**

Shutdown*

Yes

No

Click **No** to enable the interface.

Interface Name (1…31)*

1-31

Enter a number for the NAT pool interface to use for service-side NAT. For example, *natpool22* .

Description

Enter a description for the interface.

IPv4 Address*

Enter the IPv4 address of the interface. The address length determines the number of NAT addresses that the router use at the same time. A vEdge router can support a maximum of 250 NAT IP addresses.

Refresh Mode

Select how NAT mappings are refreshed:

bi-directional

Keep active the NAT mappings for inbound and outbound traffic.

outbound

Keep active the NAT mappings for outbound traffic. This is the default.

UDP Timeout

1-65536 minutes

Enter the time when NAT translations over UDP sessions time out.
*Default:* 1 minute

TCP Timeout

1-65536 minutes

Enter the time when NAT translations over TCP sessions time out.
*Default:* 60 minutes (1 hour)

Block ICMP

On

Off

Select whether a vEdge router that is acting as a NAT device should receive inbound ICMP error messages. By default, the router blocks these error messages. Click **Off** to receive the ICMP error messages.

Direction

Select the direction in which the NAT interface performs address translation:

inside

Translate the source IP address of packets that are coming from the service side of the vEdge router and that are destined to transport side of the router. This is the default.

outside

Translate the source IP address of packets that are coming to the vEdge router from the transport side of the vEdge router and that are destined to a service-side device.

Overload

Yes

No

Click **No** to disable dynamic NAT. By default, dynamic NAT is enabled.

## Tracker

1. To create one or more tracker interfaces, select the Tracker tab and click New Tracker.
2. Select one or more interfaces to track the status of service interfaces.
3. To save the tracker interfaces, click Add. To save the feature template, click Save.

## CLI Equivalent Commands

Use the following commands to configure NAT Pool interfaces.

```
vpn vpn-id
  interface natpoolnumber
    ip address prefix/length
    nat
      tracker tracker-name1 tracker-name2, tracker-name3
      direction (inside | outside)
      [no] overload
      refresh (bi-directional | outbound)
      static source-ip ip-address1 translate-ip ip-address2 (inside | outside)
      tcp-timeout minutes
      udp-timeout minutes
    [no] shutdown
```

# Configure Port-Forwarding Rules

To create port-forwarding rules to allow requests from an external network to reach devices on the internal network:

1. Select the Port Forward tab.
2. Click **New Port Forwarding Rule** , and configure the following parameters. You can create up to 128 rules.

**Parameter Name**

**Values**

**Description**

Port Start Range

Enter the starting port number. This number must be less than or equal to the ending port number.

Port End Range

Enter the ending port number. To apply port forwarding to a single port, specify the same port number for the starting and ending numbers. When applying port forwarding to a range of ports, the range includes the two port numbers that you specify.

Protocol

TCP

UDP

Select the protocol to apply the port-forwarding rule to. To match the same ports for both TCP and UDP traffic, configure two rules.

VPN

0-65535

Private VPN in which the internal server resides.

Private IP

Enter an IP address to use within the firewall. A best practice is to specify the IP address of a service-side VPN.

3. To save the rule, click **Add** .

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

## CLI Equivalent Commands

```
vpn vpn-id
  interface natpoolnumber
    nat
      port-forward port-start port-number1 port-end port-number2 proto (tcp | udp)
        private-ip-address ip address private-vpn vpn-id
```

# Configure Static NAT

To configure a static NAT of service-side source IP addresses:

1. Select the Static NAT tab. Then click **New Static NAT** and configure the following parameters to add a static NAT mapping:

**Parameter Name**

**Values**

**Description**

Mark as Optional Row

Check **Mark as Optional Row** to mark this configuration as device-specific. To include this configuration for a device, enter the requested variable values when you attach a device template to a device, or create a template variables spreadsheet to apply the variables. See Create a Template Variables Spreadsheet .

Source IP

Enter the NAT private source IP address.

Translate IP

To map a public IP address to a private source address, enter the public IP address.

Static NAT Direction

Select the direction in which to perform network address translation.

inside

Translate the IP address of packets that are coming from the service side of the vEdge router and that are destined for the transport side of the router.

outside

Translate the IP address of packets that are coming to the vEdge router from the transport side of the vEdge router and that are destined for a service-side device.

2. To save the NAT mapping, click **Add** .

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

## CLI Equivalent Commands

```
vpn vpn-id
  interface natpoolnumber
    nat
      port-forward port-start port-number1 port-end port-number2 proto (tcp | udp)
        private-ip-address ip address private-vpn vpn-id
```

# Release Information

Introduced in vManage NMS Release 16.3.
In Release 17.2.2, add support for tracker interface status.
In Release 18.4, updated images; add support for multiple tracker interfaces.

# VPN Interface PPP

Use the VPN Interface PPP template for vEdge Cloud and vEdge router devices.

Point-to-Point Protocol (PPP) is a data link protocol used to establish a direct connection between two nodes. PPP properties are associated with a PPPoE-enabled interface on vEdge routers to connect multiple users over an Ethernet link.

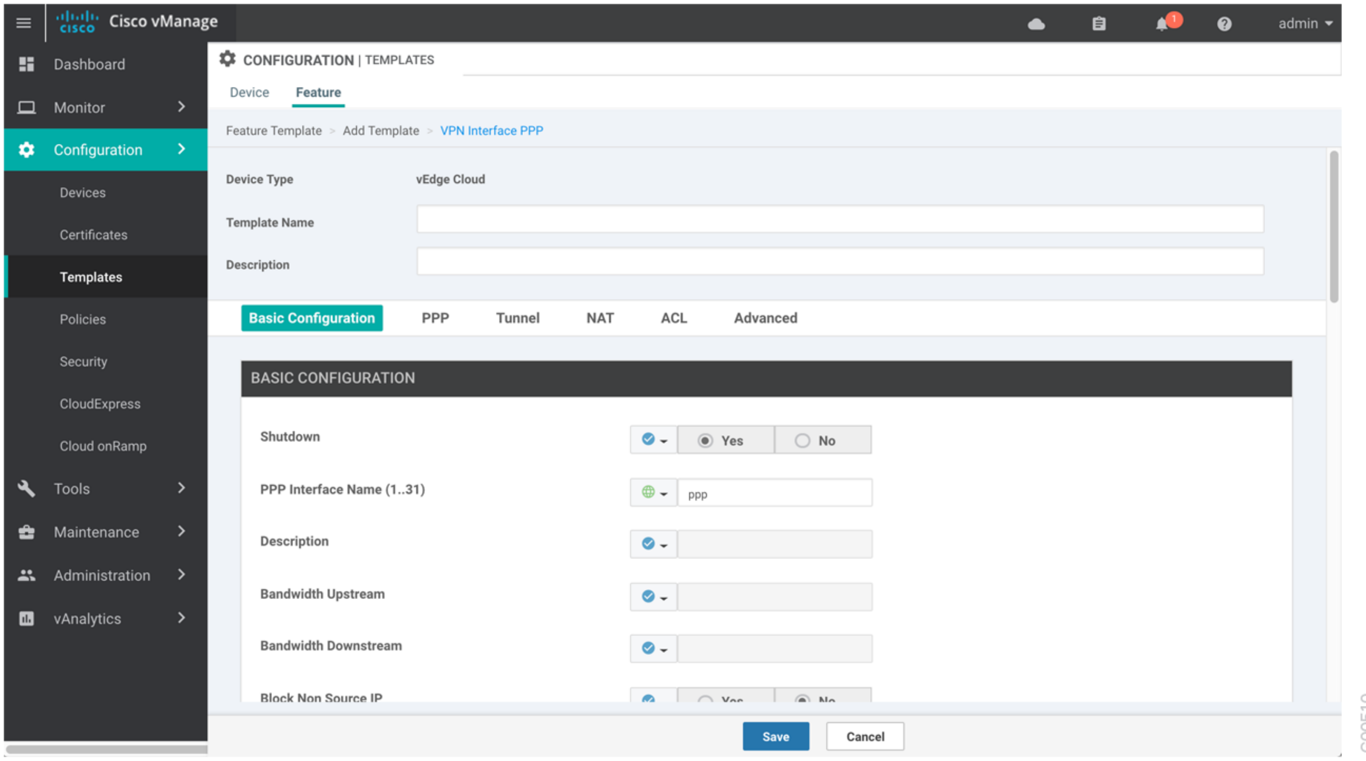
To configure PPPoE on vEdge routers using vManage templates:

1. Create a VPN Interface PPP feature template to configure PPP parameters for the PPP virtual interface, as described in this article.
2. Create a VPN Interface PPP Ethernet feature template to configure a PPPoE-enabled interface. See the VPN Interface PPP Ethernet help topic.
3. Optionally, create a VPN feature template to modify the default configuration of VPN 0. See the VPN help topic.

# 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. Click the Transport & Management VPN tab located directly beneath the Description field, or scroll to the Transport & Management VPN section.

6. Under Additional VPN 0 Templates, located to the right of the screen, click VPN Interface PPP.




7. From the VPN Interface PPP drop-down, click Create Template. The VPN Interface PPP template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN Interface PPP 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:

| 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 Viptela device to a device template** .<br><br>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](#) .<br><br>To change the default key, type a new string and move the cursor out of the Enter Key box.<br><br>Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID. |

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

## Configure a PPP Virtual Interface

To configure a PPP virtual interface, select the Basic Configuration tab and configure the following parameters. Parameters marked with an asterisk are required to configure the interface. You must also configure an authentication protocol and a tunnel interface for the PPP interface, and you must ensure that the maximum MTU for the PPP interface is 1492 bytes.

| **Parameter Name** | **Description** |
|---|---|
| Shutdown* | Click No to enable the PPP virtual interface. |
| PPP Interface Name* | Enter the number of the PPP interface. It can be a number from 1 through 31. |
| Description | Enter a description for the PPP virtual interface. |
| Bandwidth Upstream | For transmitted traffic, set the bandwidth above which to generate notifications.<br>*Range:* 1 through ($2^{32}$ / 2) – 1 kbps |
| Bandwidth Downstream | For received traffic, set the bandwidth above which to generate notifications.<br>*Range:* 1 through ($2^{32}$ / 2) – 1 kbps |
| Block Non-Source IP | Click Yes to have the interface forward traffic only if the source IP address of the traffic matches the interface's IP prefix range. |

To save the feature template, click Save.

*CLI equivalent:*

```
vpn 0
  interface pppnumber
    banddwidth-downstream kbps
    bandwidth-upstream kbps
    block-non-source-ip
    ppp
      no shutdown
```

## Configure the Access Concentrator Name and Authentication Protocol

To configure the access concentrator name, select the PPP tab and configure the following parameters:

| Parameter Name | Description |
|---|---|
| AC Name | Name of the access concentrator used by PPPoE to route connections to the Internet. |
| Authentication Protocol | Select the authentication protocol used by PPPoE:<br><br>• CHAP—Enter the hostname and password provided by your Internet Service Provider (ISP). *hostname* can be up to 255 characters.<br><br>• PAP—Enter the username and password provided by your ISP. *username* can be up to 255 characters.<br><br>• PAP and CHAP—Configure both authentication protocols. Enter the login credentials for each protocol. To use the same username and password for both, click Same Credentials for PAP and CHAP. |

To save the feature template, click Save.

*CLI equivalent:*

```
vpn 0
  interface pppnumber
    ppp
      ac-name name
      authentication
        chap hostname name password password
        pap password password sent-username name
```

## Create a Tunnel Interface

On vEdge routers, you can configure up to four tunnel interfaces. This means that each vEdge router can have up to four TLOCs.

For the control plane to establish itself so that the overlay network can function, you must configure WAN transport interfaces in VPN 0.

To configure a tunnel interface for the PPP interface, select the Tunnel Interface tab and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Tunnel Interface | Click On to create a tunnel interface. |
| Color | Select a color for the TLOC. |
| Control Connection | If the vEdge router has multiple TLOCs, click No to have the tunnel not establish a TLOC. The default is On, which establishes a control connection for the TLOC. |
| Maximum Control Connections | Specify the maximum number of vSmart controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0.<br><br>*Range:* 0 through 8<br>*Default:* 2 |
| vBond As STUN Server | Click On to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the vEdge router is located behind a NAT. |
| Exclude Controller Group List | Set the vSmart controllers that the tunnel interface is not allowed to connect to.<br>*Range:* 0 through 100 |
| vManage Connection Preference | Set the preference for using a tunnel interface to exchange control traffic with the vManage NMS.<br>*Range:* 0 through 8<br>*Default:* 5 |
| Low-Bandwidth Link | Select to characterize the tunnel interface as a low-bandwidth link. |
| Allow Service | Select On or Off for each service to allow or disallow the service on the interface. |

To configure additional tunnel interface parameters, click Advanced Options and configure the following parameters:

| Parameter Name | Description |
|---|---|
| GRE | Use GRE encapsulation on the tunnel interface. By default, GRE is disabled.<br><br>If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation. |
| IPsec | Use IPsec encapsulation on the tunnel interface. By default, IPsec is enabled.<br><br>If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation. |

| | |
|---|---|
| IPsec Preference | Specify a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value.<br><br>*Range:* 0 through 4294967295<br>*Default:* 0 |
| IPsec Weight | Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel.<br><br>*Range:* 1 through 255<br>*Default:* 1 |
| Carrier | Select the carrier name or private network identifier to associate with the tunnel.<br><br>*Values:* carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default<br>*Default:* default |
| Bind Loopback Tunnel | Enter the name of a physical interface to bind to a loopback interface. |
| Last-Resort Circuit | Select to use the tunnel interface as the circuit of last resort. |
| NAT Refresh Interval | Enter the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection.<br>*Range:* 1 through 60 seconds<br>*Default:* 5 seconds |
| Hello Interval | Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection.<br>*Range:* 100 through 10000 milliseconds<br>*Default:* 1000 milliseconds (1 second) |
| Hello Tolerance | Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down.<br><br>*Range:* 12 through 60 seconds<br>*Default:* 12 seconds |

*CLI equivalent:*

```
vpn 0
  interface interface-name
    tunnel-interface
      allow-service service-name
      bind interface-name
      carrier carrier-name
      color color
      encapsulation (gre | ipsec)
        preference number
        weight number
      hello-interval milliseconds
      hello-tolerance seconds
      last-resort-circuit
      max-control-connections number
      nat-refresh-interval seconds
      vbond-as-stun-server
```

## Configure the Interface as a NAT Device

To configure an interface to act as a NAT device, select the NAT tab and configure the following parameters:

| Parameter Name | Description |
|---|---|

| | |
|---|---|
| NAT | Click On to have the interface act as a NAT device. |
| Refresh Mode | Select how NAT mappings are refreshed, either outbound or bidirectional (outbound and inbound).<br><br>*Default* : Outbound |
| UDP Timeout | Specify when NAT translations over UDP sessions time out.<br><br>*Range* : 1 through 65536 minutes<br><br>*Default* : 1 minutes |
| TCP Timeout | Specify when NAT translations over TCP sessions time out.<br><br>*Range* : 1 through 65536 minutes<br><br>*Default* : 60 minutes (1 hour) |
| Block ICMP | Select On to block inbound ICMP error messages. By default, a vEdge router acting as a NAT device receives these error messages.<br><br>*Default* : Off |
| Respond to Ping | Select On to have the vEdge router respond to ping requests to the NAT interface's IP address that are received from the public side of the connection. |

To create a port forwarding rule, click Add New Port Forwarding Rule and configure the following parameters. You can define up to 128 port-forwarding rules to allow requests from an external network to reach devices on the internal network.

| Parameter Name | Description |
|---|---|
| Port Start Range | Enter a port number to define the port or first port in the range of interest.<br><br>*Range:* 0 through 65535 |
| Port End Range | Enter the same port number to apply port forwarding to a single port, or enter the larger number to apply it to a range or ports.<br>*Range:* 0 through 65535 |
| Protocol | Select the protocol to whcih to apply the port-forwarding rule, either TCP or UDP. To match the same ports for both TCP and UDP traffic, configure two rules. |
| VPN | Specify the private VPN in which the internal server resides. This VPN is one of the VPN identifiers in the overlay network.<br>*Range:* 0 through 65535 |
| Private IP | Specify the IP address of the internal server to which to direct traffic that matches the port-forwarding rule. |

To save a port forwarding rule, click Add.

To save the feature template, click Save.

*CLI equivalent:*

```
vpn vpn-id
  interface interface-name
    nat
      block-icmp-error
      port-forward port-start port-number1 port-end port-number2 proto (tcp | udp)
        private-ip-address ip-address private-vpn vpn-id
      refresh (bi-directional | outbound)
      respond-to-ping
```

```
      tcp-timeout minutes
      udp-timeout minutes
```

## Apply Access Lists

To apply a rewrite rule, access lists, and policers to a router interface, select the ACL tab and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Rewrite Rule | Click On, and specify the name of the rewrite rule to apply on the interface. |
| Ingress ACL – IPv4 | Click On, and specify the name of the access list to apply to IPv4 packets being received on the interface. |
| Egress ACL – IPv4 | Click On, and specify the name of the access list to apply to IPv4 packets being transmitted on the interface. |
| Ingress ACL – IPv6 | Click On, and specify the name of the access list to apply to IPv6 packets being received on the interface. |
| Egress ACL – IPv6 | Click On, and specify the name of the access list to apply to IPv6 packets being transmitted on the interface. |
| Ingress Policer | Click On, and specify the name of the policer to apply to packets being received on the interface. |
| Egress Policer | Click On, and specify the name of the policer to apply to packets being transmitted on the interface. |

To save the feature template, click Save.

*CLI equivalent:*

```
vpn 0
  interface pppnumber
    access-list acl-name (in | out)
    ipv6 access-list acl-name (in | out)
    policer policer-name (in |out)
    rewrite-rule name
```

## Configure Other Interface Properties

To configure other interface properties, select the Advanced tab and configure the following properties:

| Parameter Name | Description |
|---|---|
| MAC Address | Specify a MAC address to associate with the interface, in colon-separated hexadecimal notation. |
| IP MTU | Specify the maximum MTU size of packets on the interface.<br>*Range:* 576 through 1804<br>*Default:* 1500 bytes |
| TCP MSS | Specify the maximum segment size (MSS) of TPC SYN packets passing through the vEdge router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented.<br>*Range:* 552 to 1460 bytes<br>*Default:* None |
| Clear Dont Fragment | Click On to clear the Don't Fragment bit in the IPv4 packet header for packets being transmitted out the interface. When the DF bit is cleared, packets larger than that interface's MTU are fragmented before being sent. |
| TLOC Extension | Enter the name of the physical interface on the same router that connects to the WAN transport circuit. This configuration then binds this service-side interface to the WAN transport. A second vEdge router at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN. |

| | |
|---|---|
| Tracker | Enter the name of a tracker to track the status of transport interfaces that connect to the internet. |
| ICMP Redirect | Click Disable to disable ICMP redirect messages on the interface. By default, an interface allows ICMP redirect messages. |

To save the feature template, click Save.

*CLI equivalent:*

```
vpn vpn-id
  interface interface-name
    clear-dont-fragment
    icmp-redirect-disable
    mac-address mac-address
    mtu bytes
    tcp-mss-adjust bytes
    tloc-extension interface-name
    tracker tracker-name
```

## Release Information

Introduced in vManage NMS in Release 15.3.
In Release 16.3, add support for IPv6.
In Release 17.1, support ability to configure both CHAP and PAP authentication on a PPP interface.
In Release 17.2.2, add support for interface status tracking.
In Release 18.2, add support for disabling ICMP redirect messages.

## VPN Interface PPP Ethernet

Use the VPN Interface PPP Ethernet template for vEdge Cloud and vEdge router devices.

Point-to-Point Protocol (PPP) is a data link protocol used to establish a direct connection between two nodes. PPP properties are associated with a PPPoE-enabled interface on vEdge routers to connect multiple users over an Ethernet link.

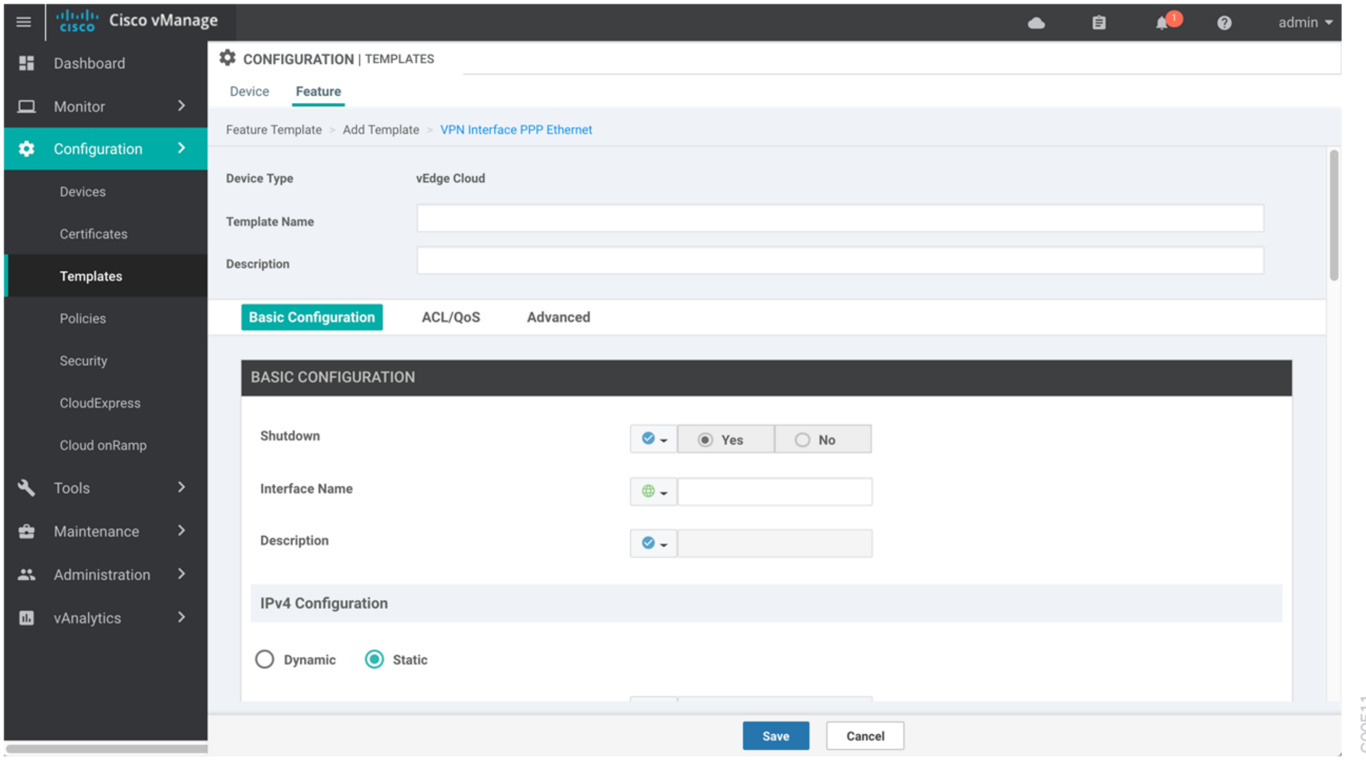
To configure PPPoE on vEdge routers using vManage templates:

1. Create a VPN Interface PPP Ethernet feature template to configure a PPPoE-enabled interface as described in this article.
2. Create a VPN Interface PPP feature template to configure PPP parameters for the PPP virtual interface. See the VPN Interface PPP help topic
3. Optionally, create a VPN feature template to modify the default configuration of VPN 0. See the VPN help topic.

## 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. Click the Transport & Management VPN tab located directly beneath the Description field, or scroll to the Transport & Management VPN section.

6. Under Additional VPN 0 Templates, located to the right of the screen, click VPN Interface PPP.




7. From the VPN Interface PPP Ethernet drop-down, click Create Template. The VPN Interface PPP Ethernet template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN Interface PPP 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:

| 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 Viptela device to a device template** .<br><br>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 .<br><br>To change the default key, type a new string and move the cursor out of the Enter Key box.<br><br>Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID. |

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

## Configure a Basic PPPoE-Enabled Interface

To create a PPPoE-enabled interface on a vEdge router, select the Basic Configuration tab and configure the following parameters. Parameters marked with an asterisk are required to configure the interface.

| Parameter Name | Description |
|---|---|
| Shutdown* | Click No to enable the PPPoE-enabled interface. |
| Interface Name* | Enter the name of the physical interface in VPN 0 to associate with the PPP interface.<br><br>For IOS XE routers, you must spell out the interface names completely (for example, **GigabitEthernet0/0/0** ), and you must configure all the router's interfaces even if you are not using them so that they are configured in the shutdown state and so that all default values for them are configured. |
| Description | Enter a description of the PPPoE-enabled interface. |
| IPv4 Configuration* | To configure a static address, click Static and enter an IPv4 address.<br><br>To set the interface as a DHCP client so that the interface to receive its IP address from a DHCP server, click Dynamic. You can optionally set the DHCP distance to specify the administrative distance of routes learned from a DHCP server. The default DHCP distance is 1. |
| IPv6 Configuration* | To configure a static address for an interface in VPN 0, click Static and enter an IPv6 address.<br><br>To set the interface as a DHCP client so that the interface to receive its IP address from a DHCP server, click Dynamic. You can optionally set the DHCP distance to specify the administrative distance of routes learned from a DHCP server. The default DHCP distance is 1. You can optionally enable DHCP rapid commit, to speed up the assignment of IP addresses. |
| DHCP Helper | Enter up to eight IP addresses for DHCP servers in the network, separated by commas, to have the interface be a DHCP helper. A DHCP helper interface forwards BOOTP (Broadcast) DHCP requests that it receives from the specified DHCP servers. |
| Bandwidth Upstream | For transmitted traffic, set the bandwidth above which to generate notifications.<br>*Range:* 1 through ($2^{32}$ / 2) – 1 kbps |
| Bandwidth Downstream | For received traffic, set the bandwidth above which to generate notifications.<br>*Range:* 1 through ($2^{32}$ / 2) – 1 kbps |

To save the feature template, click Save.

*CLI equivalent:*

```
vpn 0
  interface pppnumber
    bandwidth-downstream kbps
    bandwidth-upstream kbps
    description text
    dhcp-helper ip-address
    (ip address ipv4-prefix/length | ip-dhcp-client [dhcp-distance number])
    (ipv6 address ipv6-prefix/length | ipv6 dhcp-client [dhcp-distance number] [ dhcp-rapid-commit]
    pppoe-client ppp-interface pppnumber
    [no] shutdown
```

## Apply Access Lists

To configure a shaping rate to a PPPoE-enabled interface and to apply a QoS map, a rewrite rule, access lists, and policers to the interface , select the ACL/QOS tab and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Shaping Rate | Configure the aggregate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps). |
| QoS Map | Specify the name of the QoS map to apply to packets being transmitted out the interface. |
| Rewrite Rule | Click On, and specify the name of the rewrite rule to apply on the interface. |
| Ingress ACL – IPv4 | Click On, and specify the name of the access list to apply to IPv4 packets being received on the interface. |
| Egress ACL – IPv4 | Click On, and specify the name of the access list to apply to IPv4 packets being transmitted on the interface. |
| Ingress ACL – IPv6 | Egress ACL – IPv6 |
| Egress ACL – IPv6 | Egress ACL – IPv6 |
| Ingress Policer | Click O,n and specify the name of the policer to apply to packets being received on the interface. |
| Egress Policer | Click On, and specify the name of the policer to apply to packets being transmitted on the interface. |

To save the feature temp

*CLI equivalent:*

```
vpn 0
  interface pppnumber
    access-list acl-list (in | out)
    policer policer-name (in |out)
    qos-map name
    rewrite-rule name
    shaping-rate name
```

## Configure Other Interface Properties

To configure other interface properties, select the Advanced tab and configure the following properties:

| Parameter Name | Description |
|---|---|
| Duplex | Choose full or half to specify whether the interface runs in full-duplex or half-duplex mode.<br>*Default:* Full |
| MAC Address | Specify a MAC address to associate with the interface, in colon-separated hexadecimal notation. |
| IP MTU | Specify the maximum MTU size of packets on the interface.<br>*Range:* 576 through 1804<br>*Default:* 1500 bytes |
| PMTU Discovery | Click On to enable path MTU discovery on the interface. PMTU determines the largest MTU size that the interface supports so that packet fragmentation does not occur. |
| Flow Control | Select a setting for bidirectional flow control, which is a mechanism for temporarily stopping the transmission of data on the interface.<br>*Values:* autonet, both, egress, ingress, none<br>*Default:* autoneg |

| | |
|---|---|
| TCP MSS | Specify the maximum segment size (MSS) of TPC SYN packets passing through the vEdge router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented.<br>*Range:* 552 to 1460 bytes<br>*Default:* None |
| Speed | Specify the speed of the interface, for use when the remote end of the connection does not support autonegotiation.<br>*Values:* 10, 100, or 1000 Mbps<br>*Default:* Autonegotiate (10/100/1000 Mbps) |
| Static Ingress QoS | Specify a queue number to use for incoming traffic.<br>*Range:* 0 through 7 |
| ARP Timeout | Specify how long it takes for a dynamically learned ARP entry to time out.<br>*Range:* 0 through 2678400 seconds (744 hours)<br>*Default:* 1200 seconds (20 minutes) |
| Autonegotiation | Click Off to turn off autonegotiation. By default, an interface runs in autonegotiation mode. |
| TLOC Extension | Enter the name of a physical interface on the same router that connects to the WAN transport. This configuration then binds this service-side interface to the WAN transport. A second vEdge router at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN. |
| Power over Ethernet (on vEdge 100m and vEdge 100wm routers) | Click On to enable PoE on the interface. |
| ICMP Redirect | Click Disable to disable ICMP redirect messages on the interface. By default, an interface allows ICMP redirect messages. |

To save the feature template, click Save.

*CLI equivalent:*

```
vpn 0
  interface pppnumber
    arp-timeout seconds
    [no] autonegotiate
    duplex (full | half)
    flow-control control
    icmp-redirect-disable
    mac-address mac-address
    mtu bytes
    pmtu
    pppoe-client
      ppp-interface pppnumber
    speed speed
    static-ingress-qos number
    tcp-mss-adjust bytes
    tloc-extension interface-name
```

## Release Information

Introduced in vManage NMS Release 15.3.
In Release 16.3, add support for IPv6.
In Release 18.2, add support for disabling ICMP redirect messages.

# VPN Interface SVI

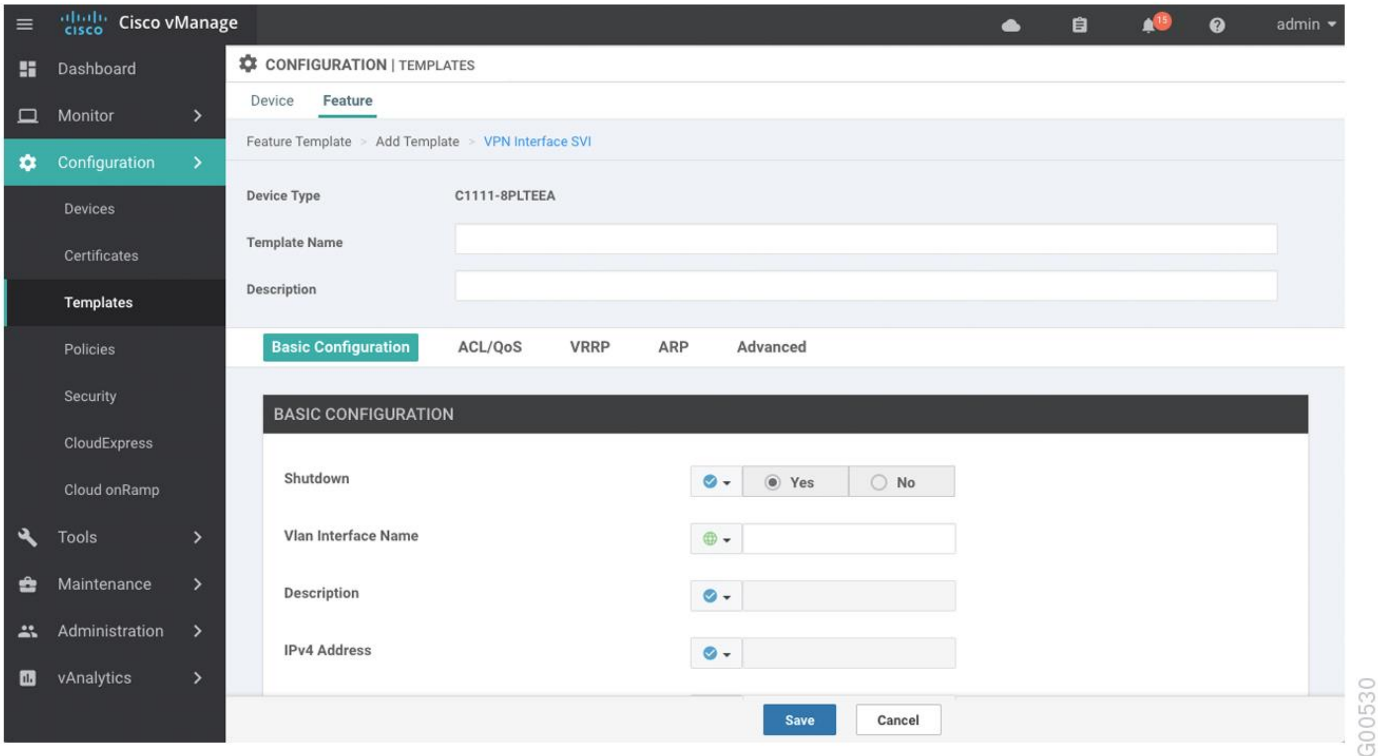
Use the VPN Interface SVI template for Cisco IOS XE routers running the SD-WAN software.

You configure a switch virtual interface (SVI) to configure a VLAN interface.

To configure DSL interfaces on Cisco routers using vManage templates, create a VPN Interface SVI feature template to configure VLAN interface parameters, as described in this article.

## 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. If you are configuring the SVI in the transport VPN (VPN 0):
    a. Click the Transport & Management VPN tab located directly beneath the Description field, or scroll to the Transport & Management VPN section.
    b. Under Additional VPN 0 Templates, located to the right of the screen, click VPN Interface SVI.
6. If you are configuring the SVI in a service VPN (VPNs other than VPN 0):
    a. Click the Service VPN tab located directly beneath the Description field, or scroll to the Service VPN section.
    b. In the Service VPN drop-down, enter the number of the service VPN.
    c. Under Additional VPN Templates, located to the right of the screen, click VPN Interface SVI.
7. From the VPN Interface SVI drop-down, click Create Template. The VPN Interface SVI template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining VLAN Interface 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:

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

## Configure Basic Interface Functionality

To configure basic VLAN interface functionality in a VPN, select the Basic Configuration tab and configure the following parameters. Parameters marked with an asterisk are required to configure an interface.

| **Parameter Name** | **Description** |
|---|---|
| Shutdown* | Click No to enable the VLAN interface. |
| VLAN Interface Name* | Enter the VLAN identifier of the interface.<br>*Range:* 1 through 1094 |
| Description | Enter a description for the interface. |
| IPv4 Address* | Enter the IPv4 address for the interface. |
| DHCP Helper* | Enter up to eight IP addresses for DHCP servers in the network, separated by commas, to have the interface be a DHCP helper. A DHCP helper interface forwards BOOTP (Broadcast) DHCP requests that it receives from the specified DHCP servers. |
| IP MTU | Specify the maximum MTU size of packets on the interface.<br>*Range:* 576 through 1804<br>*Default:* 1500 bytes |

To save the feature template, click Save.

## Apply Access Lists

To apply a rewrite rule, access lists, and policers to a router interface, select the ACL tab and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Ingress ACL – IPv4 | Click On, and specify the name of the access list to apply to IPv4 packets being received on the interface. |
| Egress ACL – IPv4 | Click On, and specify the name of the access list to apply to IPv4 packets being transmitted on the interface. |
| Ingress Policer | Click On, and specify the name of the policer to apply to packets being received on the interface. |
| Egress Policer | Click On, and specify the name of the policer to apply to packets being transmitted on the interface. |

To save the feature template, click Save.

## Configure VRRP

To have an interface run the Virtual Router Redundancy Protocol (VRRP), which allows multiple routers to share a common virtual IP address for default gateway redundancy, select the VRRP tab. Then click Add New VRRP and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Group ID | Enter the virtual router ID, which is a numeric identifier of the virtual router. You can configure a maximum of 24 groups.<br>*Range:* 1 through 255 |
| Priority | Enter the priority level of the router. There router with the highest priority is elected as primary. If two vEdge routers have the same priority, the one with the higher IP address is elected as primary.<br>*Range:* 1 through 254<br>*Default:* 100 |

| | |
|---|---|
| Timer | Specify how often the VRRP primary sends VRRP advertisement messages. If subordinate routers miss three consecutive VRRP advertisements, they elect a new primary.<br>*Range:* 1 through 3600 seconds<br>*Default:* 1 second |
| Track OMP<br>Track Prefix List | By default, VRRP uses of the state of the service (LAN) interface on which it is running to determine which vEdge router is the primary virtual router. if a vEdge router loses all its WAN control connections, the LAN interface still indicates that it is up even though the router is functionally unable to participate in VRRP. To take WAN side connectivity into account for VRRP, configure one of the following:<br><br>Track OMP—Click On for VRRP to track the Overlay Management Protocol (OMP) session running on the WAN connection. If the primary VRRP router loses all its OMP sessions, VRRP elects a new default gateway from those that have at least one active OMP session.<br><br>Track Prefix List—Track both the OMP session and a list of remote prefixes, which is defined in a prefix list configured on the local router. If the primary VRRP router loses all its OMP sessions, VRRP failover occurs as described for the Track OMP option. In addition, if reachability to one of the prefixes in the list is lost, VRRP failover occurs immediately, without waiting for the OMP hold timer to expire, thus minimizing the amount of overlay traffic is dropped while the vEdge routers determine the VRRP primary. |
| IP Address | Enter the IP address of the virtual router. This address must be different from the configured interface IP addresses of both the local vEdge router and the peer running VRRP. |

## Add ARP Table Entries

To configure static Address Resolution Protocol (ARP) table entries on the interface, select the ARP tab. Then click Add New ARP and configure the following parameters:

| Parameter Name | Description |
|---|---|
| IP Address | Enter the IP address for the ARP entry in dotted decimal notation or as a fully qualified host name. |
| MAC Address | Enter the MAC address in colon-separated hexadecimal notation. |

To save the ARP configuration, click Add.

To save the feature template, click Save.

## Configure Other Interface Properties

To configure other interface properties, select the Advanced tab and configure the following properties:

| Parameter Name | Description |
|---|---|
| TCP MSS | Specify the maximum segment size (MSS) of TPC SYN packets passing through the vEdge router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented.<br>*Range:* 552 to 1460 bytes<br>*Default:* None |
| ARP Timeout | Specify how long it takes for a dynamically learned ARP entry to time out.<br>*Range:* 0 through 2678400 seconds (744 hours)<br>*Default:* 1200 (20 minutes) |

To save the feature template, click Save.

## Release Information

Introduced in vManage NMS in Release 18.3.

## VPN Interface T1/E1

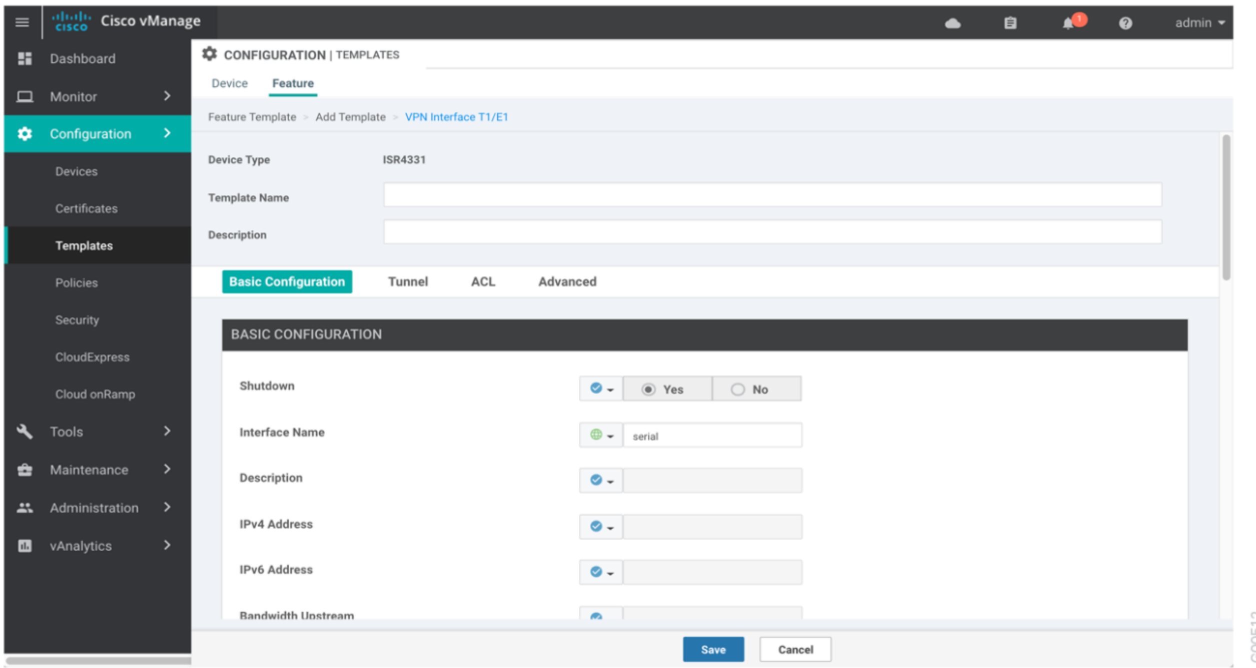
Use the VPN Interface T1/E1 template for Cisco IOS XE routers running the SD-WAN software.

To configure the T1/E1 interfaces in a VPN using vManage templates:

1. Create a VPN Interface T1/E1 feature template to configure T1/E1 interface parameters, as described in this article.
2. Create a T1/E1 Controller template to configure the T1 or E1 network interface module (NIM) parameters. See the T1/E1 Controller help topic.
3. Create a VPN feature template to configure VPN parameters. See the VPN help topic.

## 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 template for VPN 0 or VPN 512:
    a. Click the Transport & Management VPN tab located directly beneath the Description field, or scroll to the Transport & Management VPN section.
    b. Under Additional VPN 0 Templates, located to the right of the screen, click VPN Interface.
    c. From the VPN Interface drop-down, click Create Template. The VPN Interface T1/E1 template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN Interface Ethernet parameters.
6. To create a template for VPNs 1 through 511, and 513 through 65530:
    a. Click the Service VPN tab located directly beneath the Description field, or scroll to the Service VPN section.
    b. Click the Service VPN drop-down.
    c. Under Additional VPN templates, located to the right of the screen, click VPN Interface.
    d. From the VPN Interface drop-down, click Create Template. The VPN Interface Ethernet template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN Interface Ethernet 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 and select one of the following:

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

## Configure Basic Interface Functionality

To configure basic interface functionality in a VPN, select the Basic Configuration tab and configure the following parameters. Parameters marked with an asterisk are required to configure an interface.

| Parameter Name | Description |
|---|---|
| Shutdown* | Click No to enable the interface. |
| Interface name* | Enter a name for the interface. The name should be in the format **serial** *slot* **/** *subslot* **/** *port* **:** *channel-group* .<br><br>You must also configure a number for the channel group in the T1/E1 Controller feature configuration template. |
| Description | Enter a description for the interface. |
| IPv4 Address* | Enter an IPv4 address. |
| IPv6 Address* | Enter an IPv6 address. |
| Bandwidth Upstream | For transmitted traffic, set the bandwidth above which to generate notifications.<br>*Range:* 1 through ($2^{32}$ / 2) – 1 kbps |
| Bandwidth Downstream | For received traffic, set the bandwidth above which to generate notifications.<br>*Range:* 1 through ($2^{32}$ / 2) – 1 kbps |
| IP MTU | Specify the maximum MTU size of packets on the interface.<br>*Range:* 576 through 1804<br>*Default:* 1500 bytes |

To save the feature template, click Save.

## Create a Tunnel Interface

You can configure up to four tunnel interfaces. This means that each vEdge router can have up to four TLOCs.

For the control plane to establish itself so that the overlay network can function, you must configure WAN transport interfaces in VPN 0.

To configure a tunnel interface, select the Interface Tunnel tab and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Tunnel Interface | Click On to create a tunnel interface. |
| Color | Select a color for the TLOC. |
| Control Connection | If the router has multiple TLOCs, click No to have the tunnel not establish a TLOC. The default is On, which establishes a control connection for the TLOC. |
| Maximum Control Connections | Specify the maximum number of vSmart controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0.<br><br>*Range:* 0 through 8<br>*Default:* 2 |
| vBond As Stun Server | Click On to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the vEdge router is located behind a NAT. |
| Exclude Controller Group List | Set the vSmart controllers that the tunnel interface is not allowed to connect to.<br>*Range:* 0 through 100 |

| | |
|---|---|
| vManage Connection Preference | Set the preference for using a tunnel interface to exchange control traffic with the vManage NMS.<br>*Range:* 0 through 8<br>*Default:* 5 |
| Port Hop | Click On to enable port hopping, or click Off to disable it. If port hopping is enabled globally, you can disable it on an individual TLOC (tunnel interface). To control port hopping on a global level, use the System configuration template.<br>*Default:* Enabled (on vEdge routers); disabled (on vManage NMSs and vSmart controllers) |
| Low-Bandwidth Link | Select to characterize the tunnel interface as a low-bandwidth link. |
| Allow Service | Select On or Off for each service to allow or disallow the service on the interface. |

To configure additional tunnel interface parameters, click Advanced Options:

| Parameter Name | Description |
|---|---|
| Encapsulation | Select the encapsulation type to use on the tunnel interface, either IPsec or GRE. The default is IPsec.<br><br>If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation. |
| IPsec | By default, IPsec is enabled on the tunnel interface. To disable IPsec, click Off. |
| IPsec Preference | Specify a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value.<br><br>*Range:* 0 through 4294967295<br>*Default:* 0 |
| IPsec Weigh | Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel.<br><br>*Range:* 1 through 255<br>*Default:* 1 |
| Carrier | Select the carrier name or private network identifier to associate with the tunnel.<br><br>*Values:* carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default<br>*Default:* default |
| Bind Loopback Tunnel | Enter the name of a physical interface to bind to a loopback interface. |
| Last-Resort Circuit | Select to use the tunnel interface as the circuit of last resort. |
| NAT Refresh Interval | Enter the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection.<br>*Range:* 1 through 60 seconds<br>*Default:* 5 seconds |
| Hello Interval | Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection.<br>*Range:* 100 through 10000 milliseconds<br>*Default:* 1000 milliseconds (1 second) |
| Hello Tolerance | Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down.<br><br>*Range:* 12 through 60 seconds<br>*Default:* 12 seconds |

To save the feature template, click Save.

# Apply Access Lists and QoS Parameters (on vEdge Routers)

To configure a shaping rate to a router interface and to apply a QoS map, a rewrite rule, access lists, and policers to a router interface, select the ACLtab and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Shaping Rate | Configure the aggregate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps). |
| QoS Map | Specify the name of the QoS map to apply to packets being transmitted out the interface. |
| Rewrite Rule | Click On, and specify the name of the rewrite rule to apply on the interface. |
| Ingress ACL – IPv4 | Click On, and specify the name of the access list to apply to IPv4 packets being received on the interface. |
| Egress ACL – IPv4 | Click On, and specify the name of the access list to apply to IPv4 packets being transmitted on the interface. |
| Ingress ACL – IPv6 | Click On, and specify the name of the access list to apply to IPv6 packets being received on the interface. |
| Egress ACL – IPv6 | Click On, and specify the name of the access list to apply to IPv6 packets being transmitted on the interface. |
| Ingress Policer | Click On, and specify the name of the policer to apply to packets received on the interface. |
| Egress Policer | Click On, and specify the name of the policer to apply to packets being transmitted on the interface. |

To save the feature template, click Save.

# Configure Other Interface Properties

To configure other interface properties, select the Advanced tab and configure the following parameters:

| Parameter Name | Description |
|---|---|
| PMTU Discovery | Click On to enable path MTU discovery on the interface. PMTU determines the largest MTU size that the interface supports so that packet fragmentation does not occur. |
| TCP MSS | Specify the maximum segment size (MSS) of TPC SYN packets passing through the vEdge router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented.<br>*Range:* 552 to 1460 bytes<br>*Default:* None |
| Clear-Dont-Fragment | Click On to clear the Don't Fragment (DF) bit in the IPv4 packet header for packets being transmitted out the interface. When the DF bit is cleared, packets larger than that interface's MTU are fragmented before being sent. |
| Static Ingress QoS | Specify a queue number to use for incoming traffic.<br>*Range:* 0 through 7 |
| Autonegotiation | Click Off to turn off autonegotiation. By default, an interface runs in autonegotiation mode. |
| TLOC Extension | Enter the name of a physical interface on the same router that connects to the WAN transport. This configuration then binds this service-side interface to the WAN transport. A second vEdge router at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN. |

# Release Information

Introduced in vManage NMS Release 18.2.

## WiFi Radio

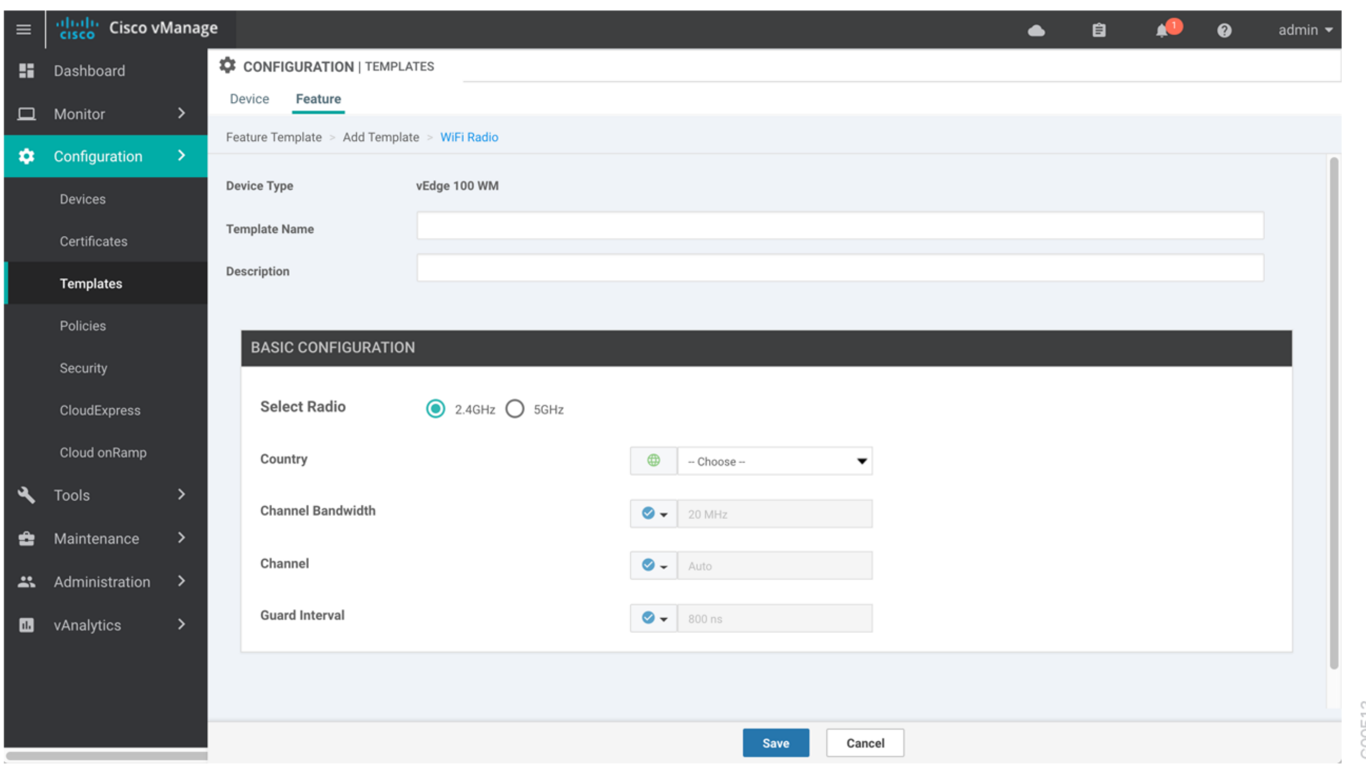
Use the WiFi Radio template for all vEdge router devices that support wireless LANs (WLANs), including the vEdge 100wm router.

To configure WLAN radio parameters using vManage templates:

1. Create a WiFi Radio template to configure WLAN radio parameters, as described in this article.
2. Create a Wifi SSID template to configure an SSID and related parameters. See the WiFi SSID help topic.

## 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 vEdge router model that supports wireless LANs (WLANs).
5. Click the WLAN tab located directly beneath the Description field, or scroll to the WLAN section.
6. From the WiFi Radio drop-down, click Create Template. The WiFi Radio template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining WiFi Radio 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 and select one of the following:

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

## Configure the WLAN Radio Frequency

To configure the WLAN radio frequency, in the Basic Configuration tab, configure the following parameters. Parameters marked with an asterisk are required to configure the radio.

| Parameter Name | Description |
|---|---|
| Select Radio* | Select the radio band. It can be 2.4 GHz or 5 GHz. |
| Country* | Select the country where the router is installed. |
| Channel Bandwidth | Select the IEEE 802.11n and 802.11ac channel bandwidth. For a 5-GHz radio band, the default value is 80 MHz, and for 2.4 GHz, the default is 20 MHz. |
| Channel | Select the radio channel. The default is "auto", which automatically selects the best channel. For 5-GHz radio bands, you can configure dynamic frequency selection (DFS) channels. |
| Guard Interval | Select the guard interval. For a 5-GHz radio band, the default value is the short guard interval (SGI) of 400 ns, and for 2.4 GHz, the default is 800 ns. |

To save the feature template, click Save.

*CLI equivalent:*

```
wlan frequency
  channel channel
  channel-bandwidth megahertz
  country country
  guard-interval nanoseconds
```

## Release Information

Introduced in vManage NMS Release 16.3.

# WiFi SSID

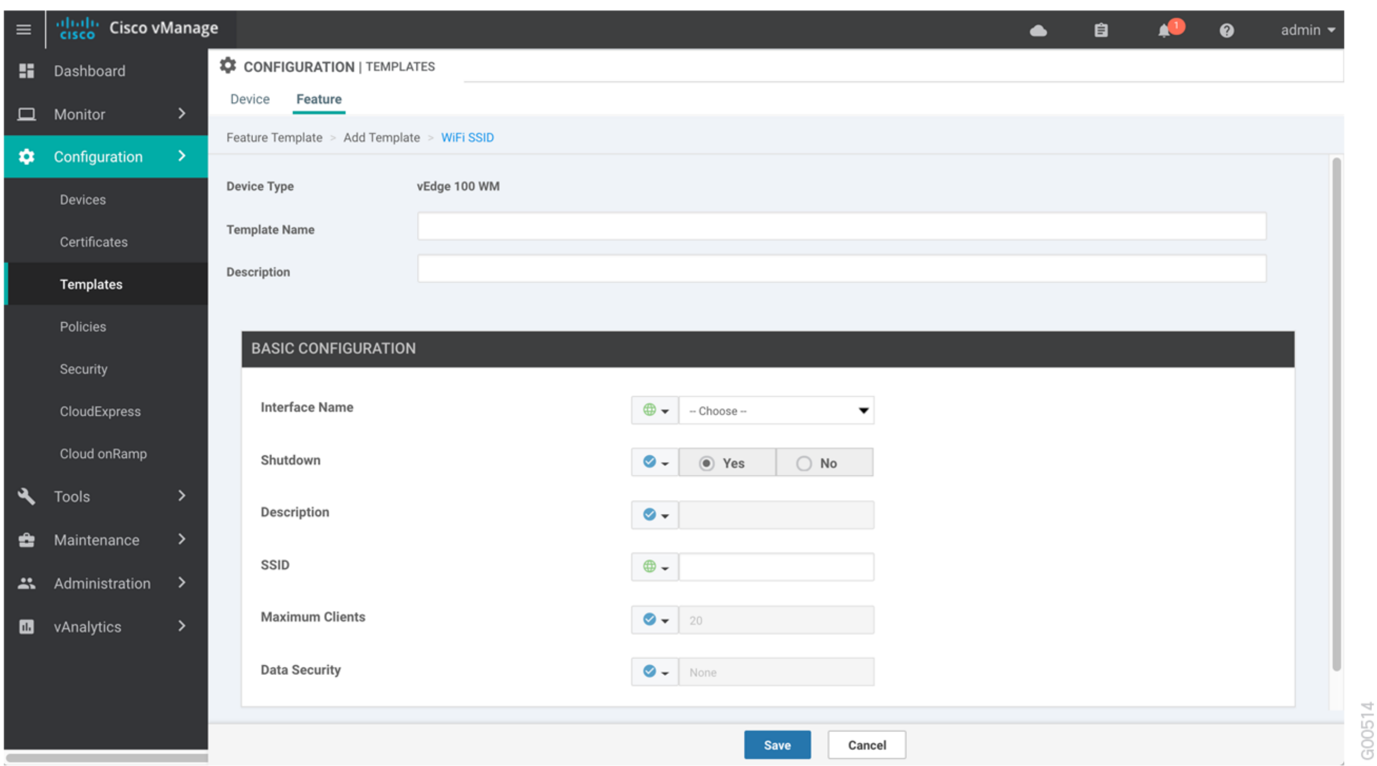
You can use the WiFi SSID template for all vEdge router devices that support wireless LANs (WLANs), including vEdge 100vm routers

To configure SSIDs on the WLAN radio using vManage templates:

1. Create a WiFi SSID template to configure the VAP interfaces to use as SSIDs, as described in this article.
2. Create a WiFi Radio template to configure WLAN radio parameters. See the Configuration ▶ Templates ▶ WiFi Radio help topic.
3. Create a Bridge template to assign the VAP interface to a bridging domain. See the Configuration ▶ Templates ▶ Bridge help topic.
4. Create a device template that incorporates the WiFi Radio feature template and the Wifi SSID feature template. See the Configuration ▶ Templates help topic.

## 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 a vEdge router model that supports wireless LANs (WLANs).
5. Click the WLAN tab located directly beneath the Description field, or scroll to the WLAN section.
6. Under Additional WiFi Radio Templates, located to the right of the screen, click WiFi SSID.




7. From the WiFi SSID drop-down, click Create Template. The WiFi SSID template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining WiFi SSID 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:

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

## WLAN SSID Configuration

To configure SSIDs on a vEdge router, configuring the following parameters in the Basic Configuration tab. Parameters marked with an asterisk are required to configure the SSIDs.

| Parameter Name | Description |
|---|---|
| Interface Name* | Select the VAP interface name. |
| Shutdown* | Click No to enable the interface. |
| Description (optional) | Enter a description for the interface. |
| SSID* | Enter the name of the SSID. It can be a string from 4 through 32 characters. The SSID must be unique.<br><br>You can configure up to four SSIDs.<br><br>Each SSID is called a virtual access point (VAP) interface. To a client, each VAP interfaces appears as a different access point (AP) with its own SSID. To provide access to different networks, assign each VAP to a different VLAN. |
| Maximum Clients | Enter the maximum number of clients allowed to connect to the WLAN.<br>*Range:* 1 through 50<br>*Default:* 25 |

| | |
|---|---|
| Data Security | Select the security type to enable user authentication or enterprise WPA security.<br><br>For user authentication, select from WPA Personal, WPA/WPA2 Personal, or WPA2 Personal, and then enter a clear text or an AES-encrypted key.<br><br>For enterprise security, select from WPA Enterprise, WPA/WPA2 Enterprise, or WPA2 Enterprise, and then enter a RADIUS server tag. |
| RADIUS Server | If you select one of the enterprise security methods based on using a RADIUS authentication server, enter the RADIUS server tag. |
| WPA Personal Key | If you select one of the personal security methods based on preshared keys, enter either a clear text or an AES-encrypted password. |
| Management Security | If you select one of the WPA2 security methods, select the encryption of management frames to be none, optional, or required. |

To save the feature template, click Save.

*CLI equivalent:*

```
wlan frequency
  interface vapnumber
    data-security security
    description text
    mgmt-security security
    radius-servers tag
    no shutdown
    ssid ssid
    wpa-personal-key password
```

## Release Information

Introduced in vManage NMS Release 16.3.

# Dashboard

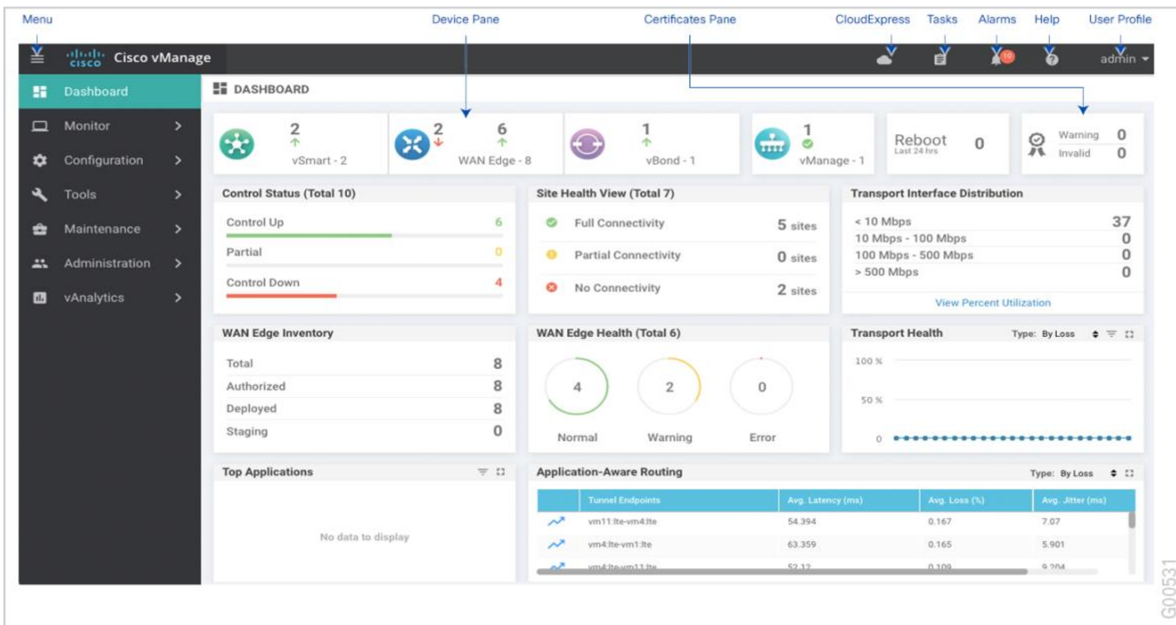
## Dashboard

Use the dashboard screen to monitor, at a glance, the overall health of the Viptela overlay network.

## Top Bar

The top bar is located at the top of every vManage screen and includes the following screen elements:

- Menu icon—Click the icon to expand or collapse the vManage menu. The vManage menu is closed by default.
- vManage application server logo. To change the logo, see [How to Load a Custom Logo onto the vManage Web Application Server.]()
- Cloud onRamp icon—Enables Cloud onRamp service to optimize access to cloud applications. When Cloud onRamp service is enabled, the icon turns blue.
- Tasks icon—Click on the icon to see a list of all active and completed tasks started from the vManage NMS. While the task is in progress, the Tasks tab displays a counter on the top. When the task is completed, the count disappears and Completed Tasks count is incremented. To view details about any task, click the task to display its Status screen.
- Alarm bell icon—Displays the total count of all active alarms. Click on the icon to see a list of all active and cleared alarms. To view details about any alarm, click the alarm to display its Alarms Details screen.
- Help—Links to product help, software version information about the vManage NMS software, and current time and timezone on the vManage server.
- Hostname—Hostname of the vManage NMS that you are logged into.
- User profile drop-down—Click to sign out or edit user-related options in your profile.



## Device Pane

The Device pane, which runs across the top of the Dashboard screen, displays all control connections from the vManage NMS to the vSmart controllers, WAN Edge routers, and vBond orchestrators in the overlay network. It also displays the status of the vManage NMSs in the network.

For each device, the Device pane shows:

- Total number of connections.
- Number of up connections.
- Number of down connections.

Click the number or the Up or Down arrow to display a table with detailed information for each connection. The Dashboard page automatically refreshes when the status of the members of a vManage cluster changes.

Click the More Actions icon to the right of each table row to access the Device Dashboard or Real Time view in the Monitor ► Network screen or to access the Tools ► SSH Terminal screen.

## Reboot Pane

The Reboot pane displays the total number of reboots in the last 24 hours for all devices in the network, including soft and cold reboots and reboots that occurred as a result of power-cycling a device. Click the Reboot pane to open the Reboot popup window which lists, for each reboot, the system IP and hostname of the device that rebooted, the time the reboot occurred, and the reason for the reboot. If the same device reboots more than each, each reboot option is reported separately.

In the Reboot popup window, click the Crashes tab to list, for all device crashes, the system IP and hostname of the device on which the crash occurred, the crash index, and the core time and filename.

## Certificates Pane

The Certificates pane displays the state of all certificates on all controller devices, and it shows a count of all expired or invalidated certificates. Click the Certificates pane to open the Certificate Details popup window, which displays the hostname and system IP of the device on which the certificate is installed, the certificate serial number, and its expiration date and status.

## Control Status Pane

The Control Status pane displays whether vSmart and WAN Edge devices are connected to the required number of vSmart controllers. Each vSmart controller must connect to all other vSmart controllers in the network. Each WAN Edge router must connect to the configured maximum number of vSmart controllers.

The Control Status pane shows three counts:

- Control Up—Total number of devices with the required number of operational control plane connections to a vSmart controller.
- Partial—Total number of devices with some, but not all, operational control plane connections to vSmart controllers.
- Control Down—Total number of devices with no control plane connection to a vSmart controller.

Click any row to display a table with device details. Click the More Actions icon to the right of each table row to access the Device Dashboard or Device Details view in the Monitor ► Network screen.

## Site Health View Pane

The Site Health View pane displays the state of a site's data connections. When a site has multiple WAN Edge routers, this pane displays the state for the entire site, not for individual devices. The Site Health View pane displays three states:

- Full WAN Connectivity—Total number of sites where all BFD sessions on all WAN Edge routers are in the up state.
- Partial WAN Connectivity—Total number of sites where a TLOC or a tunnel is in the down state. These sites still have limited data plane connectivity.
- No WAN Connectivity—Total number of sites where all BFD sessions on all WAN Edge routers are in the down state. These sites have no data plane connectivity.

Click a row to display a popup window with detailed information on each site, node, or tunnel. Click the More Actions icon to the right of each table row to access the Device Dashboard or Real Time view in the Monitor ► Network screen or the Tools ► SSH Terminal screen.

## Transport Interface Distribution

The Transport Interface Distribution pane displays interface usage in the last 24 hours for all WAN Edge interfaces in VPN 0. This includes all TLOC interfaces. Click a row to see details of interface usage.

## WAN Edge Inventory Pane

The WAN Edge Inventory pane provides four counts:

- Total—Total number of WAN Edge routers whose authorized serial number has been uploaded on the vManage server. The serial number is uploaded in the Configuration ► Devices screen.
- Authorized—Total number of authorized WAN Edge routers in the overlay network. These are routers marked as Valid in the Configuration ► Certificates ► WAN Edge List screen.
- Deployed—Total number of deployed WAN Edge routers. These are routers marked as Valid that are now operational in the network.
- Staging—Total number of WAN Edge routers in staging state. These are routers you configure at a staging site before shipping them to the actual branch and making them a part of the overlay network. These routers do not take part in any routing decisions nor do they affect network monitoring through the vManage NMS.

Click any row to display a table with the hostname, system IP, site ID, and other details of each router.

## WAN Edge Health Pane

The WAN Edge Health pane displays an aggregated view for each router state and a count of how many WAN Edge routers are in that state, thereby describing the health of the hardware nodes. The three states are:

- Normal—Number of routers with memory, hardware, and CPU in normal state. Using less than 70% of total memory or total CPU is classified as normal.
- Warning—Number of routers with memory, hardware, or CPU in warning state. Using between 70% and 90% of total memory or total CPU is classified as a warning.
- Error—Number of routers with memory, hardware, or CPU in error state. Using more than 90% of total memory or total CPU is classified as an error.

Click the number or the state to display a table with the last 12 or 24 hours of memory usage, CPU utilization, and hardware-related alarms, including temperature, power supply, and PIM modules. Click the More Actions icon to the right of each table row to access the Device Dashboard or Device Details view in the Monitor ► Network screen or the Tools ► SSH Terminal screen.

## Transport Health Pane

The Transport Health pane displays the aggregated average loss, latency, and jitter for all links and all combinations of colors (for example, all LTE-to-LTE links, all LTE-to-3G links).

From the Type drop-down, select loss, latency, or jitter.

Click the Filter icon to select a time period for which to display data.

Click the Expand icon to open the Transport Health pop-up window. This full-screen window displays a more detailed view of the same information. To display the information in tabular format, click the Details tab. You can change the displayed type and time period as described above.

## Top Applications Pane

The Top Applications pane displays DPI flow information for traffic transiting WAN Edge routers in the overlay network.

Click the Filter icon to select a time period for which to display data. From the VPN drop-down list, select a VPN to display DPI information for all flows in that VPN.

Click the Expand icon to open the Top Applications pop-up window. This full-screen window displays a more detailed view of the same information. You can change the VPN and time period as described above.

## Application-Aware Routing Pane

The Application-Aware Routing pane displays the 10 worst tunnels based on criteria you specify from the Type drop-down list, including loss, latency, and jitter. So, if you choose loss, this pane shows the ten tunnels with the greatest average loss over the last 24 hours.

Click any row to display a graphical representation of the data. Select a time period for which to display data or click Custom to display a drop-down for specifying a custom time period.

Click the Expand icon to open the Application-Aware Routing pop-up window. This full-screen window displays the 25 worst tunnels based on criteria you specify from the Type drop-down list, including loss, latency, and jitter.

## FireWall Enforcement Pane

The FireWall Enforcement pane displays the number of sessions that were inspected or dropped over the specified time period.

Click the Filter icon to select a time period for which to display data.

Click the Expand icon to open the FireWall Enforcement pop-up window. This full-screen window displays a more detailed view of the same information. To display the information in tabular format, click the Details tab. You can change the time period as described above.

## Top Signature Hits Pane

The Top Signature Hits pane displays the Intrusion Prevention System (IPS) signature violations by severity or by count over the specified time period.

Click the Filter icon to select a time period for which to display data.

Click the Expand icon to open the Top Signature Hits pop-up window. This full-screen window displays a more detailed view of the same information. To display the information in tabular format, click the Details tab. You can change the time period as described above.

## URL Filtering Pane

The URL Filtering pane displays the number and types of URLs that were blocked or allowed over the specified time period.

Click the Filter icon to select a time period for which to display data.

Click the Expand icon to open the URL Filtering pop-up window. This full-screen window displays a more detailed view of the same information. To display the information in tabular format, click the Details tab. You can change the time period as described above.

## Web Server Certificate Expiration Date Notification

When you establish a secure connection between your web browser and the vManage server using authentication certificates, you configure the time period for which the certification is valid, in the Administration ► Settings screen. At the end of this time period, the certificate expires. The Web Server Certificate bar shows the expiration date and time.

Starting 60 days before the certificate expires, the vManage Dashboard displays a notification indicating that the certificate is about to expire. This notification is then redisplayed 30, 15, and 7 days before the expiration date, and then daily.

## Maintenance Window Alert Notification

If an upcoming maintenance window is configured on the vManage server, in the Administration ► Settings screen, the vManage Dashboard displays a maintenance window alert notification two days before the start of the window.

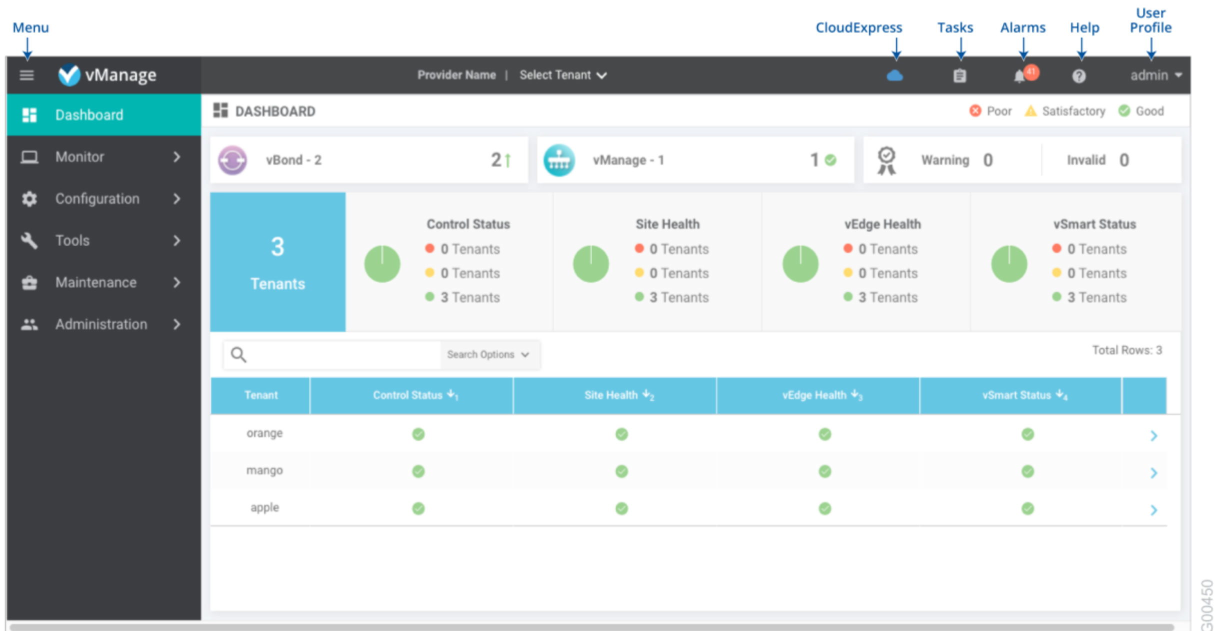
## Multitenant Dashboard

Use the multitenant dashboard screen to monitor, at a glance, the overall health of all tenants being managed by a single vManage NMS server.

## Top Bar

The top bar is located at the top of every vManage multitenant screen and includes the following screen elements:

- Menu icon—Click the icon to expand or collapse the vManage menu. The vManage menu is closed by default.
- vManage application server logo. To change the logo, see How to Load a Custom Logo onto the vManage Web Application Server.
- Provider Name—Displays the service provider name. Click the Select Tenant drop-down to display information for a single tenant.
- Alarm bell icon—Displays the total count of all active alarms. Click on the icon to see a list of all active and cleared alarms. To view details about any alarm, click the alarm to display its Alarms Details screen.
- Tasks icon—Click on the icon to see a list of all active and completed tasks started from the vManage NMS. While the task is in progress, the Tasks tab displays a counter on the top. When the task is completed, the count disappears and Completed Tasks count is incremented. To view details about any task, click the task to display its Status screen.
- Help—Links to product help, software version information about the vManage NMS software, and current time and timezone on the vManage server.
- Hostname—Hostname of the vManage NMS that you are logged into.
- User profile drop-down—Click to sign out or edit user-related options in your profile.




## Provider Dashboard

If you click Provider Name in the Top Bar, the Multitenant Dashboard shows the following components:

- Device Pane—Runs across the top of the Multitenant Dashboard screen. The Device pane displays the total number control connections from the vManage NMS to the vBond orchestrators and vManage NMSs in the overlay networks of all the tenants, and the number of up and down connections. Click the number or the Up or Down arrow to display a table with detailed information for each connection. This pane also displays the number of warning messages and the number of invalid certificates.
- Tenants Pane—Displays the total number of tenants and a summary of the control status, site health, vEdge router health, and vSmart controller status for all tenants.
- Search box—Includes the Search Options drop-down, for a Contains or Match string.
- Table of tenants in the overlay network—To re-arrange the columns, drag the column title to the desired position.

## Tenant Dashboard

If you select a tenant from the Provider Name drop-down in the Top Bar, the Multitenant Dashboard shows the components described below.

### Device Pane

The Device pane, which runs across the top of the Dashboard screen, displays all control connections from the vManage NMS to the vSmart controllers and vEdge routers in the tenant's overlay network. It also displays the status of the vManage NMSs in the network.

For each device, the Device pane shows:

- Total number of connections.
- Number of up connections.

- Number of down connections.

Click the number or the Up or Down arrow to display a table with detailed information for each connection. Click the More Actions icon to the right of each table row to access the Device Dashboard or Real Time view in the Monitor ► Network screen or to access the Tools ► SSH Terminal screen.

## Reboot Pane

The Reboot pane displays the total number of reboots in the last 24 hours for all devices in the network, including soft and cold reboots and reboots that occurred as a result of power-cycling a device. Click the Reboot pane to open the Reboot popup window which lists, for each reboot, the system IP and hostname of the device that rebooted, the time the reboot occurred, and the reason for the reboot. If the same device reboots more than each, each reboot option is reported separately.

In the Reboot popup window, click the Crashes tab to list, for all device crashes, the system IP and hostname of the device on which the crash occurred, the crash index, and the core time and filename.

## Control Status Pane

The Control Status pane displays whether vSmart and vEdge devices are connected to the required number of vSmart controllers. Each vSmart controller must connect to all other vSmart controllers in the network. Each vEdge router must connect to the configured maximum number of vSmart controllers.

The Control Status pane shows three counts:

- Control Up—Total number of devices with the required number of operational control plane connections to a vSmart controller.
- Partial—Total number of devices with some, but not all, operational control plane connections to vSmart controllers.
- Control Down—Total number of devices with no control plane connection to a vSmart controller.

Click any row to display a table with device details. Click the More Actions icon to the right of each table row to access the Device Dashboard or Device Details view in the Monitor ► Network screen.

## Site Health View Pane

The Site Health View pane displays the state of a site's data connections. When a site has multiple vEdge routers, this pane displays the state for the entire site, not for individual devices. The Site Health View pane displays three states:

- Full Connectivity—Total number of sites where all BFD sessions on all vEdge routers are in the up state.
- Partial Connectivity—Total number of sites where a TLOC or a tunnel is in the down state. These sites still have limited data plane connectivity.
- No Connectivity—Total number of sites where all BFD sessions on all vEdge routers are in the down state. These sites have no data plane connectivity.

Click a row to display a popup window with detailed information on each site, node, or tunnel. Click the More Actions icon to the right of each table row to access the Device Dashboard or Real Time view in the Monitor ► Network screen or the Tools ► SSH Terminal screen.

## Transport Interface Distribution Pane

The Transport Interface Distribution pane displays interface usage in the last 24 hours for all vEdge interfaces in VPN 0. This includes all TLOC interfaces. Click a row to see details of interface usage.

## vEdge Inventory Pane

The vEdge Inventory pane provides four counts:

- Total—Total number of vEdge routers whose authorized serial number has been uploaded on the vManage server. The serial number is uploaded in the Configuration ► Devices screen.
- Authorized—Total number of authorized vEdge routers in the overlay network. These are routers marked as Valid in the Configuration ► Certificates ► vEdge List screen.
- Deployed—Total number of deployed vEdge routers. These are routers marked as Valid that are now operational in the network.
- Staging—Total number of vEdge routers in staging state. These are routers you configure at a staging site before shipping them to the actual branch and making them a part of the overlay network. These routers do not take part in any routing decisions nor do they affect network monitoring through the vManage NMS.

Click any row to display a table with the hostname, system IP, site ID, and other details of each router.

## vEdge Health Pane

The vEdge Health pane displays an aggregated view for each router state and a count of how many vEdge routers are in that state, thereby describing the health of the hardware nodes. The three states are:

- Normal—Number of routers with memory, hardware, and CPU in normal state. Using less than 70% of total memory or total CPU is classified as normal.
- Warning—Number of routers with memory, hardware, or CPU in warning state. Using between 70% and 90% of total memory or total CPU is classified as a warning.
- Error—Number of routers with memory, hardware, or CPU in error state. Using more than 90% of total memory or total CPU is classified as an error.

Click the number or the state to display a table with the last 12 or 24 hours of memory usage, CPU utilization, and hardware-related alarms, including temperature, power supply, and PIM modules. Click the More Actions icon to the right of each table row to access the Device Dashboard or Device Details view in the Monitor ► Network screen or the Tools ► SSH Terminal screen.

## Transport Health Pane

The Transport Health pane displays the aggregated average loss, latency, and jitter for all links and all combinations of colors (for example, all LTE-to-LTE links, all LTE-to-3G links).

From the Type drop-down, select loss, latency, or jitter.

Click the Filter icon to select a time period for which to display data.

Click the Expand icon to open the Transport Health pop-up window. This full-screen window displays a more detailed view of the same information. To display the information in tabular format, click the Details tab. You can change the displayed type and time period as described above.

## Top Applications Pane

The Top Applications pane displays DPI flow information for traffic transiting vEdge routers in the overlay network.

Click the Filter icon to select a time period for which to display data. From the VPN drop-down list, select a VPN to display DPI information for all flows in that VPN.

Click the Expand icon to open the Top Applications pop-up window. This full-screen window displays a more detailed view of the same information. You can change the VPN and time period as described above.

## Application-Aware Routing Pane

The Application-Aware Routing pane displays the 10 worst tunnels based on criteria you specify from the Type drop-down list, including loss, latency, and jitter. So, if you choose loss, this pane shows the ten tunnels with the greatest average loss over the last 24 hours.

Click any row to display a graphical representation of the data. Select a time period for which to display data or click Custom to display a drop-down for specifying a custom time period.

Click the Expand icon to open the Application-Aware Routing pop-up window. This full-screen window displays the 25 worst tunnels based on criteria you specify from the Type drop-down list, including loss, latency, and jitter.

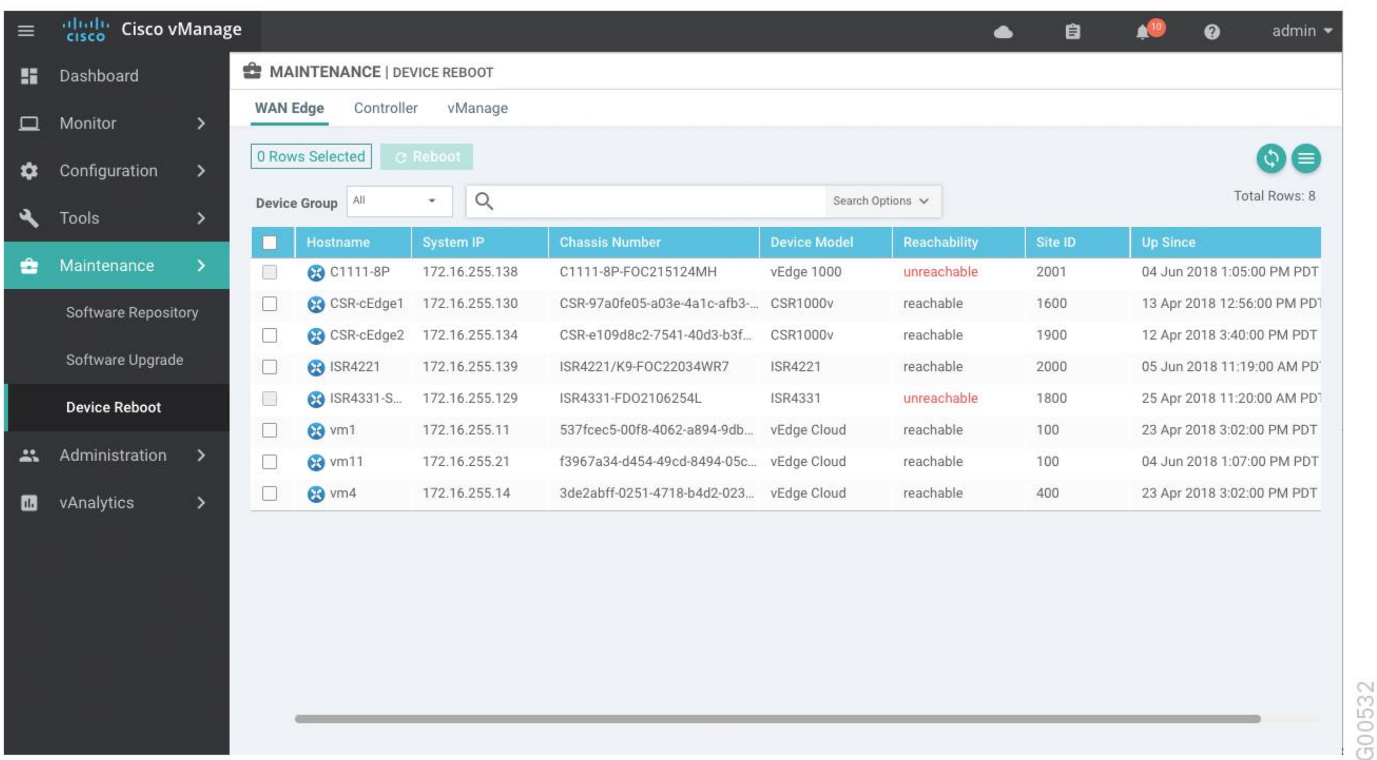
# Maintenance

## Device Reboot

Use the Device Reboot screen to reboot one or more Viptela devices.

## Screen Elements

- Top bar—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.
- Title bar—Includes the title of the screen, Device Reboot.
- vEdge tab bar—Includes the Controller and vManage tabs.
- Reboot button—Select a device from the table to activate the button and reboot the device. The Rows Selected box displays the number of rows selected in the table.
- Device Group drop-down—List of all configured device groups in the network.
- Search box—Includes the Search Options drop-down, for a Contains or Match string.
- Refresh icon—Click to refresh data in the device table with the most current data.
- Show Table Fields icon—Click to display or hide columns from the device table. By default, all columns are displayed.
- Table of devices in the overlay network—To re-arrange the columns, drag the column title to the desired position.



## Reboot a Device

To reboot one or more Viptela device in the overlay network:

1. In the title bar, click vEdge, Controller, or vManage.
2. Select one or more devices.
3. Click the Reboot button.

## View Active Devices

To view a list of devices on which the reboot operation has been performed:

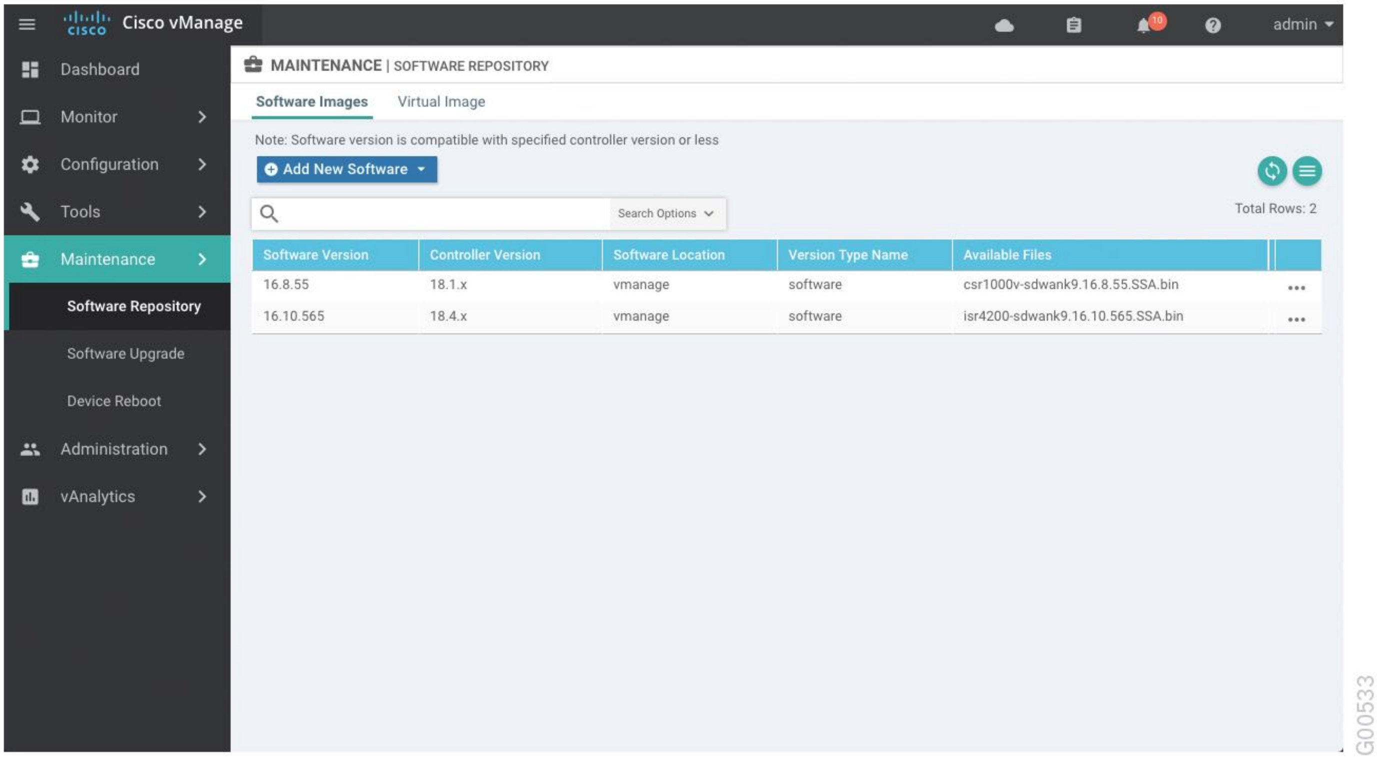
1. Click the Tasks icon located in the vManage toolbar. vManage NMS displays a list of all running tasks along with the total number of successes and failures.
2. Click a row to see details of a task. vManage NMS opens a status window displaying the status of the task and details of the device on which the task was performed.

## Software Repository

Use the Software Repository screen to download software images to the vManage software repository.

## Screen Elements

- Top bar—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.
- Title bar—Includes the title of the screen, Software Repository.
- Add New Software drop-down (on Repository screen)—Upload new software images to the vManage or remote server.
- Search box—Includes the Search Options drop-down, for a Contains or Match string.
- Refresh icon—Click to refresh data in the device table with the most current data.
- Show Table Fields icon—Click to display or hide columns from the device table. By default, all columns are displayed.
- Software repository table—List the images in the vManage software repository.




## View Software Images

When you open the Software Repository screen, the images in the repository are displayed in the table. To filter the list, search or type a string in the Search box.

The Software Version column lists the version of the software image, and the Controller Version column lists the version of controller software that is equivalent to the software version. The controller version is the minimum supported vManage controller version. The software image can operate with the listed controller version or with a higher controller version. In the following example:

| Software Version | Controller Version | Software Location | Version Type Name | Available Files | Updated On |
|---|---|---|---|---|---|
| 16.8.55 | 18.1.x | vmanage | software | csr1000v-sdwank9.16.8.55.SSA.bin | 20 Jun 2018 10:48:35 AM PDT |

The software version is 16.8.55, and the controller version is 18.1.x. Reading these two columns together tells you that software version 16.8.55 is compatible with vManage controller software versions 18.1.x and later. This means that devices running version 16.8.55 can operate with vManage servers running Releases 18.1, 18.2, and 18.3, and with later software releases, and they cannot operate with vManage servers running Release 17.2 or Release 17.1.

The Software Location column indicates where the software images are stored, either in the repository on the vManage server or in a repository in a remote location.

The Available Files column lists the names of the software image files.

The Update On column shows when the software image was added to the repository.

In the More Actions column, you can delete a software image from the repository.

# Add Software Images to the Repository

Before you can upgrade the software on a vEdge router, vSmart controller, or vManage NMS to a new software version, you need to add the software image to the vManage software repository. The repository allows you to store software images on the local vManage server and on a remote file server.

The vManage software repository allows you to store images in three ways:

- On the local vManage server, to be downloaded over a control plane connection—Here, the software images are stored on the local vManage server, and they are downloaded to the Viptela devices over a control plane connection. The receiving device generally throttles the amount of data traffic it can receive over a control plane connection, so for large files, the vManage server might not be able to monitor the software installation on the device even though it is proceeding correctly.
- On the local vManage server, to be downloaded over an out-of-band connection—Here, the software images are stored on the local vManage server, and they are downloaded to the Viptela devices over an out-of-band management connection. For this method to work, you specify the IP address of the out-of-band management interface when you copy the images to the software repository. This method is recommended when the software image files are large, because it bypasses any throttling that the device might perform and so the vManage server is able to monitor the software installation.
- On a remote server—Here, the software images remain on a remote file server that is reachable through an FTP or HTTP URL. As part of the software upgrade process, the vManage server sends this URL to the Viptela device, which then establishes a connection to the file server over which to download the software images.

To add software images to the vManage software repository:

1. Click Add New Software.
2. Select the location to store the software image:
    a. To store the software image on the local vManage server and have it be downloaded to Viptela devices over a control plane connection, select vManage. The Upload Software to vManage dialog box opens.
        i. Drag and drop the software image file to the dialog box, or click Browse to select the software image from a directory on the local vManage server.
        ii. Click Upload to add the image to the software repository. The Software Repository tables displays the added software image, and it is available for installing on the devices.
    b. To store the software image on a remote server, select Remote Server. The Location of Software on Remote Server dialog box opens.
        i. In the Version box, enter the version number of the software image.
        ii. In the URL box, enter the FTP or HTTP URL of the software image.
        iii. Click Add to add the image to the software repository. The Software Repository tables displays the added software image, and it is available for installing on the devices.
    c. To store the image on a remote vManage server and have it be downloaded to Viptela devices over an out-of-band management connection, select Remote Server - vManage. The Upload Software to Remote Server - vManage dialog box opens.
        i. In the vManage Hostname box, enter the IP address of an interface on the vManage server that is in a management VPN (typically, VPN 512).
        ii. Drag and drop the software image file to the dialog box, or click Browse to select the software image from a directory on the local vManage server.
        iii. Click Upload to add the image to the software repository. The Software Repository tables displays the added software image, and it is available for installing on the devices.

## Delete a Software Image from the Repository

To delete a software image from the vManage software repository:

1. In the software repository table, select the software image.
2. In the More actions icon to the right of the line, click Delete.

If a software image is being download to a router, you cannot delete the image until the download process completes.

## Software Upgrade

Use the Software Upgrade screen to download new software images and to upgrade the software image running on a Viptela device.

From a centralized vManage NMS, you can upgrade the software on Viptela devices in the overlay network and reboot them with the new software. You can do this for a single device or for multiple devices simultaneously.

When you upgrade a group of vBond orchestrators, vSmart controllers, and vEdge routers, the software upgrade and reboot is performed first on the vBond orchestrator, next on the vSmart controllers, and finally on the vEdge routers. For vEdge routers, up to five routers can be upgraded and rebooted in parallel at the same time.

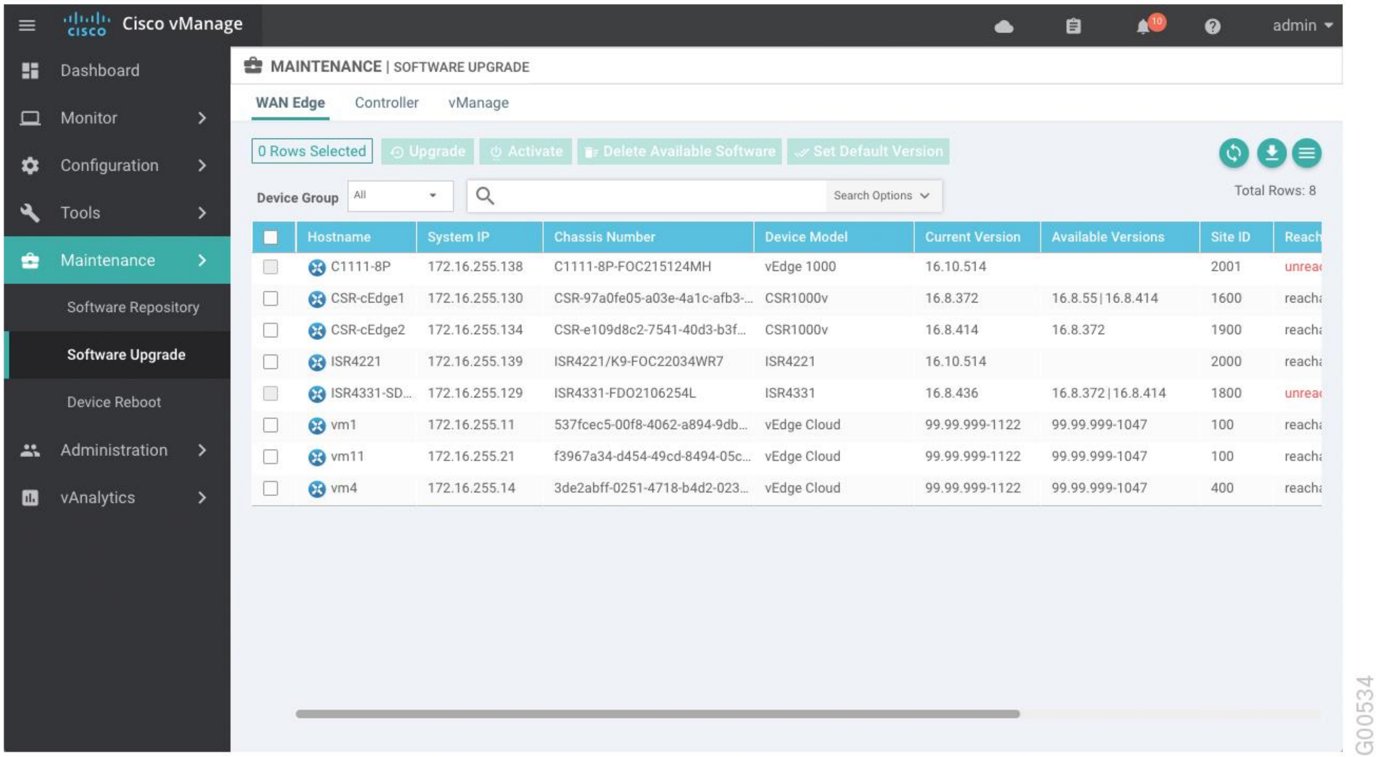
You cannot include the vManage NMS in a group software upgrade operation. You must upgrade and reboot the vManage server by itself.

It is recommended that you perform all software upgrades from the vManage NMS rather than from the CLI.

### Screen Elements

- Top bar—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.
- Title bar—Includes the title of the screen, Software Upgrade.
- Device List drop-down—Displays the list of devices in the overlay network. When you first open the Software Upgrade screen, Device List is selected by default.
  - WAN Edge tab bar—Includes the Controller and vManage tabs.
  - Rows Selected—Displays the number of rows selected from the table. Includes:
    - Upgrade button—Installs a new software version on the device. Includes:
    - Activate button—Reboots the device and activates the new software version.
    - Delete Available Software button—Delete a software version from a device.
    - Set Default Version button—Set a software image to be the default image on the device.
  - Device Group drop-down—List of all configured device groups in the network.
  - Table of devices in the overlay network—To re-arrange the columns, drag the column title to the desired position.
- Repository drop-down—Click Repository from the Device List drop-down to display the list of software images on the vManage or remote server.
  - Add New Software drop-down (on Repository screen)—Upload new software images to the vManage or remote server.
  - Table of software images—To re-arrange the columns, drag the column title to the desired position.
- Search box—Includes the Search Options drop-down, for a Contains or Match string.
- Refresh icon—Click to refresh data in the device table with the most current data.

- Export icon—Click to download all data to a file, in CSV format (on Device List screen only).
- Show Table Fields icon—Click to display or hide columns from the device table. By default, all columns are displayed.




## View Software Images

To view a list of software images in the repository on the vManage server or on a remote server, from the Device List drop-down, click Repository.

## Upgrade a Software Image

To upgrade the software image on a device:

1. In the title bar, click the WAN Edge, Controller, or vManage tab.
2. Select one or more devices on which to upgrade the software image.
3. Click the Upgrade button. The Software Upgrade dialog box opens.
4. Select the software version to install on the device. If the software is located on a Remote Server, select the VPN in which the software image is located.
5. To automatically activate the new software version and reboot the device, select the Activate and Reboot checkbox.
6. Click Upgrade. A progress bar indicates the status of the software upgrade.

If the control connection to the vManage NMS does not come up within the configured time limit, vManage NMS automatically reverts the device to the previously running software image. The configured time limit for all Viptela devices to come up after a software upgrade is 5 minutes, except for vEdge 100 routers, which have a default time of 12 minutes.

Note: If you upgrade the vEdge software to a version higher than that running on a controller device, a warning message is displayed that software incompatibilities might occur. It is recommended that you upgrade the controller software first, before upgrading the vEdge software.

## Activate a New Software Image

If you did not select the Activate and Reboot checkbox when upgrading the software image, the device continues to use the existing configuration. To activate the new software image:

1. In the title bar, click the vEdge, Controller, or vManage tab.
2. Select one or more devices on which to activate the new software image.
3. Click the Activate button. The Activate Software dialog box opens.
4. Select the software version to activate on the device.
5. Click Activate. vManage NMS reboots the device and activates the new software image.

If the control connection to the vManage NMS does not come up within the configured time limit, vManage NMS automatically reverts the device to the previously running software image. The configured time limit for all Viptela devices to come up after a software upgrade is 5 minutes, except for the vEdge 100 routers, which have a default time of 12 minutes.

## Delete a Software Image

To delete a software image from a Viptela device:

1. In the title bar, click the WAN Edge, Controller, or vManage tab.
2. Select one or more devices from which to delete a software image.
3. Click the Delete Available Software button. The Delete Available Software dialog box opens.
4. Select the software version to delete.
5. Click Delete.

## Set the Default Software Version

You can set a software image to be the default image on a Viptela device. Performing this operation overwrites the factory-default software image, replacing it with an image of your choosing. It is recommended that you set a software image to be the default only after verifying that the software is operating as desired on the device and in your network.

To set a software image to be the default image on a device:

1. In the title bar, click the vEdge, Controller, or vManage tab.
2. Select one or more devices on which you wish to change the default software image.
3. Click the Set Default Version button. The Set Default Version dialog box opens.
4. From the Version drop-down, select the software image to use as the default.
5. Click Set Default.

## Export Device Data in CSV Format

To export data for all devices to a file in CSV format, click the Export button. This icon, which is a downward-pointing arrow, is located to the right of the filter criteria both in the WAN Edge List and in the Controllers tab.

vManage NMS downloads all data from the device table to an Excel file in CSV format. The file is downloaded to your brower's default download location and is named viptela_download.csv.

## View Log of Software Upgrade Activities

To view the status of software upgrades and a log of related activities:

1. Click the Tasks icon located in the vManage toolbar. vManage NMS displays a list of all running tasks along with the total number of successes and failures.
2. Click a row to see details of a task. vManage NMS opens a status window displaying the status of the task and details of the device on which the task was performed.

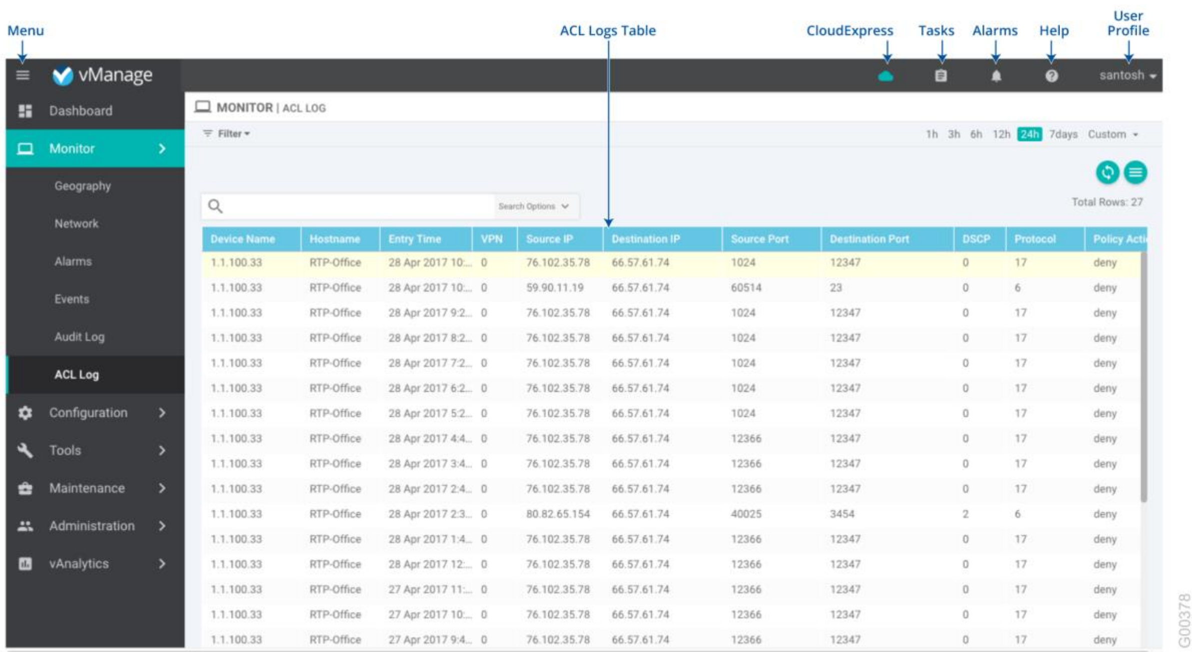
# Monitor

## ACL Log

Use the ACL Log screen to view logs for access lists (ACLs) configured on a vEdge router. Routers collect ACL logs every 10 minutes.

## Screen Elements

- Top bar—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.
- Title bar—Includes the title of the screen, ACL Log.
- Filter bar—Includes the Filter drop-down and time periods. Click the Filter icon to display a drop-down menu to add filters for ACL logs. Click a predefined or custom time period for which to display data.
- Search box—Includes the Search Options drop-down, for a Contains or Match string.
- Refresh icon—Click to refresh data in the ACL logs table with the most current data.
- Show Table Fields icon—Click to display or hide columns from the ACL logs table. By default, all columns are displayed.
- Table of ACL logs—To re-arrange the columns, drag the column title to the desired position.




## Set ACL Log Filters

To set filters for searching ACL logs:

1. Click the Filter drop-down menu.
2. In the VPN drop-down, select the entity for which you are collecting ACL logs. You can select only one VPN.

3. Click Search to search for logs that match the filter.

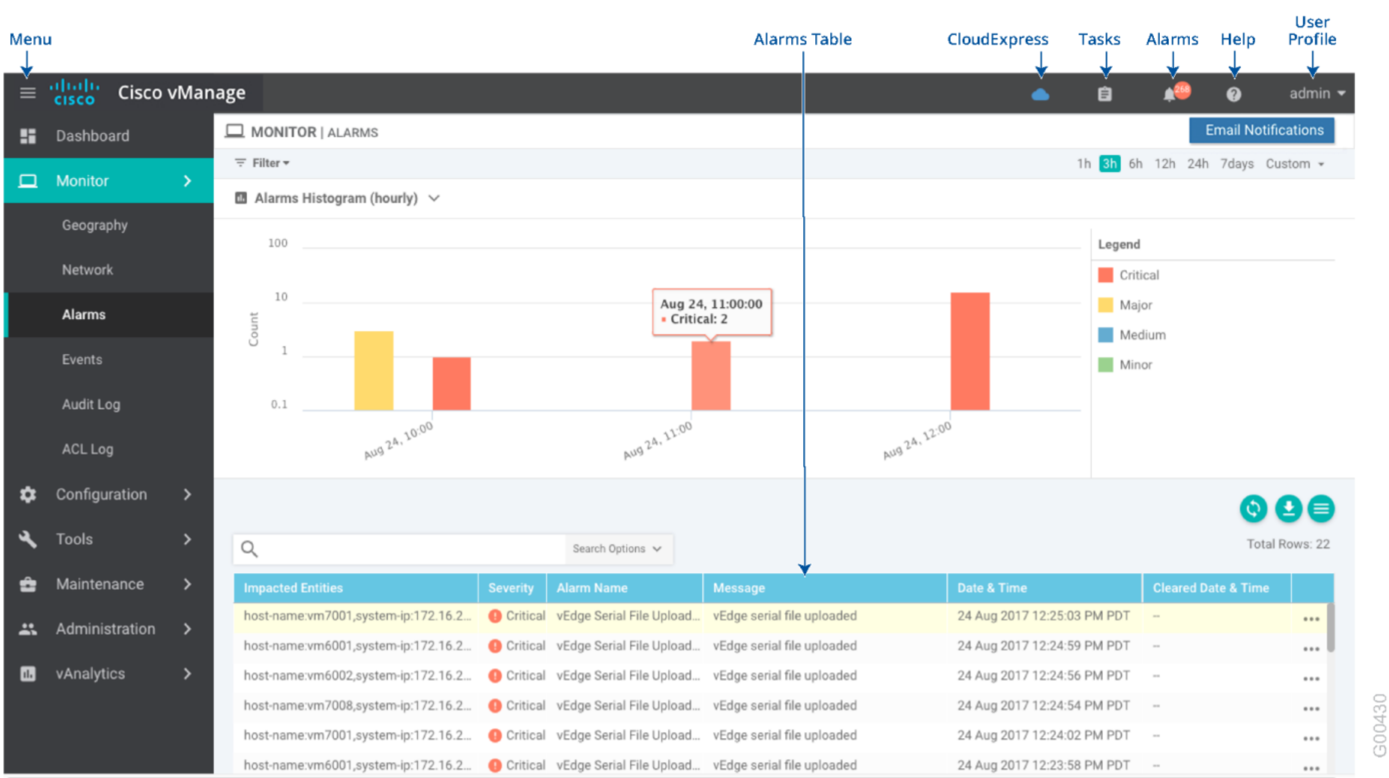
vManage NMS displays a log of activities in table format.

# Alarms

Use the Alarms screen to display detailed information about alarms generated by controllers and routers in the overlay network.

## Screen Elements

- Top bar—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.
- Title bar—Includes the title of the screen, Alarms.
  - Email Notifications—Send email notifications when the vManage server generates alarms.
- Filter bar—Includes the Filter drop-down and time periods. Click the Filter icon to display a drop-down menu to add filters for searching alarms. Click a predefined or custom time period for which to display data.
- Alarms Histogram—Displays a graphical representation of all alarms in order of severity: Critical, Major, Medium, Minor. To hide the alarms histogram, click the Alarms Histogram title or the down angle bracket to the right of it.
- Search box—Includes the Search Options drop-down, for a Contains or Match string.
- Refresh icon—Click to refresh data in the alarms table with the most current data.
- Export icon—Click to download all data to a file, in CSV format.
- Show Table Fields icon—Click to display or hide columns from the alarms table. By default, all columns are displayed.
- Table of alarms—To re-arrange the columns, drag the column title to the desired position.



## Set Alarm Filters

To set filters for searching alarms generated by one or more Viptela devices:

1. Click the Filter drop-down menu.
2. In the Severity drop-down, select the alarm severity level. You can specify more than one severity level.
3. In the Active drop-down, select active, cleared, or both types of alarm. Active alarms are alarms that are currently on the device but have not been acknowledged.
4. Click the Alarm Name drop-down, select the name of the alarm. You can specify more than one alarm name.
5. Click Search to search for alarms that match the filter.

vManage NMS displays the alarms both in table and graphical format.

## Export Alarm Data in CSV Format

To export data for all alarms to a file in CSV format, click the Export icon. This icon, which is a downward-pointing arrow, is located to the right of the Search box below the Alarms Histogram.

vManage NMS downloads all data from the alarms table to an Excel file in CSV format. The file is downloaded to your browser's default download location and is named viptela_download.csv.

## View Alarm Details

To view detailed information about any alarm:

1. Select the alarm row from the table.
2. Click the More Actions icon to the right of the row and click Alarm Details.

The Alarms Details window opens, displaying the possible cause of the alarm, impacted entities, and other details.

## Send Alarm Notifications

To send email notifications when alarms occur:

1. In the vManage Administration ► Settings screen, ensure that Email Notifications is enabled.
2. In the Monitor ► Alarms screen, click Email Notifications. A list of configured notifications is displayed in the email notifications table.
3. Click Add Email Notification.
4. In the Name field, enter a name for the email notification. The name can be up to 128 characters and can contain only alphanumeric characters.
5. In the Severity drop-down, select one or more alarm severity levels, from Critical, Major, Medium, and Minor.
6. In the Alarm Name drop-down, select one or more alarms. The alarms generated for each severity level are listed in the section Alarms Generated on vManage NMS, below.
7. In Account Details, enter the email addresses to receive email notifications:

a. Click Add New Email List.

b. In the Email List popup, click Add Email.

c. Enter the email address of a user.

d. Add additional email addresses as desired.

e. Click Save.

8. In the Email Threshold field, set the maximum number of emails to be sent per minute. The number can be a value from 1 through 30. The default is 5.

9. Click the Webhook box to trigger an HTTP callback when an alarm notification event occurs:

a. Enter the username and password to authenticate the webhook server.

b. Enter the URL of the webhook server.

10. Select the routers to which the alarm notification applies, either All Devices or a custom list. If you select Custom, a device list is displayed:

a. In the Available Devices table on the left, select one or more devices.

b. Click the right-point arrow to move the devices to the Selected Devices table on the right.

11. Click Add.

## View an Email Notification

1. Click Email Notifications.
2. For the desired email notification, click the View icon to the right of the row.
3. When you are done viewing the notification, click OK.

## Edit an Email Notification

1. Click Email Notifications.
2. For the desired email notification, click the Pencil icon to the right of the row.
3. When you are done editing the notification, click Update.

## Delete an Email Notification

1. Click Email Notifications.
2. For the desired email notification, click the Trash Bin icon to the right of the row.
3. In the confirmation popup, click OK.

## Alarms Generated on vManage NMS

The table below lists the alarms that the vManage NMS software generates. The software generates alarms when a state or condition changes, such as when a software component starts, transitions from down to up, or transitions from up to down. The severity indicates the seriousness of the alarm. When you you create email notifications, the severity that you configure in the notification determines which alarms you can receive email notifications about.

| Alarm Name | Severity | Description |
|---|---|---|
| AAA Admin Password Change | Critical | The password for the AAA user **admin** changed on a router or controller. |
| BFD Between Sites Down | Critical | All BFD sessions on all routers between two sites are in the Down state. This means that no data traffic can be sent to or transmitted between those two routers. |
| BFD Between Sites Up | Medium | A BFD session on a router between two sites transitioned to the Up state. |
| BFD Node Down | Critical | All BFD sessions for a router are in the Down state. This means that no data traffic can be sent to or transmitted from that router. |
| BFD Node Up | Medium | A BFD session for a router transitioned to the Up state. |
| BFD Site Down | Critical | All BFD sessions on all vEdge routers in a site are in the Down state. This means that no data traffic can be sent to or transmitted from that site. |
| BFD Site Up | Medium | A BFD session on a router in a site transitioned to the Up state. |
| BFD TLOC Down | Major | All BFD sessions for a TLOC (transport tunnel identified by a color) are in the Down state. This means that no data traffic can be sent to or transmitted from that transport tunnel. |
| BFD TLOC Up | Medium | A BFD session for a TLOC transitioned to the Up state. |
| BGP Router Down | Critical | All BGP sessions on a router are in the Down state. |
| BGP Router Up | Medium | A BGP session on a router transitioned to the Up state. |
| Clear Installed Certificate | Critical | All certificates on a controller or device, including the public and private keys and the root certificate, have been cleared, and the device has returned to the factory-default state. |
| Cloned vEdge Detected | Critical | A duplicate router that has the same chassis and serial numbers and the same system IP address has been detected. |
| Cloud onRamp | Major | The Cloud onRamp service was started on a router. |
| Control All vSmarts Down | Critical | All control connections from all vSmart controllers in the overlay network are in the Down state. This means that the overlay network cannot function. |
| Control Node Down | Critical | All control connections for a vEdge router are in the Down state. |
| Control Node Up | Medium | At least one control connection for a vEdge router transitioned to the Up State. |
| Control Site Down | Critical | All control connections from all Viptela devices in a site are in the Down state.This means that no control or data traffic can be sent to or transmitted from that site. |
| Control Site Up | Medium | A control connection from the vManage NMS and the vBond orchestrator in the site transitioned to the Up state. |
| Control vBond State Change | Critical Major | A control connection on a vBond orchestrator transitioned to the Down state (Critical) or the Up state (Major). |
| Control TLOC Down | Major | All control connections for a TLOC are in the Down state. |
| Control TLOC Up | Medium | A control connection for a TLOC is in the Up state. |

| | | |
|---|---|---|
| Control vManage Down | Critical | All control connections from a vManage NMS are in the Down state. |
| Control vManage Up | Medium | A control connection from a vManage NMS transitioned to the Up state. |
| Control vSmart Down | Critical | All control connections from a vSmart controller in the overlay network are in the Down state. |
| Control vSmart Up | Medium | A control connection from a vSmart controller in the overlay network transitioned to the Up state. |
| Control vSmarts Up | Medium | Control connection from all vSmart controllers in the overlay network transition to the Up state. |
| CPU Load | Critical<br>Medium | The CPU load on a controller or device has reached a critical level that could impair or shut down functionality, or a medium level that could impair functionality. |
| Default App List Update | Major | The default application and application family lists, which are used in application-aware routing policy, have changed. |
| Device Activation Failed | Critical | Activation of a software image on a controller or device failed. |
| Device Upgrade Failed | Critical | The software upgrade on a router failed. |
| DHCP Server State Change | Major | The state of a DHCP server changed. |
| Disk Usage | Critical<br>Major | The disk usage load on a controller or device has reached a critical level that could impair or shut down functionality, or a medium level that could impair functionality. |
| Domain ID Change | Critical | A domain identifier in the overlay network changed. |
| Interface Admin State Change | Critical<br>Medium | The administrative status of an interface in a controller or router changed from up to down (Critical) or down to up (Medium). |
| Interface State Change | Medium | The administrative or operational status of an interface changed. |
| Memory Usage | Critical<br>Medium | The memory usage on a controller or device has reached a critical level that could impair or shut down functionality, or a medium level that could impair functionality. |
| New CSR Generated | Critical | A controller or router generated a certificate signing request (CSR). |
| OMP All vSmarts Down | Critical | All OMP connections from all vSmart controllers in the overlay network are in the Down state. This means that the overlay network cannot function. |
| OMP vSmarts Up | | At least one OMP connection from all vSmart controllers in the overlay network is in the Up state. |
| OMP Node Down | | All OMP connections for a vEdge router are in the Down state. |
| OMP Node Up | Medium | At least one OMP connection for a vEdge router is in the Up state. |
| OMP Site Down | Critical | All OMP connections to vSmart controllers from all nodes in the a are in the Down state. This means that that site cannot participate in the overlay network. |
| OMP Site Up | Medium | At least one OMP connection to vSmart controllers from all nodes in the site is in the Up state. |
| OMP State Change | Critical<br>Medium | The administration or operational state of an OMP session between a vSmart controller and a vEdge router has changed, from Up to Down (Critical) or Down to Up (Medium). |
| OMP vSmarts Up | Medium | OMP connection from all vSmart controllers in the overlay network transition to the Up state. |

| | | |
|---|---|---|
| Org Name Change | Critical | The organization name used in the certificates for all overlay network devices changed. |
| OSPF Router Down | Critical | All OSPF connections on a router are in the Down state. |
| OSPF Router Up | Medium | An OSPF connection on a router transitioned to the Up state. |
| PIM Interface State Change | Major | The state of a PIM interface changed. |
| Process Restart | Critical | A process (daemon) on a controller or router restarted. |
| Pseudo Commit Status | Minor | The vManage NMS has started pushing a device configuration template to a controller or router. The NMS pushes a tentative configuration (called the pseudo commit) to the device and starts the rollback timer. If , with the new configuration, the control connections between the device and the vManage NMS come up, the tentative configuration becomes permanent. If the control connections do not come up, the tentative configuration is removed, and the device's configuration is rolled back to the previous configuration (that is, to the last known working). |
| Root Cert Chain Installed | Critical | The file containing the root certificate key chain was installed on a controller or router. |
| Root Cert Chain Uninstalled | Critical | The file containing the root certificate key chain was removed from a controller or router. |
| Site ID Change | Critical | A site identifier in the overlay network changed. |
| System IP Change | Critical | The system IP address on a controller or router changed. |
| System IP Reuse | Critical | The same system IP address is being used by more than one device in the overlay network. |
| System Reboot Issued | Critical<br>Medium | A device rebooted, either initiated by the device (Critical) or by a user (Medium). |
| Template Rollback | Critical | The attaching of a device configuration template to a router did not succeed in the configured rollback time, and as a result, the configuration on the device was not updated, but instead was rolled back to the previous configuration. |
| Unsupported SFP Detected | Critical | The software detected an unsupported transceiver in a hardware router. |
| vEdge Serial File Uploaded | Critical | The WAN Edge serial number file was uploaded to the vManage server. |
| vSmart/vManage Serial File Uploaded | Critical | A vManage NMS uploaded the file containing certificate serial numbers for the vManage NMSs and vSmart controllers in the overlay network. |
| ZTP Upgrade Failed | Critical | A software upgrade using ZTP failed on a controller or router. |

## Additional Information

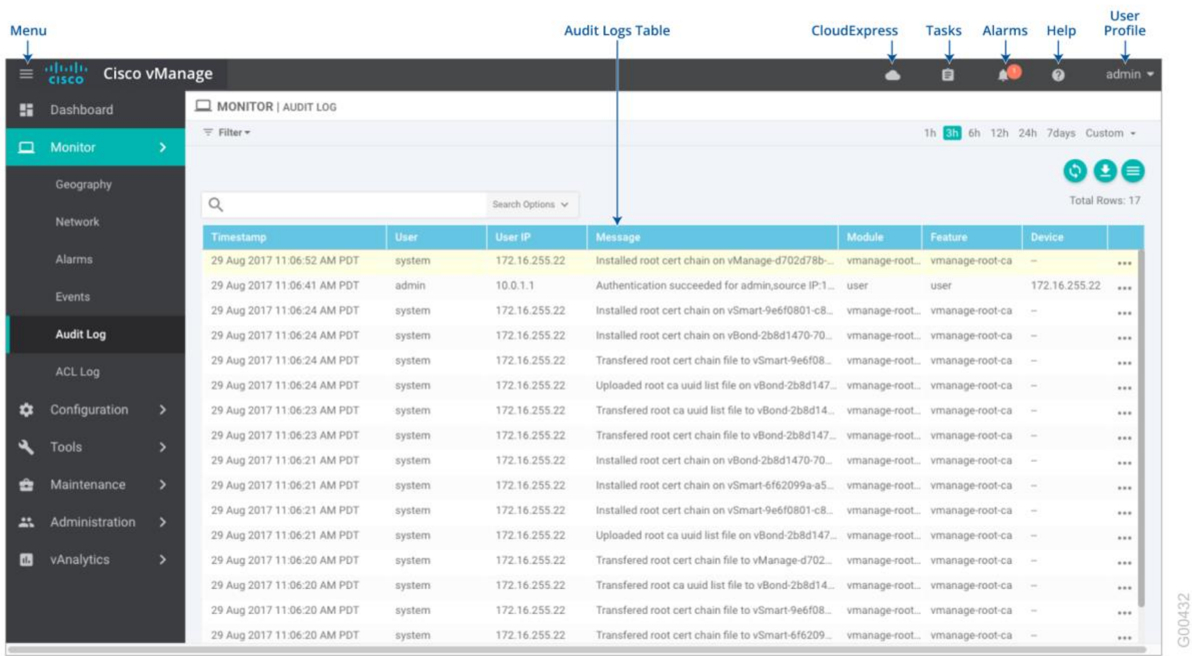
Monitor Alarms and Events

## Audit Log

Use the Audit Log screen to display a log of all activities on Viptela devices.

## Screen Elements

- Top bar—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.
- Title bar—Includes the title of the screen, Audit Log.
- Filter bar—Includes the Filter drop-down and time periods. Click the Filter icon to display a drop-down menu to add filters for audit logs. Click a predefined or custom time period for which to display data.
- Search box—Includes the Search Options drop-down, for a Contains or Match string.
- Refresh icon—Click to refresh data in the audit logs table with the most current data.
- Export icon—Click to download all data to a file, in CSV format.
- Show Table Fields icon—Click to display or hide columns from the audit logs table. By default, all columns are displayed.
- Table of audit logs, displaying the time of the log, the user on the device originating the log, log message, and other details. To re-arrange the columns, drag the column title to the desired position.




## Set Audit Log Filters

To set filters for searching audit logs:

1. Click the Filter drop-down menu.
2. In the Module drop-down, select the entity for which you are collecting audit logs. You can select more than one entity.
3. Click Search to search for logs that match the filter.

vManage NMS displays a log of activities both in table and graphical format.

## Export Audit Log Data in CSV Format

To export data for all audit logs to a file in CSV format, click the Export icon. This icon, which is a downward-pointing arrow, is located to the right of the filter criteria.

vManage NMS downloads all data from the audit logs table to an Excel file in CSV format. The file is downloaded to your brower's default download location and is named viptela_download.csv.

## View Audit Log Details

To view detailed information about any audit log:

1. Select the audit log row from the table.
2. Click the More Actions icon to the right of the row and click Audit Log Details.

The Audit Log Details popup window opens, displaying details of the audit log.

## View Changes to a Configuration Template

When you push a template configuration to a device, you can view changes between the old and the new configuration template. To view changes made to a configuration template:

1. Select the audit log row from the table. The Message column of the audit log row will contain a message to the effect that the template is successfully attached to the device.
2. Click the More Actions icon to the right of the row and click CLI Diff.

The CLI Diff popup window opens, with the Config Diff tab selected by default. This window displays a side-by-side view of the differences between the configuration that was on the device and the changes made to the configuration. To view the changes inline, click the Inline Diff button located to the right of the window.

To view the updated configuration on the device, click the Configuration tab located to the left of the window.

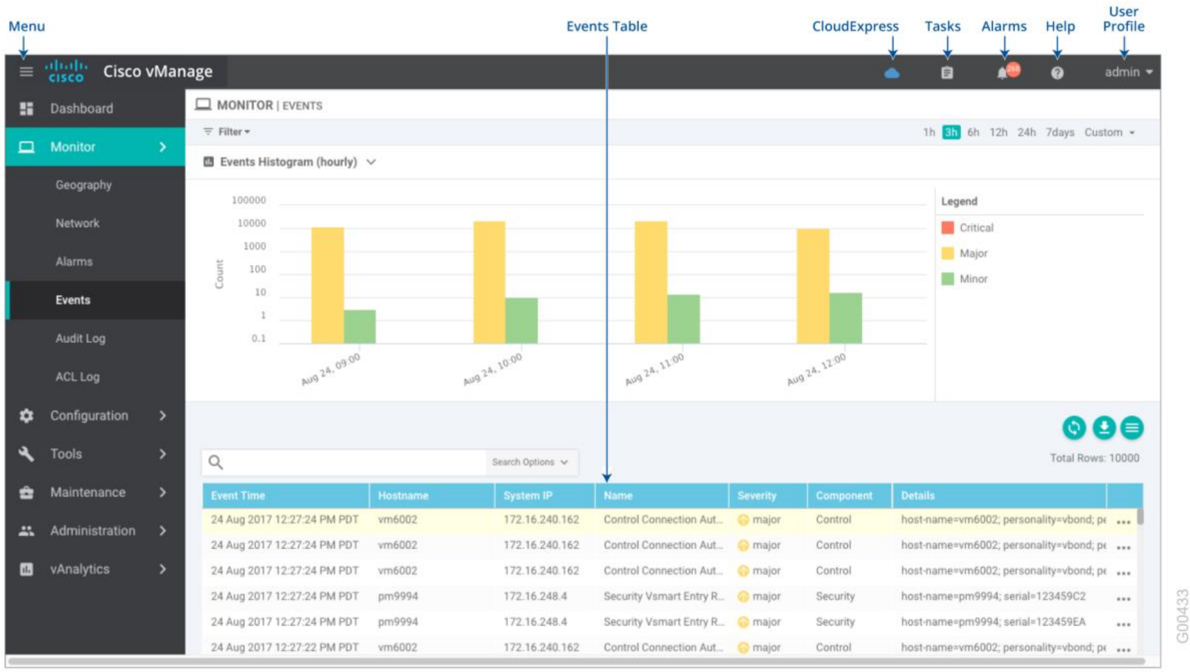
## Events

Use the Events screen to display detailed information on events generated by Viptela devices.

## Screen Elements

- Top bar—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.
- Title bar—Includes the title of the screen, Events.
- Filter bar—Includes the Filter drop-down and time periods. Click the Filter icon to display a drop-down menu to add filters for searching events. Click a predefined or custom time period for which to display data.
- Events Histogram—Displays a graphical representation of all events in order of severity: Critical, Major, Medium, Minor. To hide the events histogram, click the Events Histogram title or the down angle bracket to the right of it.
- Search box—Includes the Search Options drop-down, for a Contains or Match string.
- Refresh icon—Click to refresh data in the events table with the most current data.
- Export icon—Click to download all data to a file, in CSV format.

- Show Table Fields icon—Click to display or hide columns from the events table. By default, all columns are displayed.
- Table of events—To re-arrange the columns, drag the column title to the desired position.




## Set Event Filters

To set filters for searching events generated on one or more Viptela devices:

1. Click the Filter drop-down menu.
2. In the Severity drop-down, select the event severity level. Events generated by Viptela devices are collected by vManage NMS and classified as:

- Critical—indicates that action needs to be taken immediately.
- Major—indicates that the problem needs to be looked into but is not critical enough to bring down the network.
- Minor—is informational only.

You can specify more than one severity level.

3. In the Component drop-down, select the configuration component that caused the event. You can select more than one configuration component.
4. In the System IP drop-down, select the system IP of the devices for which to view generated events.
5. In the Event Name drop-down, select the event name for which to view generated events. You can select more than one event name.
6. Click Search to search events that match the filter.

vManage NMS displays the events both in table and graphical format.

## Export Event Data in CSV Format

To export data for all events to a file in CSV format, click the Export icon. This icon, which is a downward-pointing arrow, is located to the right of the Search box below the Events Histogram.

vManage NMS downloads all data from the events table to an Excel file in CSV format. The file is downloaded to your brower's default download location and is named viptela_download.csv.

## View Device Details

To view detailed information about a device on which an event was generated:

1. Select the event row from the table.
2. Click the More Actions icon to the right of the row and click Device Details.

The Device Details popup window opens, displaying the hostname of the device originating the event and other details.

## Geography

Use the Geography screen to view information about the Viptela devices and links in the overlay network. The Geography screen provides a map displaying the geographic location of the Viptela devices.

Note: The browser on which you are running vManage NMS must have Internet access. If you do not have Internet access, ensure that the browser has access to "*.openstreetmaps.org."

## Screen Elements

- Top bar—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.
- Title bar—Includes the title of the screen, Geography.
  - No Geographic Coordinates—Located to the right of the title bar, it displays the number of devices for which geographic coordinates are not configured.
- Filter bar—Includes the Filter button and the following tabs which reflect the default Filter selections:
  - All Groups for the device group.
  - vEdge, vEdge-vBond, vBond, vSmart, and vManage for the device types.
  - Control Up, Data Up, and Data Down for the link states.
- Map—Displays the geographic location of Viptela devices based on the latitude and longitude configured on the devices. The map includes the following elements:
  - Search box—Includes the Search Options drop-down, for a Contains or Match string. The search applies to all devices, including those that have no geographic coordinates defined.
  - + (plus) and – (minus) zoom icons.
  - Map provider icon, to choose any open source map provider.
  - Device icons for the Viptela devices:

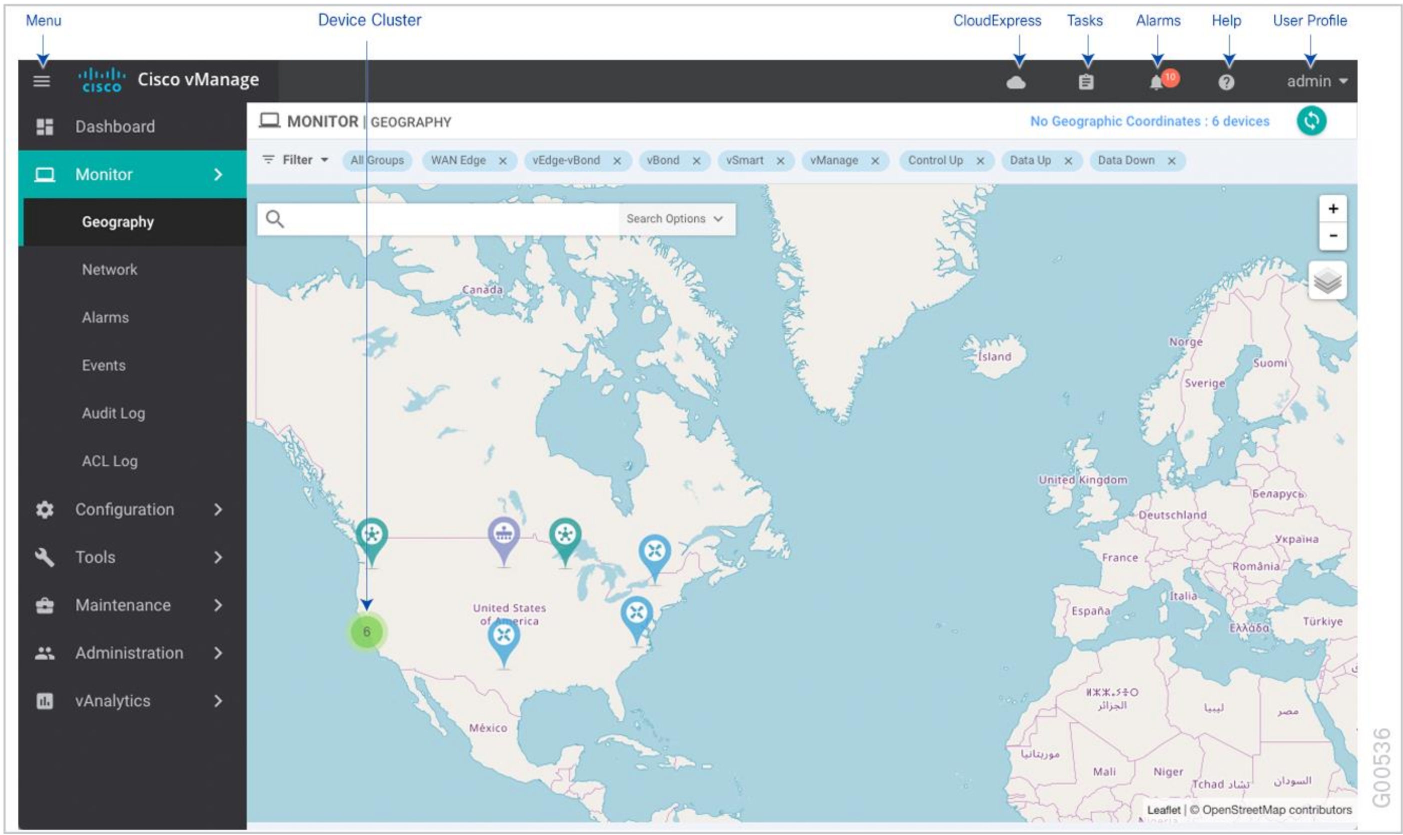
 vManage

 vSmart

 vEdge

 vBond

- Device clusters—A green circle with a number in the center indicates a cluster of devices located in an area. Click the cluster to display the individual device icons on the map.




## Set Map Filters

To select the devices and links you want to display on the map:

1. Click the Filter button to display a pull-down menu.
2. Select the device group from the pull-down menu which includes all configured device groups. By default, the group "All" is selected and displays all Viptela devices in the overlay network. The group "No Groups" includes the devices that are not part of a device group. If all devices are in a group, the "No Groups" group is not displayed.
3. Select the Viptela devices to display on the map. By default, the map displays all device types including vEdge, vEdge-vBond, vSmart, and vManage.
4. Select the state of control and data links. By default, the map displays all control and data connections.
5. Close the Filter box by moving the cursor outside the box.

The map is dynamically updated to reflect your selections. Also, as you make the device group, device type, and link selections, the tabs next to the Filter button are updated.

## View Device Information

To display basic information for a device, hover over the device icon. A hover box displays the system IP, hostname, site ID, device type, and device status.

To display detailed information for a device, double-click the device icon to open the View More Details hover box. Click Device Dashboard, Device Details, SSH Terminal, or Links to get further details for the device.

## View Link Information

By default, control and data connections are not displayed on the map. To see control and data connections for a device:

1. Double-click the device icon to open a hover box with details about the device.
2. Click Links.

Note the following:

- An active control connection between two devices is displayed on the map as a thin blue line. Multiple active connections between devices are displayed by a bold blue line. A control connection that is down is displayed on the map as a dotted red line. Multiple control connections that are down are displayed by a bold dotted red line. If you hover over the line, a hover box tells you if the connection is up or down.
- An active data connection between two devices is displayed on the map as a thin green line. Multiple active data connections are displayed by a bold green line. A data connection that is down is displayed on the map as a dotted red line. Multiple data connections that are down are displayed by a bold dotted red line. If you hover over the line, a hover box tells you if the connection is up or down.
- An active consolidated control and data connection between two devices is displayed on the map as a thick grey line.

## Configure Geographic Coordinates for a Device

To configure the geographic coordinates for a device, use the Configuration ► Templates ► System feature template.

If the Viptela device is not attached to a configuration template, you can configure the latitude and longitude directly on the device:

1. Select the Tools ► SSH Terminal screen.
2. Select the device from the left pane. The SSH Terminal screen opens in the right pane.
3. Enter the username and password to log in to the device.
4. Determine whether the device is attached to a configuration template:
 Viptela# **show system status**
 Check the values in the vManaged and Configuration template output fields. For example:
 ```
 ...
 Personality:          vedge
 Model name:           vedge-cloud
 Services:             None
 vManaged:             false
 Commit pending:       false
 Configuration template: None
 ```
 If the vManaged field is false, the device is not attached to a configuration template, and the Configuration template field says None. For such a device, you can configure the GPS coordinates directly from the CLI.

If the vManaged field is true, the device's configuration has been downloaded by the vManage server, and the Configuration template field shows the name of the configuration template. For such a device, you cannot configure the GPS coordinates directly from the CLI. If you attempt to do so, the **validate** or **commit** command fails, with the following message:
Aborted: 'system is-vmanaged': This device is being managed by the vManage. Configuration through the CLI is not allowed.

5. Enter configuration mode:
Viptela# **config**
Viptela(config)#

6. Configure the latitude and longitude on the device:
Viptela(config)# **system gps-location** **latitude** *degrees.minutes.seconds*
Viptela(config-system)# **gps-location** **longitude** *degrees.minutes.seconds*

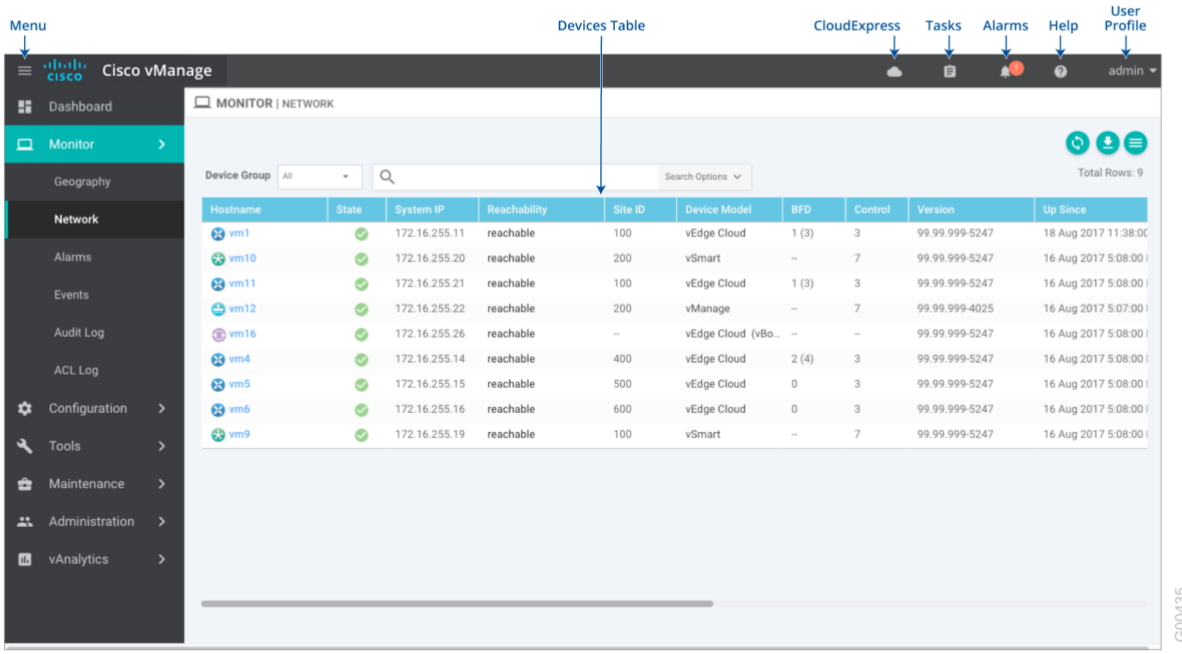
7. Save the configuration:
Viptela(config-system)# **commit**
Viptela(config-system)#

## Network

Use the Network screen to display a list of Viptela devices in the overlay network and to display detailed information about individual devices.

## Screen Elements

- Top bar—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.
- Title bar—Includes the title of the screen, Network.
- WAN Edge and CloudDock Clusters tabs—When you first open the Network screen, the WAN Edge tab is selected.
  - WAN Edge tab—Click to display a table of the overlay network devices in the network.
  - CloudDock Clusters tab—Click to display a table of the CloudDock clusters in the network.
- Device Groups drop-down—Lists all configured device groups in the network.
- Search box—Includes the Search Options drop-down, for a Contains or Match string.
- Refresh icon—Click to refresh data in the device table with the most current data.
- Export icon—Click to download all data to a file, in CSV format.
- Show Table Fields icon—Click to display or hide columns from the device table. By default, all columns are displayed.
- Table of devices in the overlay network—To re-arrange the columns, drag the column title to the desired position.




## View List of Devices

The Network screen lists the Viptela devices in the overlay network. When you first come to the Network screen, the device group "All" is selected, and the screen shows status information for all Viptela devices in the overlay network.

To see a list of devices in a particular group, select that device group.

To filter the devices by reachability, hostname, system IP address, site ID, and device model, select from the sort options in the drop-down or type a string in the Search box.

To display information about an individual device, click its hostname.

## Export Device Data in CSV Format

To export data for all devices to a file in CSV format, click the Export button. This button is located to the right of the filter criteria.

vManage NMS downloads all data from the device table to an Excel file in CSV format. The file is downloaded to your brower's default download location and is named viptela_download.csv.

## View Information about a Device

To view high-level information about a device, select the device from the Monitor ► Network screen:

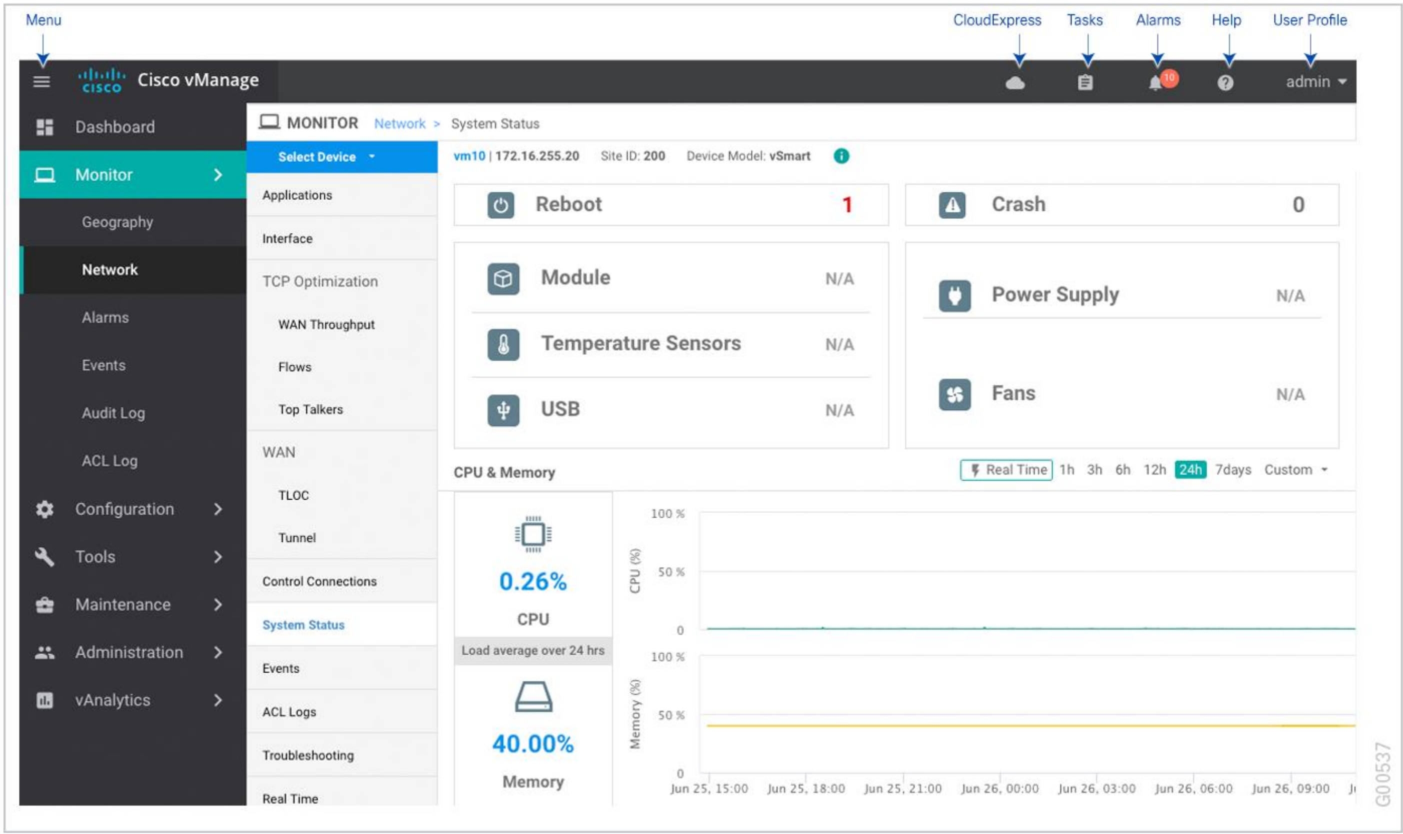
1. From the Device Groups drop-down list, select the device group to which the device belongs. The device table lists all the devices in the selected group.

2. Select the device by clicking its hostname. The left pane lists the information categories about the device. In the right pane, the System Status category is selected, which displays status information about the device.

To select a different device, either click the Select Device drop-down located at the top of the left pane, or click Network in the title bar and then select a device by clicking its hostname.

After you select a device by clicking its hostname, the screen changes and displays the following elements:

- Select Device bar—A horizontal bar that includes these elements:
  - Select Device drop-down
  - Device name
  - Device IP address
  - Device site location
  - Device model
  - More Info drop-down
- Left pane—A vertical pane that lists the categories of information you can display about the device:
  - Applications—DPI flow information.
  - Interface—Interface status and statistics.
  - TCP Optimization—Statistics related to find-tuning the processing of TCP data traffic.
  - WAN—TLOC and tunnel status and statistics.
  - Control Connections—Status and statistics for control connections.
  - System Status—Reboot and crash information, hardware component status, and CPU and memory usage.
  - Events—Latest syslog events.
  - ACL Logs—Logging files for access lists (ACLs).
  - Troubleshooting—Ping and traceroute traffic connectivity tools.
  - Real Time—Real-time device information for feature-specific operational commands.
- Right pane—Displays information about the selected category.




## View Device Status Summary

To view summary status information about a device:

1. From the Monitor ► Network screen, select a device.

2. From the Select Device bar, click the More Info drop-down located to the right of the bar. vManage NMS opens a drop box with summary information about the device.

To close the device status summary, click More Info again or click anywhere on the screen outside the drop-down.

## View DPI Flows

To view DPI flow information on a vEdge router:

1. From the Monitor ► Network screen, select a device.

2. Click Applications in the left pane. The right pane displays DPI flow information for the device.

The upper part of the right pane contains:

- Filter bar—Located directly under the device name, this bar includes the Filter icon and time periods. Click the Filter icon to display a drop-down menu to select the desired VPN and TLOC. Click a predefined or custom time period for which to display data.

- DPI flow information in graphical format.

- DPI flow graph legend—Select an application family to display information for just that flow. Click the Total Network Traffic checkbox to display flow information as a proportion of total network traffic.

The lower part of the right pane contains:

- Filter criteria.
- DPI flow information table that lists all application families sorted by usage. By default, the top six application families are selected. The graphical display in the upper part of the right pane plots the flow and usage of the selected application families.
  - Click the checkbox to the left to select and deselect application families. You can select and display information for a maximum of six application families at one time.
  - Click an application family to display applications within the family.
  - Click an application to display the source IP addresses of the devices accessing the application. The Traffic per TLOC pie chart next to the graph displays traffic distribution per TLOC (color).
  - To re-arrange the columns, drag the column title to the desired position.
  - To return to the list of application families, click Applications in the title bar or click the Back button in the browser.

## View Interfaces

To view information about interfaces on a device:

1. From the Monitor ► Network screen, select a device.
2. Click Interface in the left pane. The right pane displays interface information for the device.

The upper part of the right pane contains:

- Chart Options bar—Located directly under the device name, this bar includes:
  - Chart Options drop-down—Click Chart Options to select the type of data to display.
  - IPv4 & IPv6 drop-down—Click IPv4 & IPv6 to select the type of interfaces to display. The information is displayed in graphical format. By default, the graph is Combined, showing interfaces on which both IPv4 and IPv6 addresses are configured. To display IPv4 and IPv6 interfaces in separate graphs, select the Separated toggle button.
  - Time periods—Click either Real Time, a predefined time period, or a custom time period for which to display data.
- Interface information in graphical format.
- Interface graph legend—Select an interface to display information for just that interface.

The lower part of the right pane contains:

- Filter criteria.
- Interface table that lists information about all interfaces. By default, the first six interfaces are selected. The graphical display in the upper part of the right pane plots information for the selected interfaces.
  - Click the checkbox to the left to select and deselect interfaces. You can select and display information for a maximum of 30 interfaces at one time.
  - To re-arrange the columns, drag the column title to the desired position.
  - For cellular interfaces, click the interface name to display a screen that shows detailed information about the cellular interface.

## View TCP Optimization Information

If TCP optimization is enabled on a router, you can view information about how the optimization is affecting the processing and throughput of TCP data traffic on the router:

1. From the Monitor ► Network screen, select a vEdge router.
2. Click TCP Optimization–WAN Throughput in the left page. The right pane displays the WAN throughput, in megabits per second.

The upper part of the right pane contains the following elements:

- Chart Options bar—Located directly under the device name, this bar includes the Filter Options drop-down and time periods. Click Filter to limit the data to display based on VPN, local TLOC color, destination IP address, remote TLOC color, and remote system IP address. Click a predefined or custom time period for which to display data.
- Average optimized throughput information in graphical format.
- WAN graph legend—Identifies non-optimized and TCP optimized packet throughput.

The lower part of the right pane shows the hourly average throughput and the total optimized throughput, both in megabits per second.

Click TCP Optimization–Flows in the left pane to display information about TCP-optimized traffic flows. The upper part of the right pane contains the following elements:

- Chart Options bar—Located directly under the device name, this bar includes the Filter drop-down and time periods. Click Filter to limit the data to display based on VPN, local TLOC color, destination IP address, remote TLOC color, and remote system IP address. Click a predefined or custom time period for which to display data.
- Average optimized throughput information in graphical format.
- Flows graph legend—Identifies traffic flows.

The lower part of the right pane contains the following elements:

- Set perspective—Select the flow direction.
- Search box—Includes the Search Options drop-down, for a Contains or Match string.
- Flow table that lists the flow destination, usage, and percentage of total traffic for all TCP-optimized flows. By default, the first six flows are selected. Click the checkbox to the left to select and deselect flows to display. The graphical display in the upper part of the right pane plots information for the selected flows.

Click TCP Optimization–Connections in the left pane to display status information about all the tunnels over which the most TCP-optimized traffic is flowing. The upper part of the right pane contains the following elements:

- TCP Optimization Connections in graphical format
- Connection State boxes—Select the connection state or states to display TCP optimization information about.

The lower part of the right pane contains the following elements:

- Filter criteria.
- Flow table that lists information about each of the tunnels, including the tunnel's connection state.

## View TLOC Loss, Latency, and Jitter Information

To view information about TLOC loss, latency, and jitter:

1. From the Monitor ► Network screen, select a device.

2. Click WAN–TLOC in the left pane. The right pane displays the aggregated average loss or latency/jitter information for all TLOC colors.

The upper part of the right pane contains the following elements:

- Chart Options bar—Located directly under the device name, this bar includes the Chart Options drop-down and time periods. Click Chart Options to select the type of data to display. Click a predefined or custom time period for which to display data.
- TLOC information in graphical format. The time interval in the graph is determined by the value of the BFD application-aware routing poll interval .
- TLOC graph legend—Select a TLOC color to display information for just that TLOC.

The lower part of the right pane contains the following elements:

- Search box—Includes the Search Options drop-down, for a Contains or Match.
- TLOC color table that lists average jitter, loss, and latency data about all TLOCs. By default, the first six colors are selected. The graphical display in the upper part of the right pane plots information for the selected interfaces.
  - Click the checkbox to the left to select and deselect TLOC colors. You can select and display information for a maximum of 30 TLOCs at one time.
  - Click Application Usage to the right to display DPI flow information for that TLOC.

## View Tunnel Connections

To view all tunnel connections for a device:

1. From the Monitor ► Network screen, select a device.
2. Click WAN–Tunnel in the left pane. The right pane displays information about all tunnel connections.

The upper part of the right pane contains the following elements:

- Chart Options bar—Located directly under the device name, this bar includes the Chart Options drop-down and time periods. Click Chart Options to select the type of data to display. Click a predefined or custom time period for which to display data.
- Tunnel information in graphical format.
- Tunnel graph legend—Select a tunnel to display information for just that tunnel.

The lower part of the right pane contains the following elements:

- Search box—Includes the Search Options drop-down, for a Contains or Match.
- Tunnel table that lists average latency, loss, and jitter data about all tunnel end points. By default, the first six tunnels are selected. The graphical display in the upper part of the right pane plots information for the selected tunnels.
  - Click the arrow to the left to view the tunnel end points for that TLOC color.
  - Click the checkbox to the left to select and deselect tunnels. You can select and display information for a maximum of 30 tunnels at one time.
  - Click Application Usage to the right to display DPI flow information for that TLOC.

## View WiFi Configuration

To view WiFI configuration for Viptela routers that support wireless LANs (WLANs), such as the vEdge 100wm routers:

1. From the Monitor ► Network screen, select a device.

2. Click WiFi in the left pane. The right pane displays information about WiFI configuration on the router.

The upper part of the right pane contains the following elements:

- AP Information bar—Located directly under the device name, it displays access point information and the Clients Details button. Click the Clients Details button to view information about clients connected to the WiFi access point during the selected time period.
- Radio frequency parameters for access points.
- SSID parameters for virtual access points (VAPs).

The lower part of the right pane contains the following elements:

- VAP receive and transmit statistics bar—Includes the time periods. Click a predefined or custom time period for which to display data.
- VAP receive and transmit statistics information in graphical format.
- VAP statistics graph legend—Select a VAP interface to display information for just that interface. Click the VAP interface again to return to the previous display.

## View Client Details

To view details of clients connected to the WiFi access point, click the Clients Details button on the WiFi screen.

The upper part of the Clients Info right pane contains the following elements:

- Clients Details title bar—Includes the Clients Usage tab.
- Time periods—Click a predefined or custom time period for which to display data.
- Information of clients connected to the WiFi access point in graphical format. Select a column to display information for just those clients in tabular format in the lower part of the screen.

The lower part of the Clients Info right pane contains the following elements:

- Filter criteria.
- Table of clients connected to the WiFi access point.

## View Client Usage

To view data usage details of all clients connected to the WiFi access point, click the Clients Usage tab.

The upper part of the Clients Usage right pane contains the following elements:

- Time periods—Click a predefined or custom time period for which to display data.
- Data usage of all clients connected to the WiFi access point in graphical format.
- Data usage information graph legend—Select a client MAC address to display information for just that client.

The lower part of the Clients Usage right pane contains the following elements:

- Filter criteria.
- Data usage information table. By default, the first six clients are selected.

## View Control Connections

To view all control connections for a device:

1. From the Monitor ► Network screen, select a device.
   If you select a controller device—a vBond orchestrator, a vManage NMS, or a Smart controller—the Control Connections screen opens by default.
2. If you select a vEdge router, click Control Connections in the left pane. The right pane displays information about all control connections that the device has with other controller devices in the network.

The upper part of the right pane contains the following elements:

- Expected and actual number of connections.
- Control connection data in graphical format. If the device has multiple interfaces, vManage NMS displays a graphical topology of all control connections for each color.

The lower part of the right pane contains the following elements:

- Search box—Includes the Search Options drop-down, for a Contains or Match.
- Control connections data in tabular format. By default, the first six control connections are selected. The graphical display in the upper part of the right pane plots information for the selected control connections.
  - Click the arrow to the left to view the control connections for that TLOC color.
  - Click the checkbox to the left to select and deselect control connections. You can select and display information for a maximum of six control connections at one time.

## View System Status

To view system status about a device:

1. From the Monitor ► Network screen, select a device.
   When you select a vEdge router, the System Status screen opens by default.
2. Click System Status in the left pane. The right pane displays information about the device.

The right pane contains the following elements:

- Reboot—Number of times the device has rebooted. For details about each reboot, click Reboot. The Reboot screen opens and contains the following elements:
  - Search box—Includes the Search Options drop-down, for a Contains or Match.
  - Table listing all the reboots on the device along with the time and reason for the reboot. If the device is down for 90 seconds or longer, the reason shows as "Unknown". The Last Updated column displays the time when the vManage NMS retrieved the reboot data from the device.
- Crash—Number of times the device has crashed. For details about each crash, click Crash. The Crash screen opens and contains the following elements:
  - Search box—Includes the Search Options drop-down, for a Contains or Match.
  - Table listing all the crashes on the device along with the time of crash and name of the core file created as a result of the crash.
- Status of hardware components, applicable only if the selected device is a hardware vEdge router:
  - Module

  - Temperature sensors
  - USB
  - Power supply
  - Fans

The status of a hardware component is represented in one of the following ways:

- Green check mark—Component is operational.
- Red circle with an X—Component is down.
- Orange triangle with an exclamation point—Component has an error.
- N/A—Not applicable since the selected device is not a hardware vEdge router.
- CPU & Memory—To the right are the time periods. Click a predefined or custom time period for which to display data.
  - CPU usage—Displays the CPU usage, as a percentage of available CPU, over the selected time range.
  - Memory usage—Displays the memory usage, as a percentage of available memory, over the selected time period.

## View Events

To view the number of critical, major, or minor events on a device:

1. From the Monitor ► Network screen, select a device.
2. Click Events in the left pane. The right pane displays information about all events on the device.

The upper part of the right pane contains the following elements:

- Filter bar—Includes the Filter drop-down and time periods. Click the Filter icon to display a drop-down menu to add filters for searching events by severity, component, and event name. Click a predefined or custom time period for which to display data.
- Events Histogram—Displays a graphical representation of all events. To hide the events histogram, click the Events Histogram title or the down angle bracket to the right of it.

The lower part of the right pane has the following elements:

- Search box—Includes the Search Options drop-down, for a Contains or Match.
- Events table.
  - To re-arrange the columns, drag the column title to the desired position.
  - To change the sort order in a column, click the Up or Down arrow in the column title.

## View ACL Logs

To view logs for access lists (ACLs) configured on a vEdge router:

1. From the Monitor ► Network screen, select a vEdge router.
2. Click ACL Logs in the left pane. The right pane displays information about all localized data policy (ACL) logs on the router. You configure these logs by including the **log** action in an ACL.

The upper part of the right pane contains the following elements:

- Filter bar—Includes the Filter drop-down and time periods. Click the Filter icon to display a drop-down menu to add filters for searching logs by VPN. Click a predefined or custom time period for which to display data.
- Search box—Includes the Search Options drop-down, for a Contains or Match.

The lower part of the right pane contains the following elements:

- Logs table.
  - To re-arrange the columns, drag the column title to the desired position.
  - To change the sort order in a column, click the Up or Down arrow in the column title.

# Troubleshoot a Device

You can troubleshoot connectivity or traffic health for all devices in the overlay network.

## Check Device Connectivity

To troubleshoot connectivity for a device in the network, you can do the following:

- Check device bringup
- Ping the device
- Run a speed test
- Run a traceroute
- View control connections in real time

### Check Device Bringup

To verify the status of a device bringup (available on vEdge routers only):

1. From the Monitor ► Network screen, select the device.
2. Click Troubleshooting in the left pane.
3. From the Connectivity pane, click Device Bringup.

The Device Bringup screen opens and displays:

- Troubleshooting drop-down—Located to the right of the Select Device drop-down. Click an option to view troubleshooting information. To close the drop-down, click the Troubleshooting button again.
- Device bringup state—Indicated by one of the following states:
  - Green check mark—Indicates that the device has successfully established control-plane connections with the controller devices in the network and is up and running.
  - Gray check mark—Indicates that ZTP was disabled in the Administration ► Settings screen when the device initially came up. You will see this state for the Software Image Update box only.

- Red check mark—Indicates that the device failed to establish control-plane connections with the controller devices in the network and is not up and running.
- Yellow exclamation point—Indicates that vManage NMS could not find the reason for a failure on the device.

## Ping a Device

To verify that a device is reachable on the network, ping the device to send ICMP ECHO_REQUEST packets to it:

1. From the Monitor ► Network screen, select the device.
2. Click Troubleshooting in the left pane.
3. From the Connectivity pane, click Ping.
4. In the Destination IP field, enter the IP address of the device to ping.
5. In the VPN drop-down, select the VPN to use to reach the device.
6. In the Source/Interface drop-down, select the interface to use to send the ping packets.
7. In the Probes field, select the protocol type to use to send the ping packets.
8. In the Source Port field, enter the number of the source port.
9. In the Destination Port field, enter the number of the destination port.
10. In the Type of Service field, enter the value for the type of service (ToS) field to include in the ping packets.
11. In the Time to Live field, enter the round-trip time for sending this ping packet and receiving a response, in milliseconds.
12. Click the Don't Fragment slider to set the Don't Fragment bit in the ping packets.
13. Click Advanced Options to specify additional parameters:
    a. In the Count field, enter the number of ping requests to send. The range is 1 through 30. The default is 5.
    b. In the Payload Size field, enter the size of the packet to send. The default is 64 bytes, which comprises 56 bytes of data and 8 bytes of ICMP header. The range for data is 56 through 65507 bytes.
    c. Click the Rapid slider to send 5 ping requests in rapid succession and to display statistics only for packets transmitted and received, and the percentage of packets lost.
14. Click Ping.

## Run a Speed Test

To check the actual bandwidth of a circuit from one device to another:

1. In the Administration ► Settings screen, ensure that Data Stream is enabled.
2. From the Monitor ► Network screen, select the device.
3. Click Troubleshooting in the left pane.
4. From the Connectivity pane, click Speed Test.
5. In the Source Circuit drop-down, select the color of tunnel interface on the local device.

6. In the Destination Device drop-down, select the remote device by the device's name and system IP address.
7. In the Destination Circuit drop-down, select the color of the tunnel interface on the remote device.
8. Click Start Test. The speed test sends a single packet from the source to the destination and receives the acknowledgement from the destination.

The middle part of the right pane reports the results of the speed test. The clock reports the circuit's speed based on the round-trip time. The download speed shows the speed from the source to the destination, and the upload speed shows the speed from the destination to the source, both in Mbps. The configured downstream and upstream bandwidths for the circuit are also displayed.

When a speed test completes, the test results are added to the table at the lower part of the right pane.

## Run a Traceroute

To display the path that packets take to reach a host or IP address on the network:

1. From the Monitor ► Network screen, select the device.
2. Click Troubleshooting in the left pane.
3. From the Connectivity pane, click Trace Route.
4. In the Destination IP field, enter the IP address of a device on the network.
5. In the VPN drop-down, select the VPN to use to reach the device.
6. In the Source/Interface drop-down, select the interface to use to send traceroute probe packets.
7. Click Advanced Options.
8. kIn the Size field, enter the size of the traceroute probe packets, in bytes.
9. Click Start to trigger a traceroute to the requested destination.

The lower part of the right pane displays:

- Output—Raw output of the path the traceroute probe packets take to reach the destination.
- Graphical depiction of the path the traceroute probe packets take to reach the destination.

## View Control Connections in Real Time

To display a real-time view the control plane connections on a vEdge router:

1. From the Monitor ► Network screen, select the device. The device must be a vEdge router.
2. Click Troubleshooting in the left pane.
3. From the Connectivity pane, click Control Connections.

The control plane connection screen is updated automatically, every 15 seconds.

The upper part of the right pane shows figures illustrates the operational control plane tunnels between the vEdge router and vManage and vSmart controllers.

The lower part of the lower pane contains a table that shows details for each of the control plane tunnels, including the remote device's IP address and the status of the tunnel end points, including the reason for the failure of an end point.

## Check Traffic Health

To check traffic health for a vEdge router in the network:

- View tunnel health
- View traffic path information
- Packet capture
- Simulate flows

### View Tunnel Health

To view the health of a tunnel from both directions (available on vEdge routers only):

1. From the Monitor ► Network screen, select the device.
2. Click Troubleshooting in the left pane.
3. From the Traffic pane, click Tunnel Health.
4. From the Local TLOC drop-down, select a source TLOC.
5. From the Remote Device drop-down, select a remote device.
6. From the Remote TLOC drop-down, select a destination TLOC.
7. Click Go. The lower part of the screen displays:

- Chart Options bar—Located directly under the device name, this bar includes the Chart Options drop-down and time periods. Click Chart Options to select the type of data to display. Click a predefined or custom time period for which to display data.
- App-route data (either loss, latency, or jitter) in graphical format for all tunnels between the two devices in each direction.
- App-route graph legend—Identifies selected tunnels from both directions.

Select a TLOC to display information for just that TLOC.

### Check Application-Aware Routing Traffic

To check application-aware routing traffic from the source device to the destination device (available on vEdge routers only):

1. From the Monitor ► Network screen, select the device.
2. Click Troubleshooting in the left pane.
3. From the Traffic pane, click App Route Visualization.
4. From the Remote Device drop-down, select a destination device.
5. Click Go. The lower part of the screen displays:

- Chart Options bar—Located directly under the device name, this bar includes the Chart Options drop-down and time periods. Click Chart Options to select the type of data to display. Click a predefined or custom time period for which to display data.
- Application-aware routing data (either loss, latency, or jitter), along with octets, in graphical format for all tunnels between the two devices.

- Application-aware routing graph legend—Identifies source and destination TLOC.

## Capture Packets

To capture control plane and data plane packets in real time, similar to a UNIX tcpdump operation, and to save these packets to a file (available on vEdge routers only):

1. From the Monitor ► Network screen, select the device.
2. Click Troubleshooting in the left pane.
3. From the Traffic pane, click App Packet Capture.
4. From the VPN drop-down, select the VPN in which to capture packets.
5. From the Interface drop-down, select the interface over which to capture packets.
6. Optionally, click Traffic Filter to filter the packets to capture based on values in their IP headers. Enter values for one or more of these fields:
    a. In Source IP, enter the packets' source IP address.
    b. In Source Port, enter the packets' source port number.
    c. In Protocol, enter the packets' protocol number
    d. In Destination IP, enter the packets' destination IP address.
    e. In Destination Port, enter the packets' destination port number.
7. Click Start. The packet capture begins, and displays its progress:
    a. Packet Capture in Progress—Packet capture stops after 5 minutes, after the file of collected packets reaches 5 MB, or when you click the Stop button.
    b. Preparing file to download—vManage NMS creates a file in libpcap format (a.pcap file).
    c. File ready, click to download the file—Click the download icon to download the generated file.

## Simulate Flows

To display the next-hop information for an IP packet (available on vEdge routers only):

1. From the Monitor ► Network screen, select the vEdge router.
2. Click Troubleshooting in the left pane.
3. From the Traffic pane, click Simulate Flows.
4. To specify the data traffic path, select values or enter data in the required fields (marked with an asterisk [*]) and optional fields. The required fields are:
    • VPN—VPN in which the data tunnel is located.
    • Source Interface—Interface from which the cflowd flow originates.
    • Source IP—IP address from which the cflowd flow originates.
    • Destination IP—Destination IP address of the cflowd flow.
    • Protocol (under Advanced Options)—Number of the protocol being used to transmit the cflowd flow.
    The optional fields are:
    • Application—Application running on the router.
    • Source Port (under Advanced Options)—Port from which the cflowd flow originates.

• Destination Port (under Advanced Options)—Destination port of the cflowd flow.
• DSCP (under Advanced Options)—DSCP value in the cflowd packets.

5. Click Advanced Options:

   a. In the Path toggle field, select whether the data traffic path information comes from the service side of the router or from the tunnel side.

   b. Select values or enter data in the required fields (marked with an asterisk [*]) and optional fields. The required fields are:
   • Protocol—Number of the protocol being used to transmit the cflowd flow.
   The optional fields are:
   • Source Port—Port from which the cflowd flow originates.
   • Destination Port—Destination port of the cflowd flow.
   • DSCP—DSCP value in the cflowd packets.

   c. Check the All Paths checkbox to display all possible paths for a packet.

6. Click Simulate to determine the next hop that a packet with the specified headers would take.

## Check Device Syslog FIles

To display the contents of a device's syslog files:

1. In the Administration ► Settings screen, ensure that Data Stream is enabled.

2. From the Monitor ► Network screen, select the vEdge router.

3. Click Troubleshooting in the left pane.

4. From the Logs pane, click Debug Log.

5. In the Log Files field, select the name of the log file. The lower part of the screen displays the log information.

# View Real-Time Data

To view real-time data for a device:

1. From the Monitor ► Network screen, select a device.

2. Click Real Time. The right pane displays system information about the device.

The right pane contains the following elements:

- Command drop-down—Located directly under the device name, this drop-down allows you to select a feature-specific operational command to display real-time device information for the selected command. The commands in the drop-down are listed alphabetically. The commands available vary depending on the device selected. When you first select Real Time, the System Information command is selected, and real-time system information about the device is displayed in tabular format.
  For some commands, you can add filters to speed up the display of information. When you select these commands from the drop-down, the Select Filter window is displayed prompting you to either Show Filters or Do Not Filter.

  – Show Filters—Displays the available filters. Fill in the desired fields and click Search to display real-time device information corresponding just to those fields. Clicking Search without filling any of the fields displays the entire information for the selected command.

  – Do Not Filter—Displays the entire real-time device information for the selected command.

- Filter criteria.

- Table with real-time information for the selected command.
  - To re-arrange the columns, drag the column title to the desired position.
  - To change the sort order in a column, click the Up or Down arrow in the column title.

# Security

## 19.1 Release Updates

## Configuring IKE-Enabled IPsec Tunnels

To securely transfer traffic from the overlay network to a service network, you can configure IPsec tunnels that run the Internet Key Exchange (IKE) protocol. IKE-enabled IPsec tunnels provide authentication and encryption to ensure secure packet transport.

You create an IKE-enabled IPsec tunnel by configuring an IPsec interface. IPsec interfaces are logical interfaces, and you configure them just like any other physical interface. You configure IKE protocol parameters on the IPsec interface, and you can configure other interface properties.

The Viptela software supports IKE, Version 1, as defined in RFC 2409 , *Internet Key Exchange* , and IKE, Version 2, as defined in RFC 7296 , *Internet Key Exchange Protocol, Version 2* .

One use for IPsec tunnels is to allow vEdge Cloud router VM instances running on Amazon AWS to connect to the Amazon virtual private cloud (VPC). You must configure IKE Version 1 on these routers.

## Configure an IPsec Tunnel

To configure an IPsec tunnel interface for secure transport traffic from a service network, you create a logical IPsec interface:

```
vEdge(config)# vpn vpn-id interface ipsecnumber
vEdge(config-interface-ipsec)# ip address ipv4-prefix/length
vEdge(config-interface-ipsec)# (tunnel-source ip-address | tunnel-source-interface interface-name)
vEdge(config-interface-ipsec)# tunnel-destination ipv4-address
vEdge(config-interface-ipsec)# no shutdown
```

You can create the IPsec tunnel in the transport VPN (VPN 0) and in any service VPN (VPN 1 through 65530, except for 512).

The IPsec interface has a name in the format **ipsec** *number* , where *number* can be from 1 through 255.

Each IPsec interface must have an IPv4 address. This address must be a /30 prefix. All traffic in the VPN that is within this IPv4 prefix is directed to a physical interface in VPN 0 to be sent securely over an IPsec tunnel.

To configure the source of the IPsec tunnel on the local device, you can specify either the IP address of the physical interface (in the **tunnel-source** command) or the name of the physical interface (in the **tunnel-source-interface** command). Ensure that the physical interface is configured in VPN 0.

To configure the destination of the IPsec tunnel, specify the IP address of the remote device in the **tunnel-destination** command.

The combination of a source address (or source interface name) and a destination address defines a single IPsec tunnel. Only one IPsec tunnel can exist that uses a specific source address (or interface name) and destination address pair.

## Configure an IPsec Static Route

To direct traffic from the service VPN to an IPsec tunnel in the transport VPN (VPN 0), you configure an IPsec-specific static route in a service VPN (a VPN other than VPN 0 or VPN 512) :

```
vEdge(config)# vpn vpn-id
vEdge(config-vpn)# ip ipsec-route prefix/length vpn 0 interface ipsecnumber [ipsecnumber2]
```

The VPN ID is that of any service VPN (VPN 1 through 65530, except for 512).

*prefix* / *length* is the IP address or prefix, in decimal four-part-dotted notation, and prefix length of the IPsec-specific static route.

The interface is the IPsec tunnel interface in VPN 0. You can configure one or two IPsec tunnel interfaces. If you configure two, the first is the primary IPsec tunnel, and the second is the backup. With two interfaces, all packets are sent only to the primary tunnel. If that tunnel fails, all packets are then sent to the secondary tunnel. If the primary tunnel comes back up, all traffic is moved back to the primary IPsec tunnel.

## Enable IKE Version 1

When you create an IPsec tunnel on a vEdge router, IKE Version 1 is enabled by default on the tunnel interface. The following properties are also enabled by default for IKEv1:

- Authentication and encryption—AES-256 advanced encryption standard CBC encryption with the HMAC-SHA1 keyed-hash message authentication code algorithm for integrity
- Diffie-Hellman group number—16
- Rekeying time interval—4 hours
- SA establishment mode—Main

By default, IKEv1 uses IKE main mode to establish IKE SAs. In this mode, six negotiation packets are exchanged to establish the SA. To exchange only three negotiation packets, enable aggressive mode:

```
vEdge(config)# vpn vpn-id interface ipsecnumber ike
vEdge(config-ike)# mode aggressive
```

By default, IKEv1 uses Diffie-Hellman group 16 in the IKE key exchange. This group uses the 4096-bit more modular exponential (MODP) group during IKE key exchange. You can change the group number to 2 (for 1024-bit MODP), 14 (2048-bit MODP), or 15 (3072-bit MODP):

```
vEdge(config)# vpn vpn-id interface ipsecnumber ike
vEdge(config-ike)# group number
```

By default, IKE key exchange uses AES-256 advanced encryption standard CBC encryption with the HMAC-SHA1 keyed-hash message authentication code algorithm for integrity. You can change the authentication:

```
vEdge(config)# vpn vpn-id interface ipsecnumber ike
vEdge(config-ike)# cipher-suite suite
```

The authentication *suite* can be one of the following:

- **aes128-cbc-sha1** —AES-128 advanced encryption standard CBC encryption with the HMAC-SHA1 keyed-hash message authentication code algorithm for integrity
- **aes128-cbc-sha2** —AES-128 advanced encryption standard CBC encryption with the HMAC-SHA256 keyed-hash message authentication code algorithm for integrity
- **aes256-cbc-sha1** —AES-256 advanced encryption standard CBC encryption with the HMAC-SHA1 keyed-hash message authentication code algorithm for integrity; this is the default.
- **aes256-cbc-sha2** —AES-256 advanced encryption standard CBC encryption with the HMAC-SHA256 keyed-hash message authentication code algorithm for integrity

By default, IKE keys are refreshed every 1 hours (3600 seconds). You can change the rekeying interval to a value from 30 seconds through 14 days (1209600 seconds). It is recommended that the rekeying interval be at least 1 hour.

```
vEdge(config)# vpn vpn-id interface ipsecnumber ike
vEdge(config-ike)# rekey seconds
```

To force the generation of new keys for an IKE session, issue the **request ipsec ike-rekey** command.

vEdge(config)# **vpn** *vpn-id* **interface ipsec** *number* **ike**

For IKE, you can also configure preshared key (PSK) authentication:

```
vEdge(config)# vpn vpn-id interface ipsecnumber ike
vEdge(config-ike)# authentication-type pre-shared-key pre-shared-secret password
```

*password* is the password to use with the preshared key. It can be an ASCII or a hexadecimal string from 1 through 127 characters long.

If the remote IKE peer requires a local or remote ID, you can configure this identifier:

```
vEdge(config)# vpn vpn-id interface ipsecnumber ike authentication-type
vEdge(config-authentication-type)# local-id id
vEdge(config-authentication-type)# remote-id id
```

The identifier can be an IP address or any text string from 1 through 63 characters long. By default, the local ID is the tunnel's source IP address and the remote ID is the tunnel's destination IP address.

## Enable IKE Version 2

When you configure an IPsec tunnel to use IKE Version 2, the following properties are also enabled by default for IKEv2:

- Authentication and encryption—AES-256 advanced encryption standard CBC encryption with the HMAC-SHA1 keyed-hash message authentication code algorithm for integrity
- Diffie-Hellman group number—16
- Rekeying time interval—4 hours

By default, IKEv2 uses Diffie-Hellman group 16 in the IKE key exchange. This group uses the 4096-bit more modular exponential (MODP) group during IKE key exchange. You can change the group number to 2 (for 1024-bit MODP), 14 (2048-bit MODP), or 15 (3072-bit MODP):

```
vEdge(config)# vpn vpn-id interface ipsecnumber ike
vEdge(config-ike)# group number
```

By default, IKE key exchange uses AES-256 advanced encryption standard CBC encryption with the HMAC-SHA1 keyed-hash message authentication code algorithm for integrity. You can change the authentication:

```
vEdge(config)# vpn vpn-id interface ipsecnumber ike
vEdge(config-ike)# cipher-suite suite
```

The authentication *suite* can be one of the following:

- **aes128-cbc-sha1** —AES-128 advanced encryption standard CBC encryption with the HMAC-SHA1 keyed-hash message authentication code algorithm for integrity
- **aes128-cbc-sha2** —AES-128 advanced encryption standard CBC encryption with the HMAC-SHA256 keyed-hash message authentication code algorithm for integrity
- **aes256-cbc-sha1** —AES-256 advanced encryption standard CBC encryption with the HMAC-SHA1 keyed-hash message authentication code algorithm for integrity; this is the default.
- **aes256-cbc-sha2** —AES-256 advanced encryption standard CBC encryption with the HMAC-SHA256 keyed-hash message authentication code algorithm for integrity

By default, IKE keys are refreshed every 4 hours (14,400 seconds). You can change the rekeying interval to a value from 30 seconds through 14 days (1209600 seconds):

```
vEdge(config)# vpn vpn-id interface ipsecnumber ike
vEdge(config-ike)# rekey seconds
```

To force the generation of new keys for an IKE session, issue the **request ipsec ike-rekey** command.

For IKE, you can also configure preshared key (PSK) authentication:

```
vEdge(config)# vpn vpn-id interface ipsecnumber ike
vEdge(config-ike)# authentication-type pre-shared-key pre-shared-secret password
```

*password* is the password to use with the preshared key. It can be an ASCII or a hexadecimal string, or it can be an AES-encrypted key.

If the remote IKE peer requires a local or remote ID, you can configure this identifier:

```
vEdge(config)# vpn vpn-id interface ipsecnumber ike authentication-type
vEdge(config-authentication-type)# local-id id
vEdge(config-authentication-type)# remote-id id
```

The identifier can be an IP address or any text string from 1 through 64 characters long. By default, the local ID is the tunnel's source IP address and the remote ID is the tunnel's destination IP address.

## Configure IPsec Tunnel Parameters

By default, the following parameters are used on the IPsec tunnel that carries IKE traffic:

- Authentication and encryption—AES-256 algorithm in GCM (Galois/counter mode)
- Rekeying interval—4 hours
- Replay window—32 packets

You can change the encryption on the IPsec tunnel to the AES-256 cipher in CBC (cipher block chaining mode, with HMAC-SHA1-96 keyed-hash message authentication or to null, to not encrypt the IPsec tunnel used for IKE key exchange traffic:

```
vEdge(config-interface-ipsecnumber)# ipsec
vEdge(config-ipsec)# cipher-suite (aes256-cbc-sha1 | aes256-gcm | null-sha1)
```

By default, IKE keys are refreshed every 4 hours (14,400 seconds). You can change the rekeying interval to a value from 30 seconds through 14 days (1209600 seconds):

```
vEdge(config-interface-ipsecnumber)# ipsec
vEdge(config-ipsec)# rekey seconds
```

To force the generation of new keys for an IPsec tunnel, issue the **request ipsec ipsec-rekey** command.

By default, perfect forward secrecy (PFS) is enabled on IPsec tunnels, to ensure that past sessions are not affected if future keys are compromised. PFS forces a new Diffie-Hellman key exchange, by default using the 4096-bit Diffie-Hellman prime module group. You can change the PFS setting:

```
vEdge(config-interface-ipsecnumber)# ipsec
vEdge(config-ipsec)# perfect-forward-secrecy pfs-setting
```

*pfs-setting* can be one of the following:

- **group-2** —Use the 1024-bit Diffie-Hellman prime modulus group.
- **group-14** —Use the 2048-bit Diffie-Hellman prime modulus group.
- **group-15** —Use the 3072-bit Diffie-Hellman prime modulus group.
- **group-16** —Use the 4096-bit Diffie-Hellman prime modulus group. This is the default.
- **none** —Disable PFS.

By default, the IPsec replay window on the IPsec tunnel is 512 bytes. You can set the replay window size to 64, 128, 256, 512, 1024, 2048, or 4096 packets:

```
vEdge(config-interface-ipsecnumber)# ipsec
vEdge(config-ipsec)# replay-window number
```

## Modify IKE Dead-Peer Detection

IKE uses a dead-peer detection mechanism to determine whether the connection to an IKE peer is functional and reachable. To implement this mechanism, IKE sends a Hello packet to its peer, and the peer sends an acknowledgment in response. By default, IKE sends Hello packets every 10 seconds, and after three unacknowledged packets, IKE declares the neighbor to be dead and tears down the tunnel to the peer. Thereafter, IKE periodically sends a Hello packet to the peer, and re-establishes the tunnel when the peer comes back online.

You can change the liveness detection interval to a value from 0 through 65535 seconds, and you change change the number of retries to a value from 0 through 255:

```
vEdge(config-interface-ipsecnumber)# dead-peer-detection seconds retries number
```

## Configure Other Interface Properties

For IPsec tunnel interfaces, you can configure only the following additional interface properties:

```
vEdge(config-interface-ipsec)# mtu bytes
vEdge(config-interface-ipsec)# tcp-mss-adjust bytes
```

## Additional Information

Security Overview

How to configure IKE-enabled IPsec tunnel interfaces on vEdge routers.

## Configuring SD-WAN Security

The Cisco SD-WAN security solution provides an integrated security solution that address all key enterprise security profiles: Compliance, Guest Access, Direct Cloud Access (DCA), and Direct Internet Access (DIA).

*Tags recommended by the template:* article:topic-guide

The Cisco SD-WAN security solution provides an integrated security solution that address all key enterprise security profiles: Compliance, Guest Access, Direct Cloud Access (DCA), and Direct Internet Access (DIA).

## Configuring Security Parameters

How to change security parameters for the control plane and the data plane in the Viptela overlay network.

This article describes how to change security parameters for the control plane and the data plane in the Viptela overlay network.

## Configure Control Plane Security Parameters

By default, the control plane uses DTLS as the protocol that provides privacy on all its tunnels. DTLS runs over UDP.

You can change the control plane security protocol to TLS, which runs over TCP. The primary reason to use TLS is that, if you consider the vSmart controller to be a server, firewalls protect TCP servers better than UDP servers.

You configure the control plane tunnel protocol on a vSmart controller:

```
vSmart(config)# security control protocol tls
```

With this change, all control plane tunnels between the vSmart controller and vEdge routers and between the controller and vManage NMSs use TLS. Control plane tunnels to vBond orchestrators always use DTLS, because these connections must be handled by UDP.

In a domain with multiple vSmart controllers, when you configure TLS on one of the vSmart controllers, all control plane tunnels from that controller to the other controllers use TLS. Said another way, TLS always takes precedence over DTLS. However, from the perspective of the other vSmart controllers, if you have not configured TLS on them, they use TLS on the control plane tunnel only to that one vSmart controller, and they use DTLS tunnels to all the other vSmart controllers and to all their connected vEdge routers. To have all vSmart controllers use TLS, configure it on all of them.

By default, the vSmart controller listens on port 23456 for TLS requests. To change this:

```
vSmart(config)# security control tls-port number
```

The port can be a number from 1025 through 65535.

To display control plane security information, use the **show control connections** command on the vSmart controller. For example:

```
vSmart-2# show control connections
                                                                                      PEER
PEER
PEER     PEER     PEER             SITE        DOMAIN      PEER             PRIVATE  PEER
PUBLIC
TYPE     PROTOCOL SYSTEM IP        ID          ID          PRIVATE IP       PORT     PUBLIC IP
PORT    REMOTE COLOR     STATE           UPTIME
---------------------------------------------------------------------------------------------------------
-----------------------------------------------------
vedge    dtls     172.16.255.11    100         1           10.0.5.11        12346    10.0.5.11
12346   lte              up                   0:07:48:58
vedge    dtls     172.16.255.21    100         1           10.0.5.21        12346    10.0.5.21
12346   lte              up                   0:07:48:51
vedge    dtls     172.16.255.14    400         1           10.1.14.14       12360    10.1.14.14
12360   lte              up                   0:07:49:02
vedge    dtls     172.16.255.15    500         1           10.1.15.15       12346    10.1.15.15
12346   default          up                   0:07:47:18
vedge    dtls     172.16.255.16    600         1           10.1.16.16       12346    10.1.16.16
12346   default          up                   0:07:41:52
vsmart   tls      172.16.255.19    100         1           10.0.5.19        12345    10.0.5.19
12345   default          up                   0:00:01:44
vbond    dtls     -                0           0           10.1.14.14       12346    10.1.14.14
12346   default          up                   0:07:49:08

vSmart-2 control connections
                                                                                      PEER
PEER
PEER     PEER     PEER             SITE        DOMAIN      PEER             PRIVATE  PEER
PUBLIC
TYPE     PROTOCOL SYSTEM IP        ID          ID          PRIVATE IP       PORT     PUBLIC IP
PORT    REMOTE COLOR     STATE           UPTIME
---------------------------------------------------------------------------------------------------------
-----------------------------------------------------
vedge    tls      172.16.255.11    100         1           10.0.5.11        12345    10.0.5.11
12345   lte              up                   0:00:01:18
vedge    tls      172.16.255.21    100         1           10.0.5.21        12345    10.0.5.21
12345   lte              up                   0:00:01:18
vedge    tls      172.16.255.14    400         1           10.1.14.14       12345    10.1.14.14
12345   lte              up                   0:00:01:18
vedge    tls      172.16.255.15    500         1           10.1.15.15       12345    10.1.15.15
12345   default          up                   0:00:01:18
vedge    tls      172.16.255.16    600         1           10.1.16.16       12345    10.1.16.16
12345   default          up                   0:00:01:18
vsmart   tls      172.16.255.20    200         1           10.0.12.20       23456    10.0.12.20
23456   default          up                   0:00:01:32
vbond    dtls     -                0           0           10.1.14.14       12346    10.1.14.14
12346   default          up                   0:00:01:33
```

## Configure DTLS on vManage NMS

If you configure the vManage NMS to use TLS as the control plane security protocol, you must enable port forwarding on your NAT. If you are using DTLS as the control plane security protocol, you do not need to do anything.

The number of ports forwarded depends on the number of vdaemon processes running on the vManage NMS. To display information about these processes and about and the number of ports that are being forwarded, use the **show control summary** command shows that four vdaemon processes are running:

```
vManage# show control summary
          VBOND     VMANAGE    VSMART    VEDGE
INSTANCE  COUNTS    COUNTS     COUNTS    COUNTS
------------------------------------------------
0           2          0          2        7
1           2          0          0        5
2           2          0          0        5
3           2          0          0        4
```

To see the listening ports, use the **show control local-properties** command:

```
vManage# show control local-properties
organization-name            vIPtela Inc Test
certificate-status           Installed
root-ca-chain-status         Installed

certificate-validity         Valid
certificate-not-valid-before May 20 00:00:00 2015 GMT
certificate-not-valid-after  May 20 23:59:59 2016 GMT

dns-name                     vbond.viptela.com
site-id                      5000
domain-id                    0
protocol                     dtls
tls-port                     23456
...
...
...
number-active-wan-interfaces 1

                 PUBLIC         PUBLIC  PRIVATE        PRIVATE
ADMIN     OPERATION  LAST
INDEX  INTERFACE IP             PORT    IP             PORT     VSMARTS  VMANAGES  COLOR
CARRIER          STATE     STATE      CONNECTION
---------------------------------------------------------------------------------------------------------
--------------------------------------------------------
0      eth0      72.28.108.37   12361   172.16.98.150  12361    2        0         silver
default          up        up        0:00:00:08
```

This output shows that the listening TCP port is 23456. If you are running vManage NMS behind a NAT, you should open the following ports on the NAT device:

- 23456 (base - instance 0 port)
- 23456 + 100 (base + 100)
- 23456 + 200 (base + 200)
- 23456 + 300 (base + 300)

Note that the number of instances is the same as the number of cores you have assigned for the vManage NMS, up to a maximum of 8.

# Configure Data Plane Security Parameters

In the data plane, IPsec is enabled by default on all vEdge routers, and by default IPsec tunnel connections use the AH-SHA1 HMAC for authentication on the IPsec tunnels. On vEdge routers, you can change the type of authentication, and you can modify the IPsec rekeying timer and the size of the IPsec anti-replay window.

## Configure Allowed Authentication Types

By default, IPsec tunnel connections use AH-SHA1 HMAC and ESP HMAC-SHA1 for authentication, choosing whichever authentication method is stronger. To modify the negotiated authentication types or to disable authentication, use the following command:

```
vEdge(config)# security ipsec authentication-type (ah-no-id | ah-sha1-hmac | none | sha1-hmac)
```

Configure each authentication type with a separate **security ipsec authentication-type** command. The command options map to the following authentication types, which are listed in order from most strong to least strong:

- **ah-sha1-hmac** enables AH-SHA1 HMAC and ESP HMAC-SHA1.
- **ah-no-id** enables a modified version of AH-SHA1 HMAC and ESP HMAC-SHA1. This option accommodates some non-Viptela devices, including the Apple AirPort Express NAT, that have a bug that causes the ID field in the IP header, a non-mutable field, to be modified. Configure the **ah-no-id** option in the list of authentication types to have the Viptela AH software ignore the ID field in the IP header so that the Viptela software can work in conjunction with these devices.
- **sha1-hmac** enables ESP HMAC-SHA1.
- **none** maps to no authentication. You can choose this option in situations where data plane authentication and integrity are not a concern.

For information about which data packet fields are affected by these authentication types, see the "Data Plane Integrity" section in Data Plane Security Overview .

vEdge routers advertise their configured authentication types in their TLOC properties. The two routers on either side of an IPsec tunnel connection negotiate the authentication to use on the connection between them, using the strongest authentication type that is configured on both of the routers. For example, if one vEdge router advertises AH-HMAC-SHA1, ESP HMAC-SHA1, and none, and a second vEdge router advertises ESP HMAC-SHA1 and none, the two routers negotiate to use ESP HMAC-SHA1 on the IPsec tunnel connection between them. If no common authentication types are configured on the two vEdge peers, no IPsec tunnel is established between them.

The encryption algorithm on IPsec tunnel connections is either AES-256-GCM or AES-256-CBC. For unicast traffic, if the remote side supports AES-256-GCM, that encryption algorithm is used. Otherwise, AES-256-CBC is used. For multicast traffic, the encryption algorithm is AES-256-CBC. You cannot modify the choice made by the software.

When the IPsec authentication type is changed, the AES key for the data path is changed.

## Change the Rekeying Timer

Before vEdge routers can exchange data traffic, they set up a secure authenticated communications channel between them. The vEdge routers use the DTLS or TLS control plane connection between them as the channel, and they use the AES-256 cipher to perform encryption. Each vEdge router generates a new AES key for its data path periodically.

By default, a key is valid for 86400 seconds (24 hours), and the timer range is 10 seconds through 1209600 seconds (14 days). To change the rekey timer value:

```
vEdge(config)# security ipsec rekey seconds
```

The configuration looks like this:

```
security
  ipsec
```

```
    rekey seconds
  !
```

When the IPsec keys are compromised, you can generate new keys immediately, without modifying the configuration of the vEdge router. To do this, issue the **request security ipsec-rekey** command on the compromised vEdge router.

For example, the following output shows that the local SA has a SPI (key) of 256:

```
vEdge# show ipsec local-sa

                                          SOURCE           SOURCE
TLOC ADDRESS     TLOC COLOR       SPI     IP               PORT    KEY HASH
------------------------------------------------------------------------------
172.16.255.15    lte              256     10.1.15.15       12346   *****b93a
```

If this key is compromised, use the **request security ipsec-rekey** command to generate a new key immediately. This command increments the existing key, so in our example the SPI changes to 257:

```
vEdge# request security ipsec-rekey
vEdge# show ipsec local-sa
                                          SOURCE           SOURCE
TLOC ADDRESS     TLOC COLOR       SPI     IP               PORT    KEY HASH
------------------------------------------------------------------------------
172.16.255.15    lte              257     10.1.15.15       12346   *****b93a
```

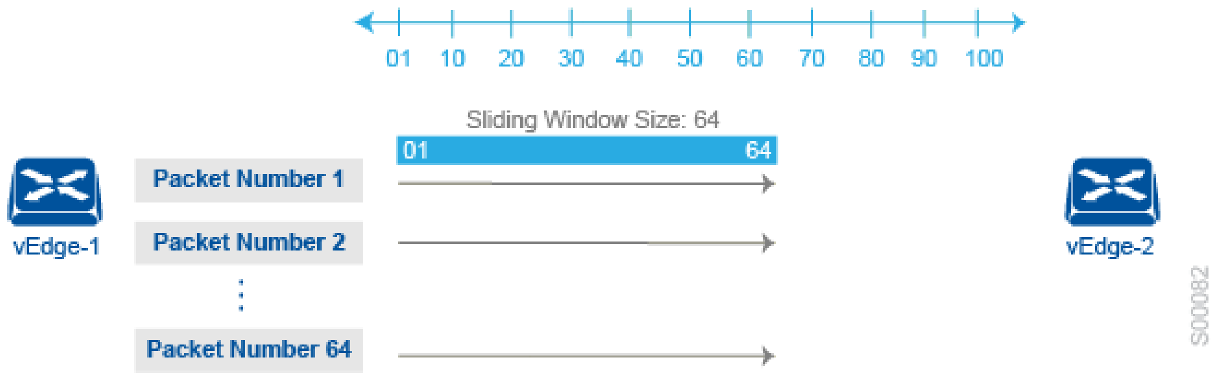
After the new key is generated, the vEdge router sends it immediately to all its DTLS or TLS peers, and they begin using it as soon as they receive it. Note that the old compromised SPI (256) will continue to be used for a short period of time, until it times out.

To stop using the compromised key immediately, issue the **request security ipsec-rekey** command twice, in quick succession. This sequence of commands removes both SPI 256 and 257, and sets the key to 258. Note, however, that some packets will be dropped for a short period of time, until all the remote vEdge routers learn the new key.

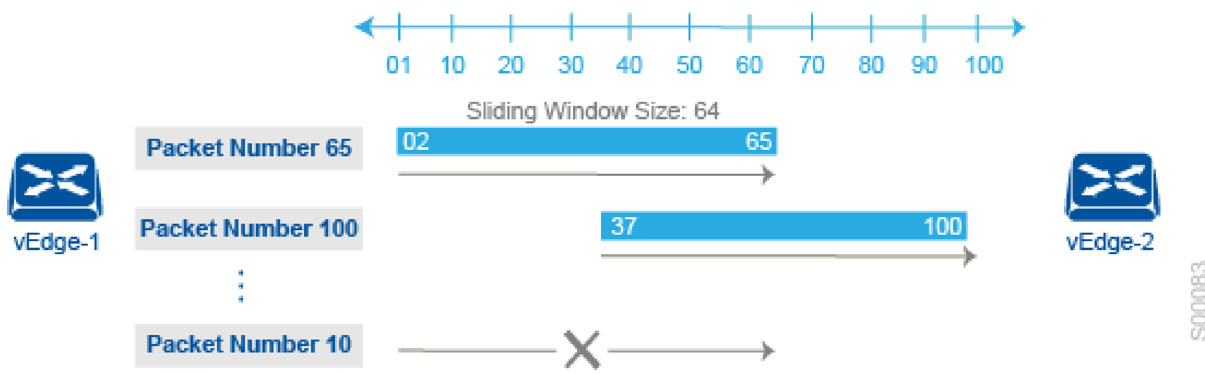
```
vEdge# request security ipsec-rekey
vEdge# request security ipsec-rekey
vEdge# ipsec local-sa
                                          SOURCE           SOURCE
TLOC ADDRESS     TLOC COLOR       SPI     IP               PORT    KEY HASH
------------------------------------------------------------------------------
172.16.255.15    lte              258     10.1.15.15       12346   *****b93a
```

## Change the Size of the Anti-Replay Window

IPsec authentication provides anti-replay protection by assigning a unique sequence number to each packet in a data stream. This sequence numbering protects against an attacker duplicating data packets. With anti-replay protection, the sender assigns monotonically increasing sequence numbers, and the destination checks these sequence numbers to detect duplicates. Because packets often do not arrive in order, the destination maintains a sliding window of sequence numbers that it will accept.




Packets with sequence numbers that fall to the left of the sliding window range are considered old or duplicates, and the destination drops them. The destination tracks the highest sequence number it has received, and adjusts the sliding window when it receives a packet with a higher value.




By default, the sliding window is set to 512 packets. It can be set to any value between 64 and 8192 that is a power of 2 (that is, 64, 128, 256, 512, 1024, 2048, 4096, or 8192). To modify the anti-replay window size, use the **replay-window** command, specifying the size of the window:

```
vEdge(config)# security ipsec replay-window  number
```

The configuration looks like this:

```
security
  ipsec
    replay-window number
  !
!
```

If QoS is configured on a vEdge router, that router might experience a larger than expected number of packet drops as a result of the IPsec anti-replay mechanism, and many of the packets that are dropped are legitimate ones. This occurs because QoS reorders packets, giving higher-priority packets preferential treatment and delaying lower-priority packets. To minimize or prevent this situation, increase the size of the anti-replay window.

## Additional Information

[show control connections]
[show security-info]
[Security Overview]

# Configuring Single Sign-On using Okta

Configuring SSO using OKTA

Okta provides secure identity management software that lets you connect any person with any application on any device using Single Sign-On (SSO).

Perform the following steps for configuring SSO:

- Configure SSO on the vManage UI
- Configure SSO on the Okta website

To configure SSO on the vManage UI:

1. In vManage, click **Administration** ► **Settings** ► **Identify Provider Settings** ► **Edit** .
2. Click **Enabled** .
3. Navigate to **Click here to download the SAML metadata** and save the content in a file. This data will be used for configuring Okta.
4. In Metadata, you need the following information to configure Okta with vManage:

- Entity ID
- Signing certificate
- Encryption certificate
- Logout URL
- Login URL

To configure SSO on the Okta website:

1. Log on to the Okta website.
2. Create a username using your email address.
   Make sure you are using the Classic UI view on Okta. If not, change your view to the Classic UI view by clicking on the **Admin** button in the upper-right corner.
3. On the next page in the upper-left corner, switch from the Developer Console view to the Classic UI view.
4. Navigate to **Add applications** ► **Add application** .
5. Select **SAML 2.0** and click **Create** .
6. Use a string for **Application name** .
7. (Optional) Upload a logo and then click **Next** .
8. At **SAML Settings** , add the SSO URL using the **samlLoginResponse** URL from the downloaded metadata from the vManage UI.
9. Copy the entityID string and paste it in the **Service Provider ID** field.
10. For **Name ID format** , select **EmailAddress** and then click **Enter** .
11. For **Application username** , select **Okta username** .
12. For **Show Advanced Settings** , enter the fields as indicated below.

| Component | Value | Configuration |
|---|---|---|

| | | |
|---|---|---|
| Response | Signed | |
| Assertion Signature | Signed | |
| Signature Algorithm | RSA-SHA256 | |
| Digest Algorithm | SHA256 | |
| Assertion Encryption | Encrypted | |
| Encryption Algorithm | AES256-CBC | |
| Key Transport Algorithm | RSA-OAEP | |
| Encryption Certificate | | 1. Copy the encryption certificate from the metadata you downloaded.<br>2. Go to **www.samltool.com** and click on **X.509 CERTS,** paste there. Click **Format X.509 Certificate** .<br>3. Make sure to remove the last empty line and then save the output ( **X.509.cert with header** ) into a text file **encryption.cer** .<br>4. Upload the file. The Firefox browser may not allow you to do the upload. You can use the Chrome browser, however. You should see the certificate information after uploading to Okta. |
| Enable Single Logout | | Make sure this is checked. |
| Single Logout URL | | Get from the metadata. |
| SP Issuer | | Use the entityID from the metadata. |
| Signature Certificate | | 5. Obtain from the metadata.<br>Format the signature certificate using **www.samltool.com** as done above.<br>6. Save to a file, for example, **signing.cer** and upload. |
| Authentication context class | X.509 Certificate | |
| Honor Force Authentication | Yes | |
| SAML issuer ID string | SAML issuer ID string | |
| Attributes Statements (optional) | Name ► Username<br>Name format (optional) ► Unspecified<br>Value ► *user.login* | |
| Group Attribute Statements (optional) | Name ► Groups<br>Name format (optional) ► Unspecified<br>Filter ► "Regex" - ".*" | |

It is mandatory to use the two strings, Username and Groups, exactly as shown above. Otherwise, you may be logged in with the default group of Basic.

13. Click **Next** .
14. For **App type** , check **This is an internal app that we have created** (optional).
15. Click **Finish** .
    This brings you to the Okta application page.
16. Click on **View Setup Instructions** .
17. Copy the IDP metadata.
18. Navigate back to the vManage UI.
19. Click on I **dentity Provider Settings** .
20. Paste the IDP metadata that you copied on to **Upload Identity Provider Metadata** , and then click **Save** .

To assign users to the application in Okta:

1. On the Okta application page, navigate to **Assignments** ▶ **People** ▶ **Assign** .
2. Select **Assign to people** from the drop-down menu.
3. Click on **Assign** next to the user(s) you selected and click **Done** .
4. To add a user, click on **Directory** ▶ **Add Person** ▶ **Save** .

Configuring SSO using Okta

## Configuring the Security Virtual Image for IPS/IDS and URL Filtering

This section describes how to install, configure, activate, and update the Cisco SD-WAN Release 18.4 IPS/IDS and URL-F Security Policy Virtual Image.

Cisco release 18.4 supports intrusion prevention/intrusion detection systems (IPS/IDS) and URL filtering (URL-F) for IOS XE and IOS XE SD-WAN devices. These features enable application hosting, real-time traffic analysis, and packet logging on IP networks. Once the image file is uploaded to the vManage Software Repository, you can create policy, profile, and device templates that will push the policies and updates to the correct devices automatically.

The following router platforms support the 18.4 security virtual image:

- Cisco Integrated Service Router 4351 (ISR-4351)
- Cisco Integrated Service Router 4331 (ISR-4331)
- Cisco Integrated Service Router 4321 (ISR-4321)
- Cisco Integrated Service Router 4221 (ISR-4221X)
- Cisco Integrated Service Router 4431 (ISR-4431)
- Cisco Integrated Service Router 4451 (ISR-4451)
- Cisco Integrated Service Router 1111X-8P (ISR-1111X-8P)
- Cisco Cloud Services Router 1000v series

IPS/IDS and URL filtering is not supported on ASR platforms for this release.

To install and configure IPS/IDS and URL-F security policies for release 18.4 requires the following workflow:

Task 1: Upload the Cisco security virtual image to vManage
Task 2: Create a security policy template for IPS/IDS or URL filtering

Task 3: Create a feature profile template for IPS/IDS or URL filtering
Task 4: Create a device template
Task 5: Attach devices to the device template

## Upload the Cisco Security Virtual Image to vManage

The IPS/IDS and URL-F feature set is contained within a TAR file, which can be downloaded from the Cisco website, and uploaded to your vManage software repository as a virtual image.

To download the security virtual image to your vManage software repository:

1. Go to https://software.cisco.com/download/home and sign on. The Software Download page displays.
2. Browse to Downloads ▶ Home ▶ Routers ▶ Branch Routers ▶ XE SD-WAN Routers.
3. From the right-most pane, select your router model. The Software Download page displays for your selected router.
4. From the list of software options, select " **UTD Snort IPS Engine Software** ."
5. From the list on the left-hand side, select an image option, such as Latest Release, or 18.4.x. The page will look similar to the following example. The correct file will begin with " **UTD Engine for** …"
6. Click the icon on the right-hand side of the window to download the image file.
7. From the vManage dashboard, select Maintenance ▶ Software Repository.
8. Select **Virtual Images** from the top options.
9. Click **Upload Virtual Image** , and select either **vManage** or **Remote Server – vManage** . The Upload Virtual Image to vManage window opens.
10. Drag and drop, or browse to the image file and select it (your image file will be different).
11. Click **Upload** . When the upload completes, a confirmation message displays. The new virtual image displays in the Virtual Images Software Repository.

## Create a Security Policy Template for IPS/IDS or URL-F

Once the image is uploaded, use the Add Security Policy configuration wizard to build your IPS/IDS or URL-F policies. For a complete description of this task, see " Intrusion Prevention Configuration on SD-WAN ."

1. From the vManage dashboard, select Configuration ▶ Security.
2. Click **Add Security Policy** . The Add Security Policy wizard displays.
3. Select your security scenario from the list of options.
4. Select the scenario that most closely fits your needs, and click **Proceed** .

## Create a Feature Profile Template for IPS/IDS or URL-F

The feature profile template configures two functions:

- **NAT** – Enable or disable network address translation, which protects internal IP addresses when outside the firewall.
- **Resource Profile** – Allocate default or high resources to different subnets or devices.

A feature profile template, while not strictly required, is recommended.

To configure a security profile template for IPS/IDS or URL-F:

1. From the vManage dashboard, select Configuration ▶ Templates.
2. Click **Feature** .
3. Click **Add Template** . The add feature template page displays.
4. From the Select Devices list on the left, select the device(s) you want to associate with the template.
5. In the Select Template ▶ Basic Information section, click **Security App Hosting** . The Security App Hosting template page displays.
6. Enter a name for the template in the Template Name field. Make it as descriptive as possible.
7. Optionally, enter a description of the template in the Description field. Scroll to the Security Policy Parameters section.
8. **NAT** – Click **On** to enable network address translation (NAT), or **Off** to disable it. By default, NAT is on.
9. Click the drop-down menu to set boundaries for the policy. The default is **Default** .

- **Global** – Enable NAT for all devices attached to the template.
- **Device Specific** – Enable NAT only for specified devices. If you select Device Specific, enter the name of a device key.
- **Default** – Enable the default NAT policy for devices attached to the template.

10. **Resource Profile** – Choose Default or High to designate the resource profile for devices attached to this template. The default is High.
11. Click the drop-down menu to set boundaries for the resource profile. The default is **Global** .

- **Global** – Enable the selected resource profile for all devices attached to the template.
- **Device Specific** – Enable the profile only for specified devices. If you select Device Specific, enter the name of a device key.
- **Default** – Enable the default resource profile for devices attached to the template.

12. When you have finished, click **Save** . The Feature Profile template displays in the Configuration ▶ Templates ▶ Feature page table.

## Create a Device Template

To activate the policies you want to apply, you can create a device template that will push the policies to the devices that need them. The available options vary with the device type. For example, vManage devices require a more limited subset of the larger device template. You will only see valid options for that device model. For information about other template options, see Templates .

To create a security device template, follow this example for vEdge 2000 model routers:

1. From the vManage dashboard, select Configuration ▶ Templates ▶ Device. The device configuration table displays.
2. Click Create Template ▶ From Feature Template. The add device template page displays.
3. Select the device model from the Select Devices list on the left. The device template page displays.
4. Enter a name for the template in the Template Name field.
5. Optionally, enter a description of the template in the Description field.

6. Scroll down the page to the four configuration sub-menus. Each field allows you to select an existing template, to create a new template, or to view the existing template. For example, to create a new System template, click **Create Template** .

Fields with an asterisk are required.

## Basic Information

7. **System** - Use the System template for all Cisco SD-WAN devices, to configure system-wide parameters using vManage templates. For a full description, see System .

8. **Logging** - Use the Logging template for all SD-WAN devices, to configure logging to either the local hard drive or a remote host. For a full description, see Logging .

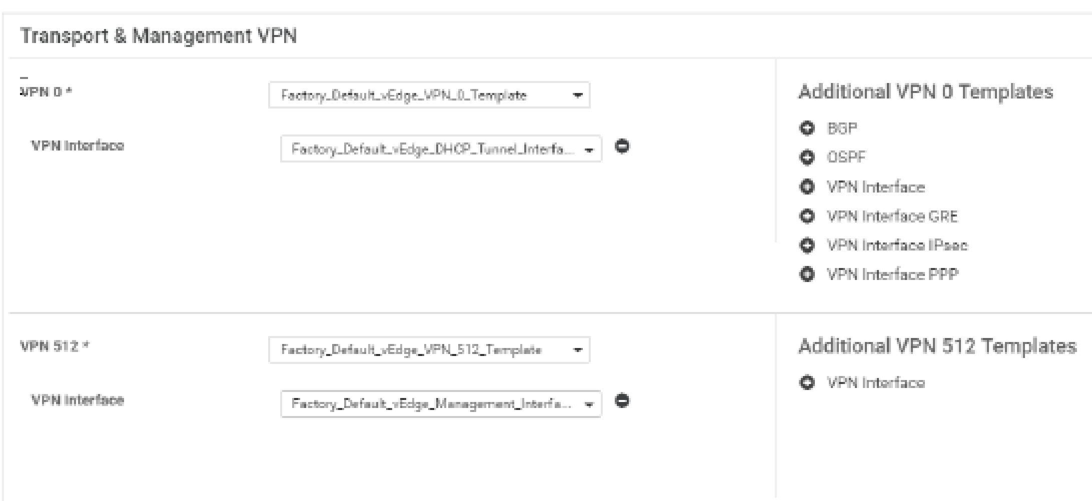
9. Optionally, from the Additional System Templates section to the right, you can select templates stored in an archive or NTP system. Click **Archive** or **NTP** to open a menu field where you can browse to the template file.

10. Select templates for the following protocols from the drop-down menus, or leave the defaults:

- **AAA** Authentication, Authorization, and Accounting - For AAA support, in combination with RADIUS and TACACS+. For a full description, see AAA .
- **BFD** Bidirectional Forwarding Detection - The BFD protocol, which detects link failures as part of the Cisco high availability solution, is enabled by default on all vEdge routers, and you cannot disable it. For a full description, see BFD .
- **OMP** Edge Overlay Management Protocol - Use OMP to establish and maintain the SD-WAN control plane. OMP is enabled by default on all SD-WAN vEdge routers, vManage NMSs, and vSmart controllers, so there is no need to explicitly configure or enable OMP. OMP must be operational for the Viptela overlay network to function. If you disable it, you disable the overlay network. For a full description, see OMP .
- **Security** - On vEdge Cloud and vEdge routers and on vBond orchestrators, use this template to configure IPsec for data plane security. On vManage NMSs and vSmart controllers, use this template to configure DTLS or TLS for control plane security. For a full description, see **Intrusion Protection, Intrusion Detection, and URL Filtering**

## Transport and Management VPN

For a full description of VPN options, see VPN .



10. From the Transport and Management VPN section, select templates for the following virtual private networks (VPNs) from the drop-down menus, or leave the defaults:

- **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.

11. Optionally, from the Additional VPN 0 Templates section to the right, you can select templates for the following protocols and interfaces:

- **BGP** Border Gateway Protocol
- **OSPF** Open Shortest Path First
- **VPN Interface** – Optionally, create templates for VPNs 1 through 511, and 513 through 65530.
- **GRE** VPN Interface Generic Routing Encapsulation
- **IPsec** VPN Interface IPsec - IPsec tunnels on vEdge routers running Internet Key Exchange (IKE) sessions.
- **PPP** VPN Interface Point-to-Point Protocol (PPP)

12. Optionally, from the Additional VPN 512 Templates section to the right, you can select templates for the management VPN, and related VPN interfaces. Choose **vEdge DHCP tunnel interface** , or the **default** management interface.

## Service VPN

For a full description of VPN options, see VPN .

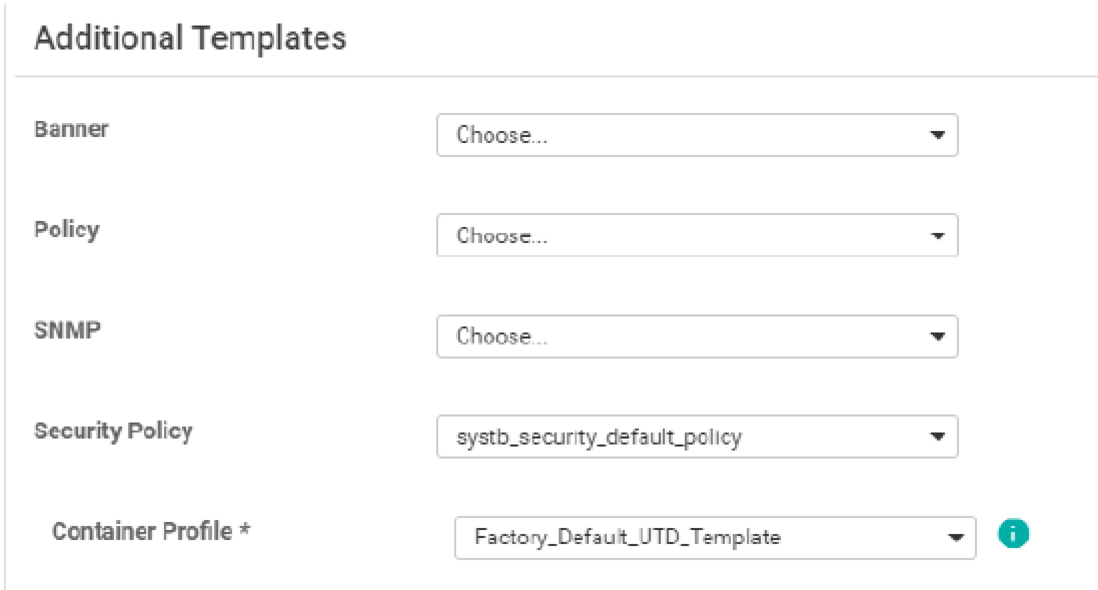
13. Optionally, from the Service VPN section, click the **+** icon to create a template for service VPNs other than VPN 0 and VPN 512.

14. Optionally, from the Service VPN section to the right, you can select templates for the following protocols and interfaces:

- **BGP** Border Gateway Protocol
- **IGMP** Internet Group Message Protocol
- Multicast routing
- **OSPF** Open Shortest Path First
- **PIM** Protocol-Independent Multicast
- **VPN Interface** – Choose vEdge DHCP tunnel interface, or the default management interface. Optionally, designate a DHCP sub-template.
- **Bridge** - VPN Interface Bridge. Optionally, designate a DHCP sub-template.
- **GRE** - VPN Interface Generic Routing Encapsulation.
- **IPsec** - VPN Interface IPsec. Optionally, designate a DHCP sub-template.
- **Natpool** - VPN Interface Natpool. Optionally, designate a DHCP sub-template.

The NAT pool defines a range of IP addresses that the firewall can use to translate the source address of connections from VPN clients. The NAT pool translates the addresses in the same way as NAT rules do. Connections that use the NAT Pool must not match any NAT rules.

## Additional Templates




15. Optionally, you can create feature templates for the following additional network elements:

- **Banner** – You can configure two different banner text strings, one to be displayed before the CLI login prompt on a Viptela device and the other to be displayed after a successful login to the device. For a full description, see Banner .
- **Policy** –
- **SNMP** – Use the Simple Network Management Protocol (SNMP) template to configure SNMP parameters for all Cisco SD-WAN devices and Cisco IOS XE routers running the SD-WAN software. For a full description, see SNMP .
- **Security Policy** – Select the IPS/IDS or URL-F Security Policy template you created (see Create a Security Policy Template for IPS/IDS or URL-F . Once you select a Security Policy template, the Container Profile option displays.
- **Container Profile** – Select the IPS/IDS or URL-F Feature Profile template you created (see Create a Feature Profile Template for IPS/IDS or URL-F ).

## Bridge Ports

16. For devices that support bridging, optionally, from the Bridge section, click the **+** icon to select the number of bridge profiles you need. Then choose the profile and an ID range between **1-63** .

## Create the Device Template

17. When you have finished assigning templates, click **Create** . The new template will display in the Configuration ► Templates ► Device table.

# Additional Information

## Intrusion Prevention Configuration on SD-WAN

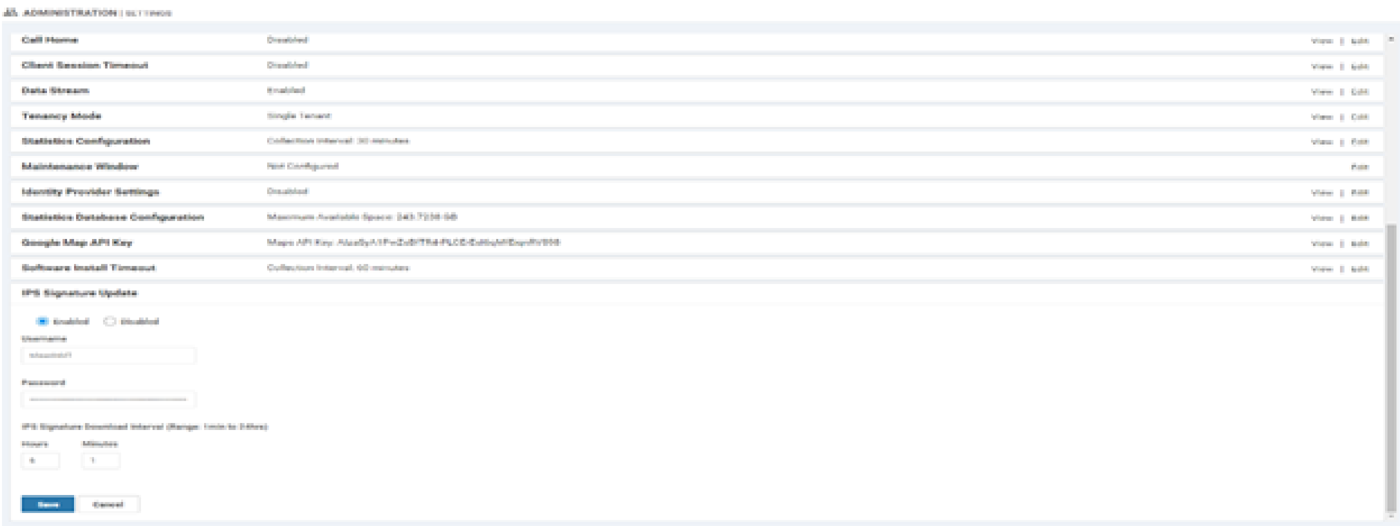
How to configure Intrusion Prevention on SD-WAN routers.

You can configure Intrusion Prevention policy with a configuration wizard. The Intrusion Prevention configuration workflow contains the following components:

- Administration Settings
- Intrusion Prevention Configuration
- Apply IPS Policy to a device

## Administration Settings

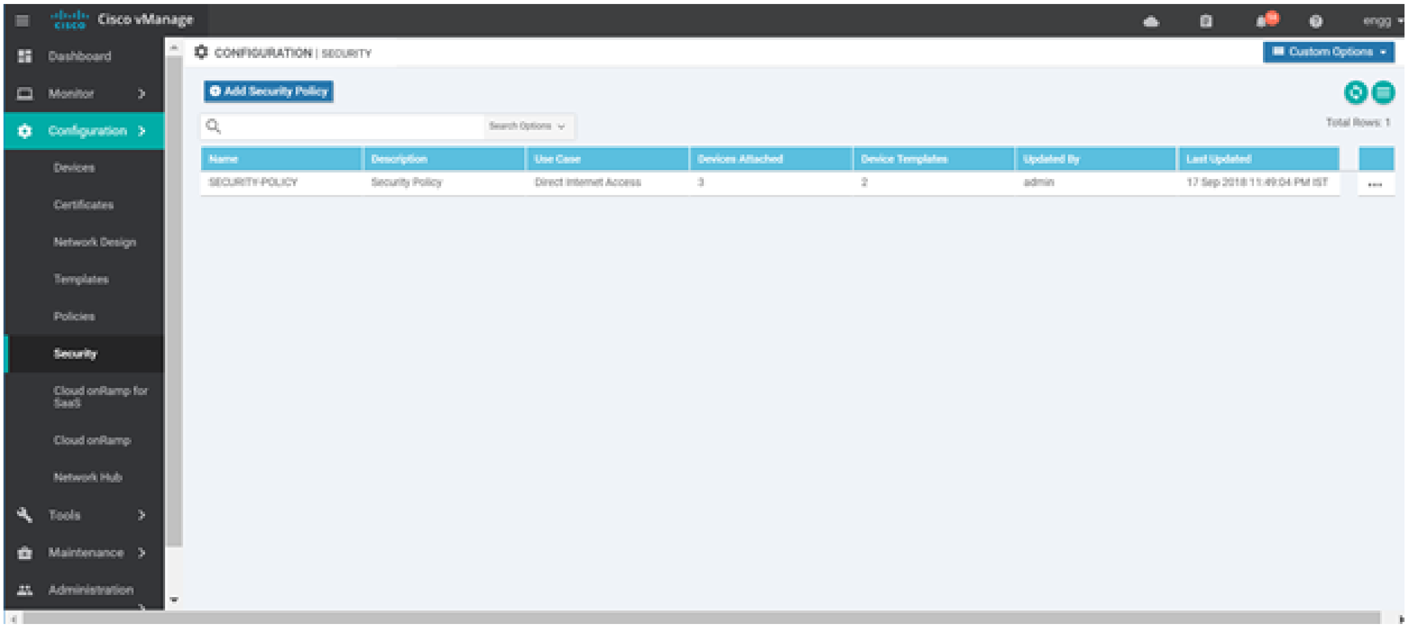
In Cisco vManage NMS, select the Administration ► Settings tab in the left side panel to configure IPS Signature Update. Click on **Edit** to **Enable/Disable** and provide **Username** and **Password** details to save the Policy details as shown in the following screenshot.



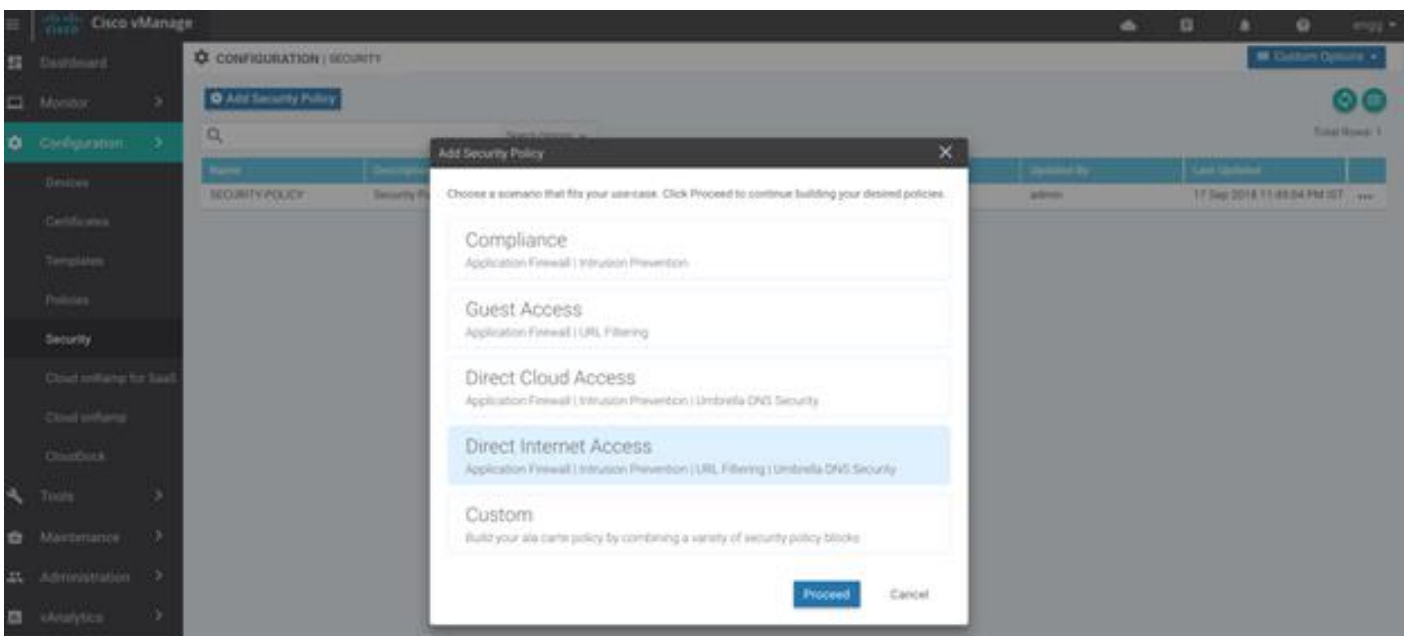

## Intrusion Prevention Configuration

To configure Intrusion Prevention through Security, use the vManage security configuration wizard:

1. In Cisco vManage NMS, select the Configuration ► Security tab in the left side panel.



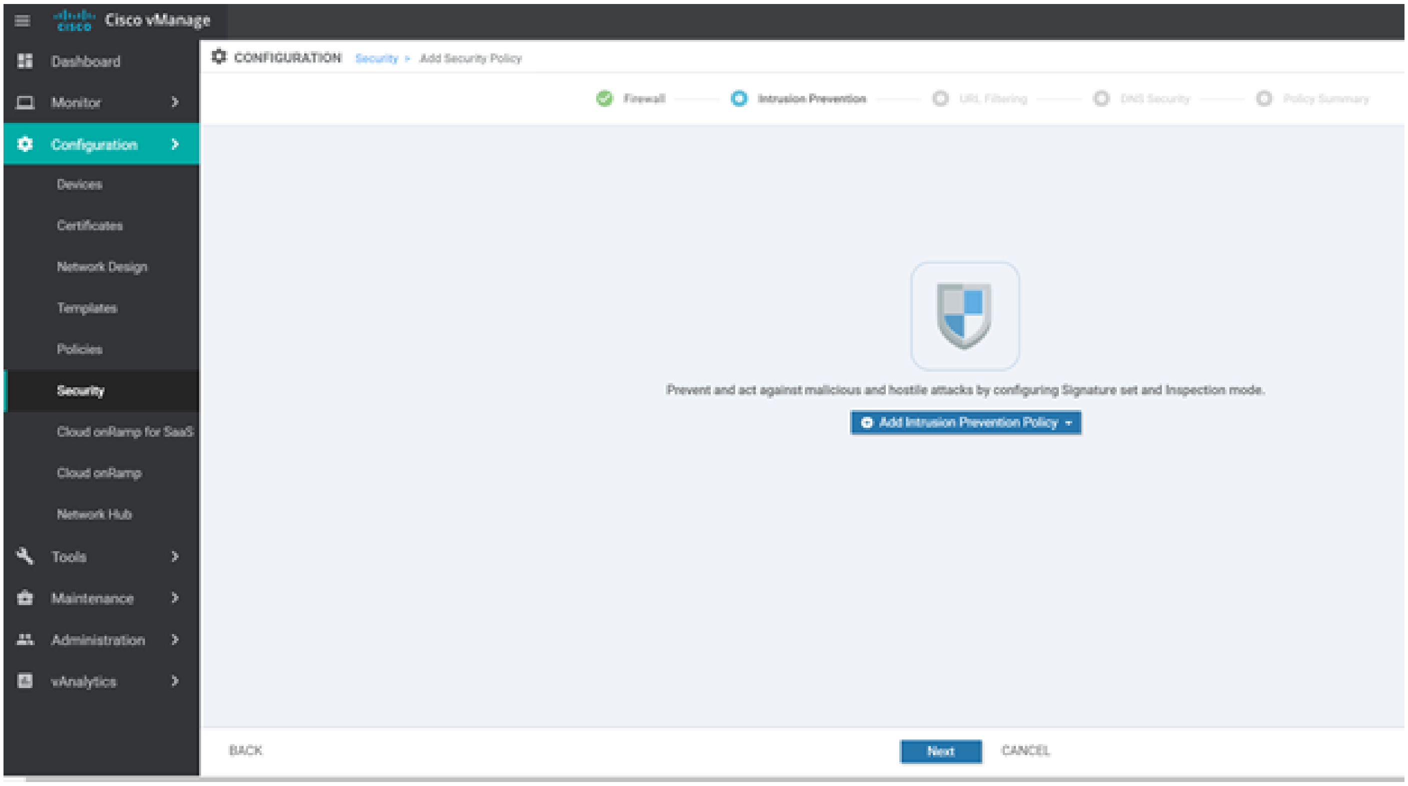

2. Click **Add Security Policy** . The Add Security Policy wizard opens, and various use-case scenarios display.



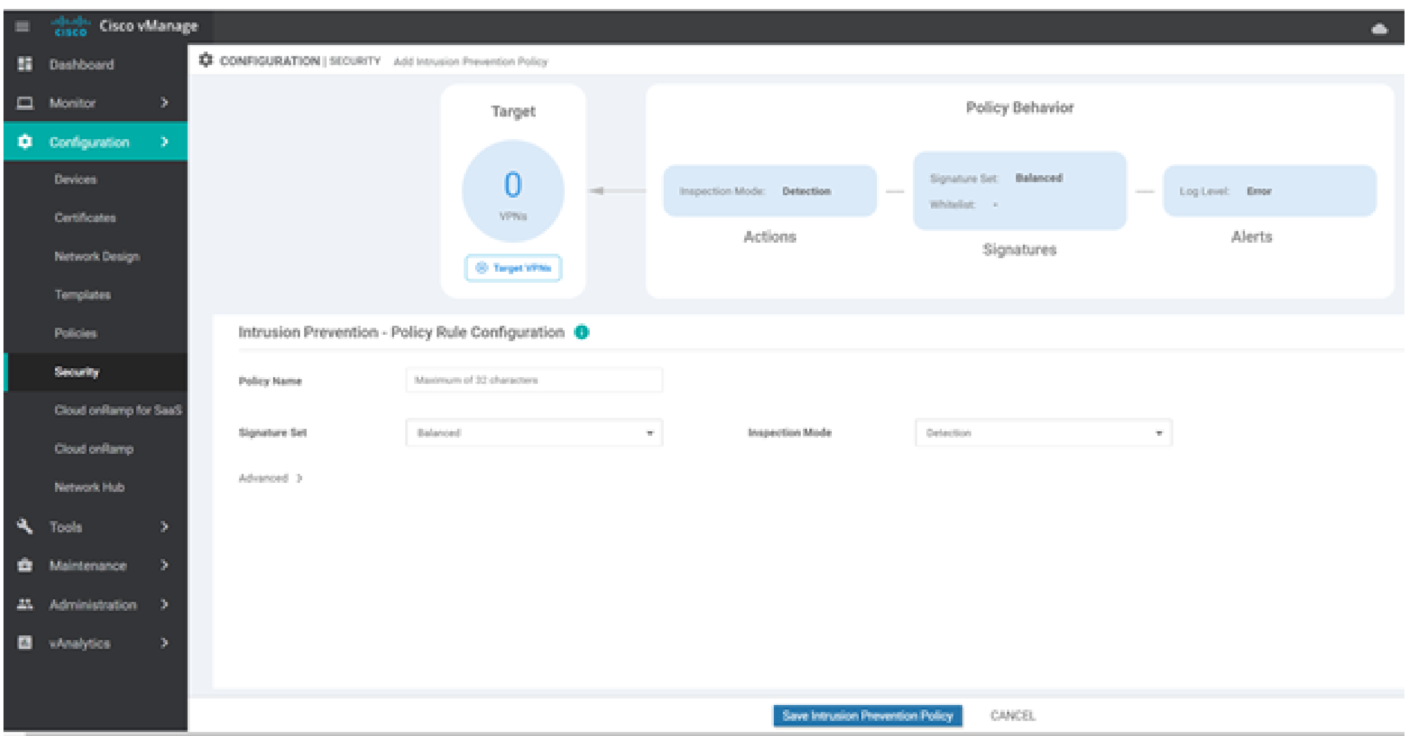

3. In Add Security Policy, select a scenario that supports intrusion prevention ( **Compliance** , **Direct Cloud Access** , **Direct Internet Access** , or **Custom** ).

4. Click **Proceed** to add an Intrusion Prevention policy in the wizard.

5. In the **Add Security Policy** wizard, click **Next** to select the **Add Intrusion Prevention** tab to create a new Intrusion Prevention Policy.




6. Click the **Add Intrusion Prevention Policy** drop-down, select **Create New** to create a new Intrusion Prevention policy. The Intrusion Prevention - Policy Rule Configuration wizard appears.




7. Enter a policy name in the **Policy Name** field.

8. Choose a signature set that defines rules for evaluating traffic from the Signature Set drop-down. The following options are available. Connectivity provides the least restrictions and the highest performance. Security provide the most protections but can affect system performance.

- Connectivity—Less restrictive/better performance (fewer rules)
- Balanced—Designed to provide protection without a significant effect on system performance
- SecuritySecurity—More protection/less performance

9. Choose mode of operation from the Inspection Mode drop-down. The following options are available:

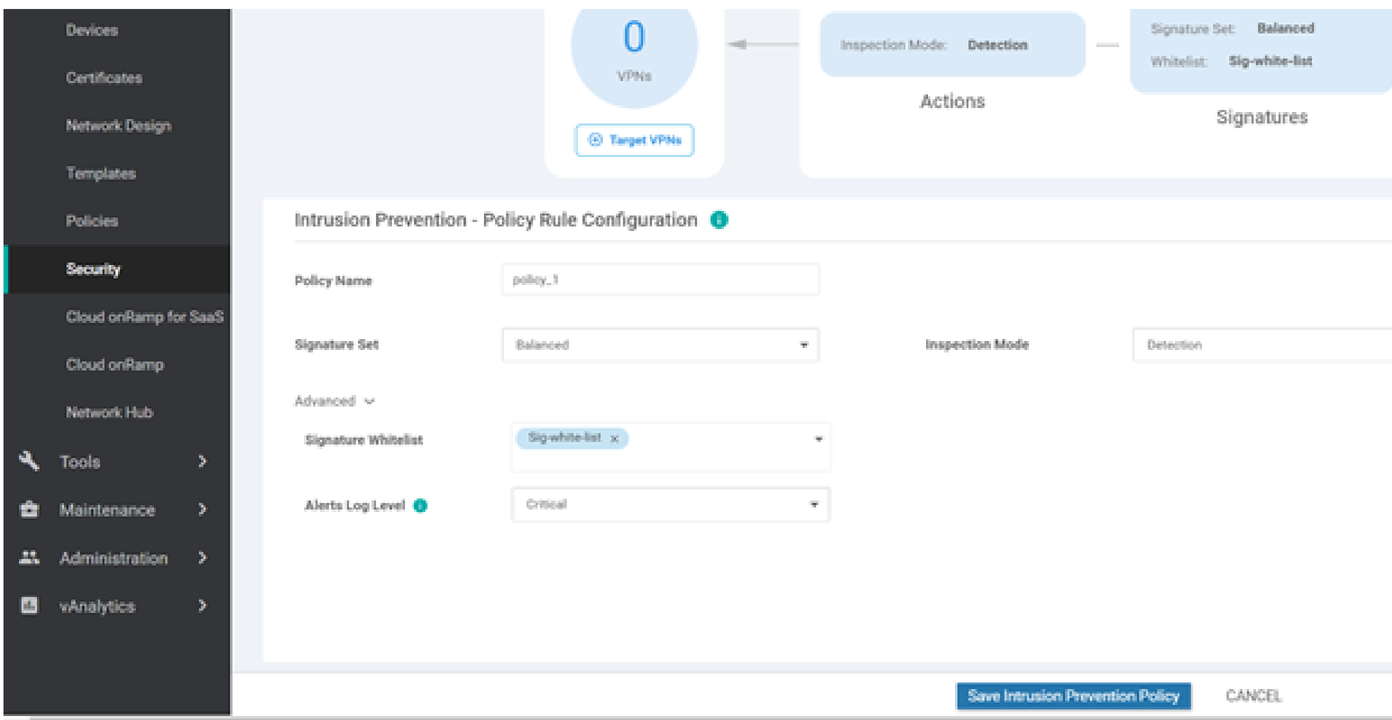
- Detection—Select this option for intrusion detection mode
- Protection—Select this option for intrusion protection mode

10. From the Advanced tab, choose one or more existing IPS signature allowed lists or create new ones as needed from the Signature Whitelist drop-down.

To create a new signature list, click **New Signature List** at the bottom of the drop-down. In the IPS Signature List Name field, enter a list name consisting of up to 32 characters (letters, numbers, hyphens and underscores only). In the IPS Signature field, enter signatures in the format Generator ID:Signature ID, separated with commas.You also can use the Import button to add a allowed list from an accessible storage location. Click Save when you are finished.

You also can create or manage IPS Signature Whitelist lists by selecting the **Configuration** ► **Security** tab in the left side panel, choosing **Lists** from the Custom Options drop-down at the top right of the page, and then selecting **Signatures** in the left panel.

To remove an IPS Signature Whitelist from the Signature Whitelist field, click the “X” next to the list name in the field.

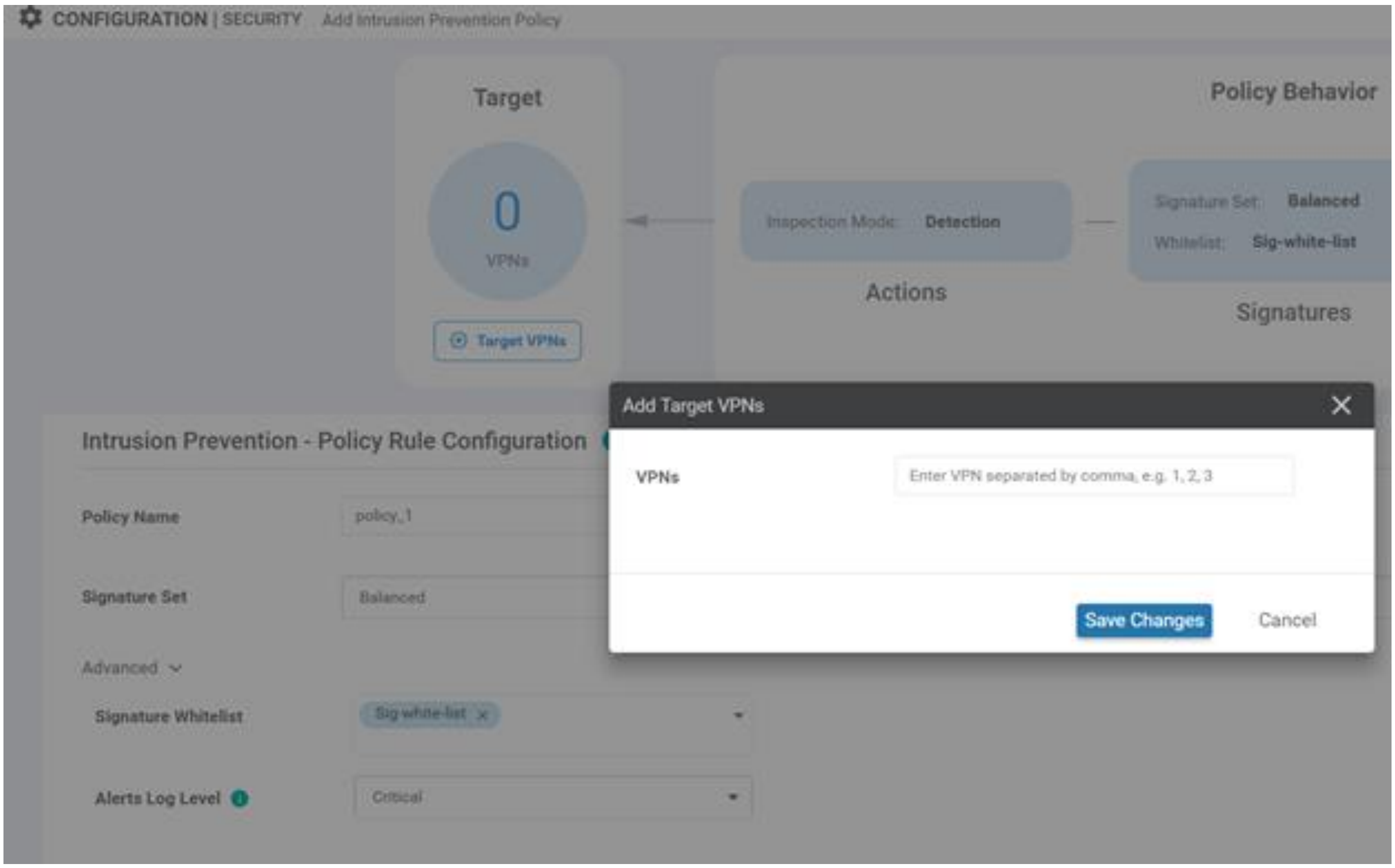



11. Choose an alert level for syslogs from the **Alert Log Level** drop-down. The options are:

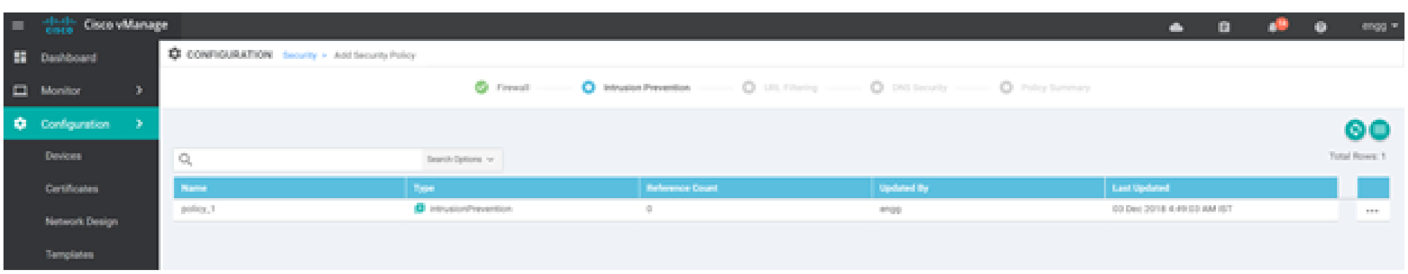
- Emergency
- Alert
- Critical

- Error
- Warning
- Notice
- Info
- Debug

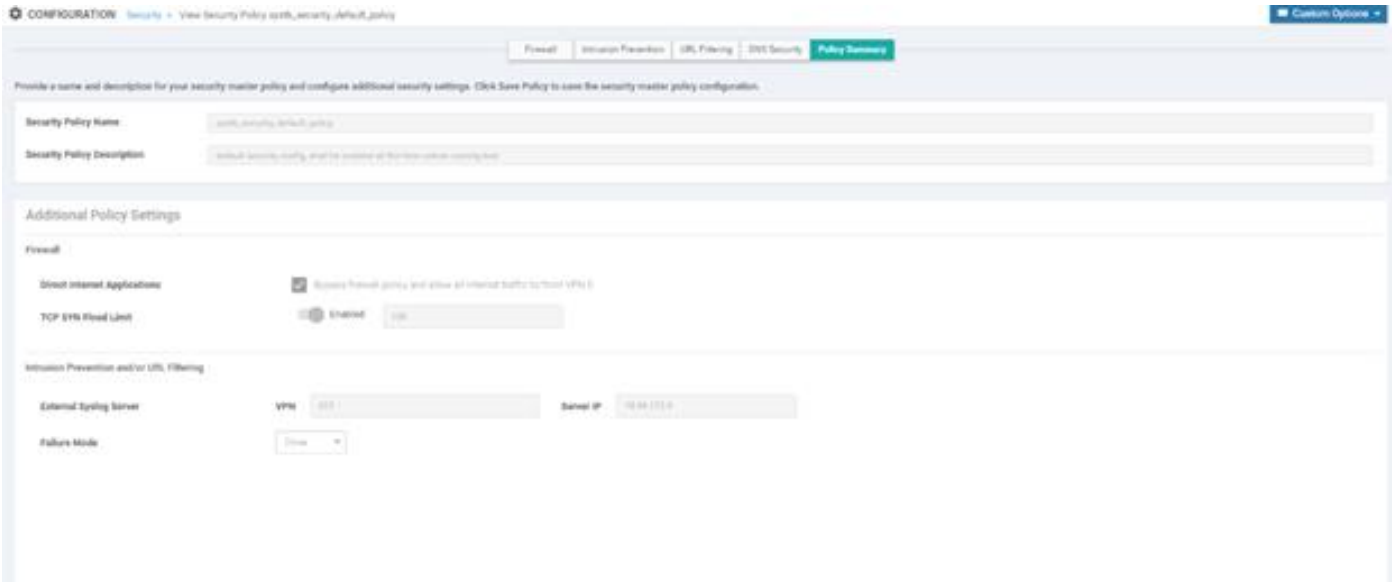
12. Click on **Target VPNs** to add required number of VPNs in Add Target VPNs wizard.




13. Click **Save Changes** to add an Intrusion Prevention policy.




14. Click on **Policy Summary** tab to attach a policy to Security Master Policy Configuration.




15. Enter Security Policy Name and Security Policy Description in the respective fields.

16. In the Additional Policy Settings tab ▶ Intrusion Prevention and/or URL Filtering, choose the following options:

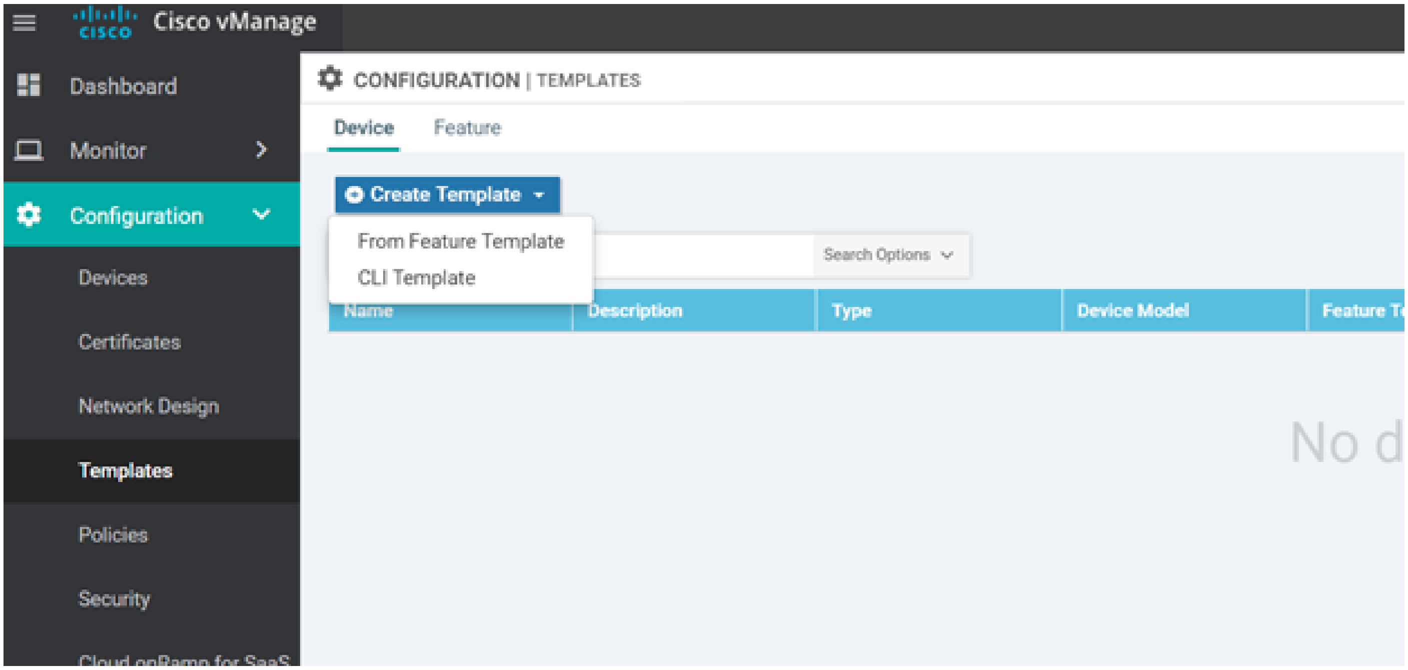
- External Syslog Server VPN
- Server IP
- Failure Mode – Open/Close

17. Click **Save Policy Changes** to configure Intrusion Security policy.

18. You can edit the existing Intrusion Prevention policy by clicking on **Custom Options** in the right-side panel of vManage ▶ Configuration ▶ Security wizard.

## Applying Intrusion Prevention Policy to a Device

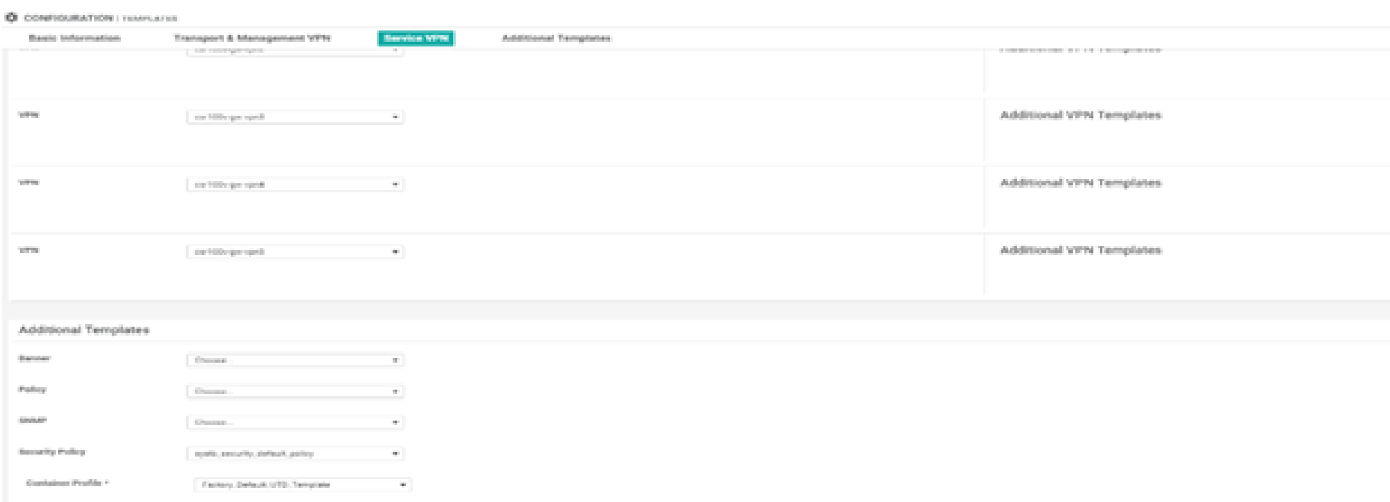
1. In vManage NMS, select the Configuration ▶ Templates screen.




2. In the Device tab, from the **Create Template** drop-down, select **From Feature Template** .

3. From the **Device Model** drop-down, select one of the IOS XE SD-WAN devices.

4. Click the **Additional Templates** tab located directly beneath the **Description** field. The screen scrolls to the **Additional Templates** section.




5. From the **Security Policy** drop-down, select the name of the **Intrusion Policy** you configured in the above procedure.

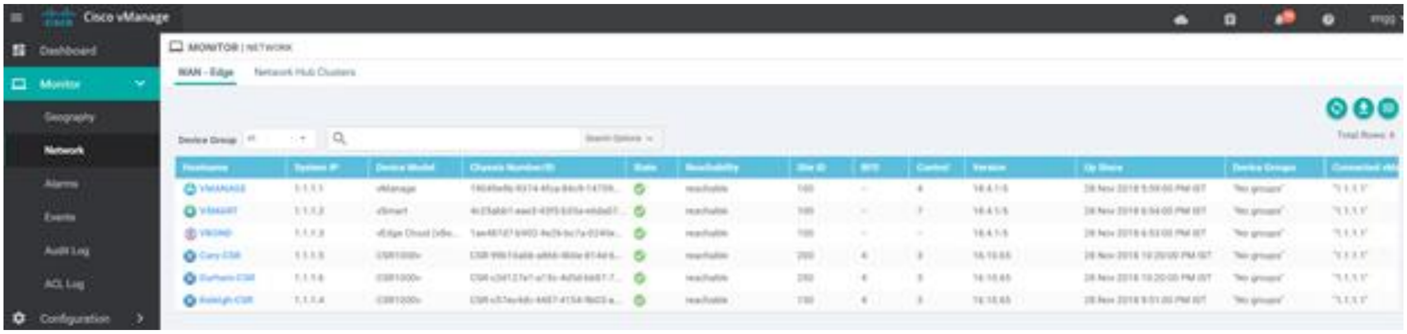
6. Click **Create** to apply Intrusion policy to a device.

## Monitoring Intrusion Prevention Feature

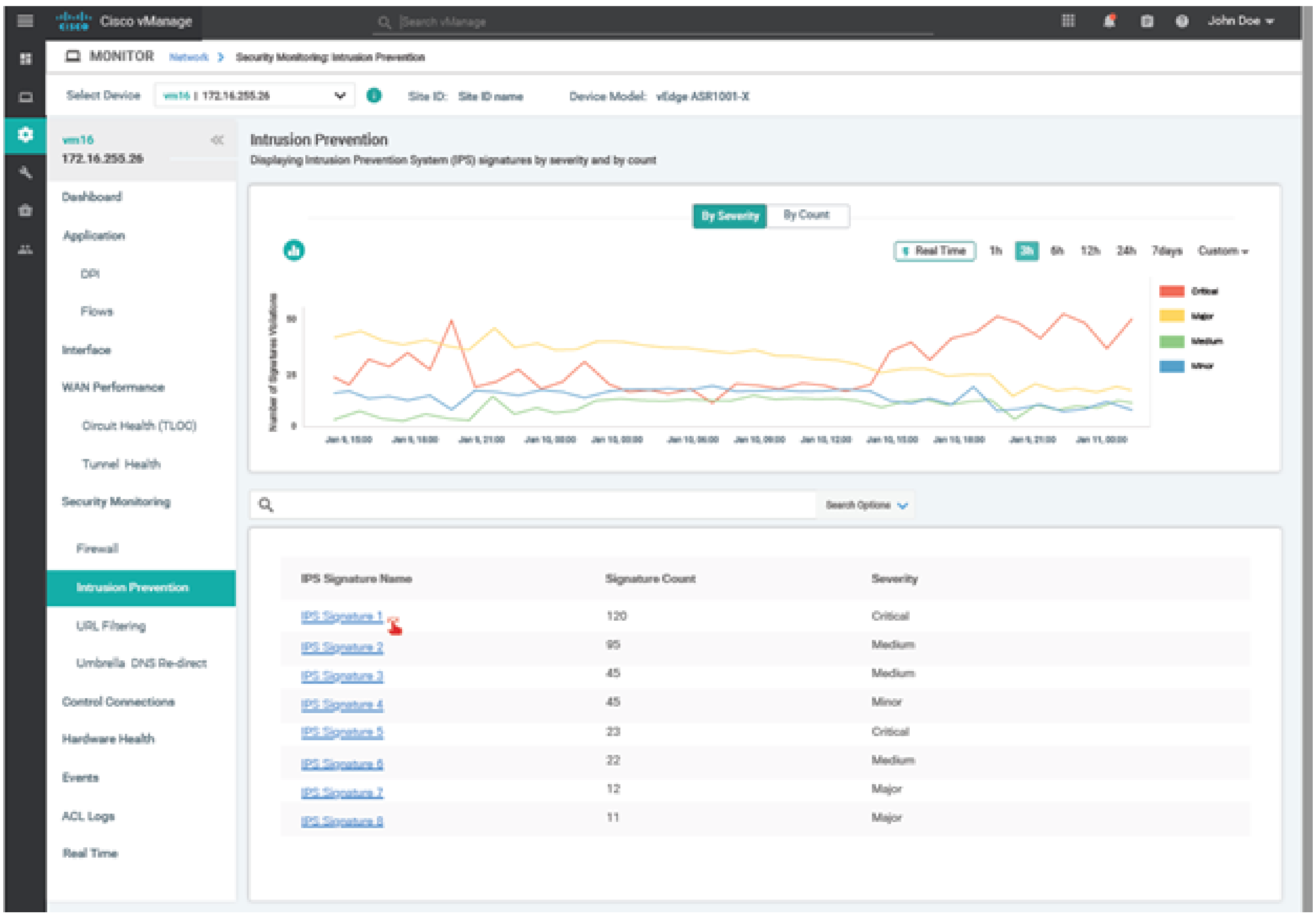
You can monitor the Intrusion Prevention System (IPS) signature violations by severity and by count using the following steps.

To monitor the Signatures of IPS Configuration on IOS XE SD-WAN device:

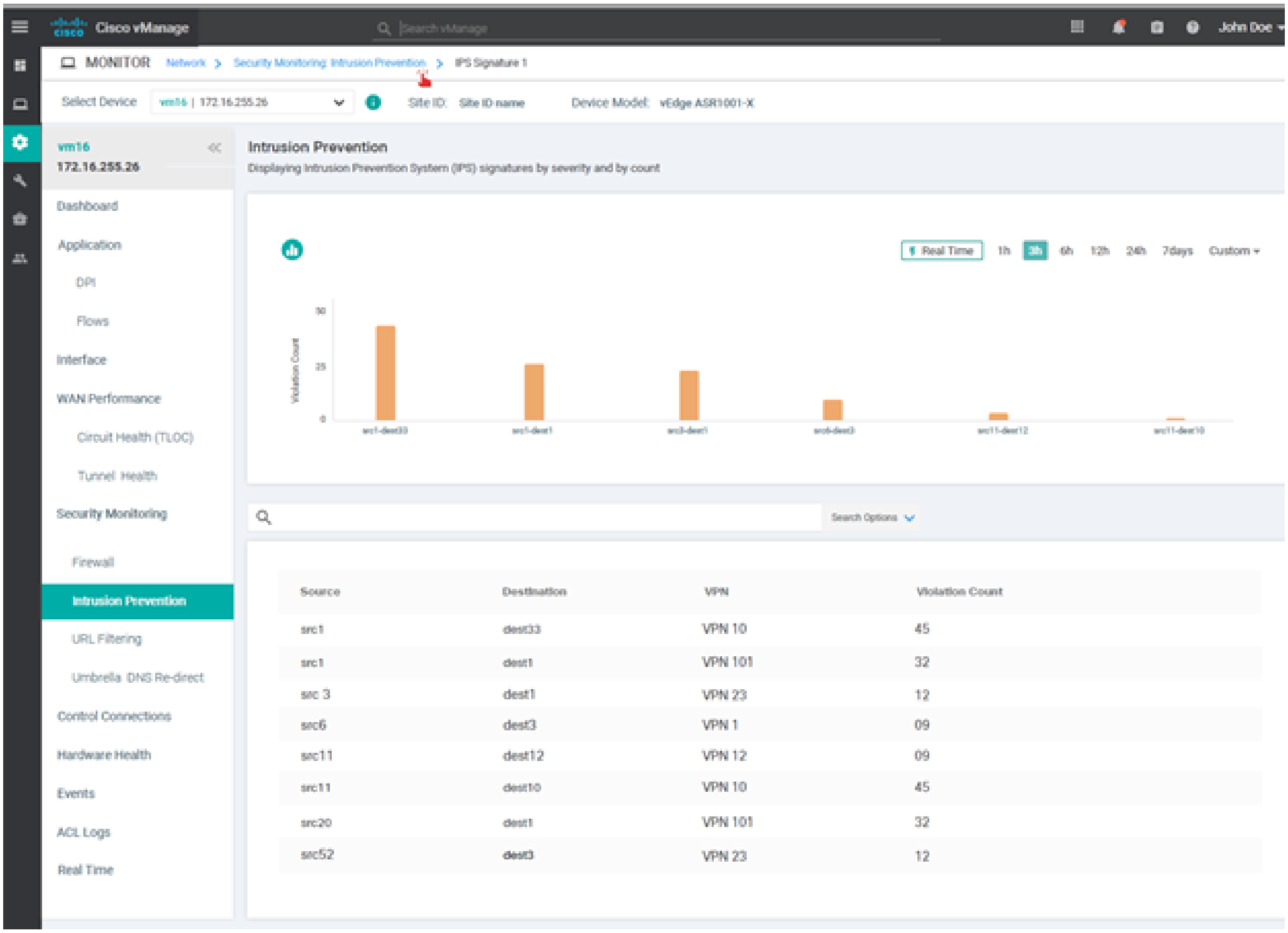
1. From the Monitor ► Network screen, select a device.




2. In the left panel, under **Security Monitoring** , select **Intrusion Prevention** tab. The Intrusion Prevention wizard displays.




3. Click **By Severity** or **By Count** to designate how you want to display intrusion prevention information.




Close message

[Learn more]

Welcome to your new guide!

Click on "New" to build out your guide.

How to configure Intrusion Prevention on SD-WAN routers.

# URL Filtering Configuration on vManage

How to configure URL Filtering on a vManage

# URL Filtering Configuration on SD-WAN

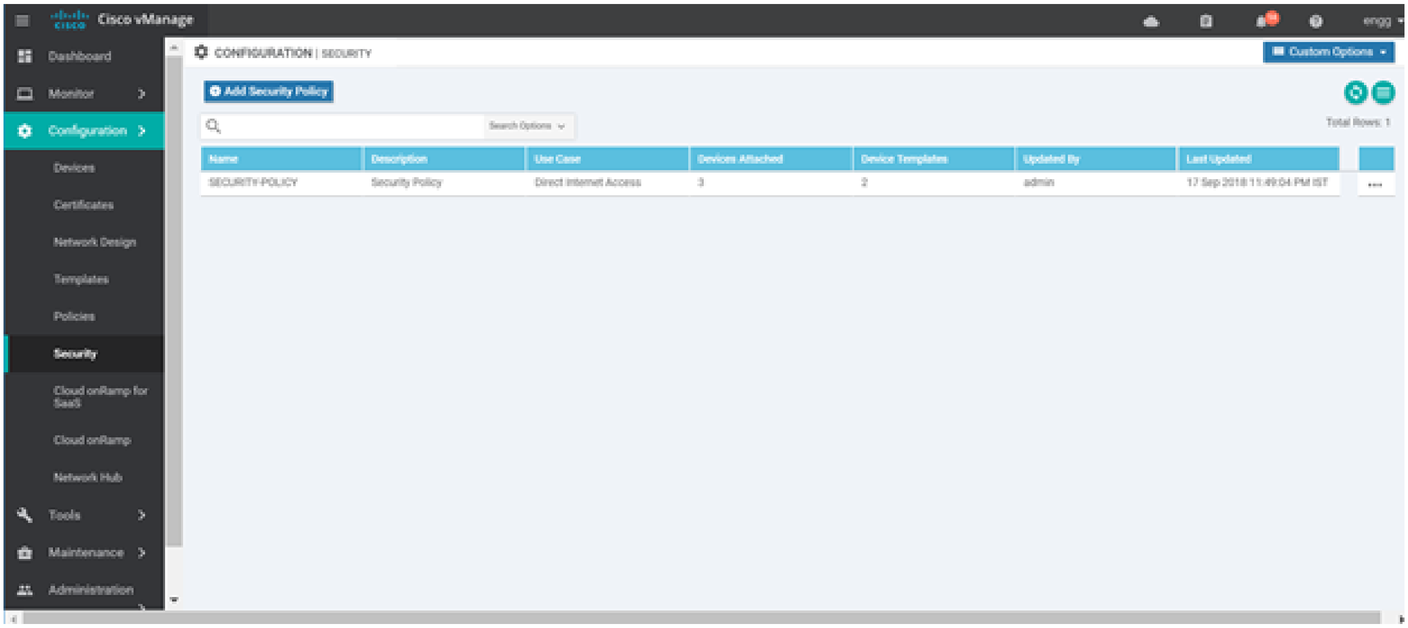
The URL Filtering feature enables the user to provide controlled access to Internet websites or Intranet sites by configuring URL-based policies and filters on the device. The URL Filtering feature is implemented using the Snort Intrusion Prevention engine.

You can configure URL Filtering with a Security configuration wizard.

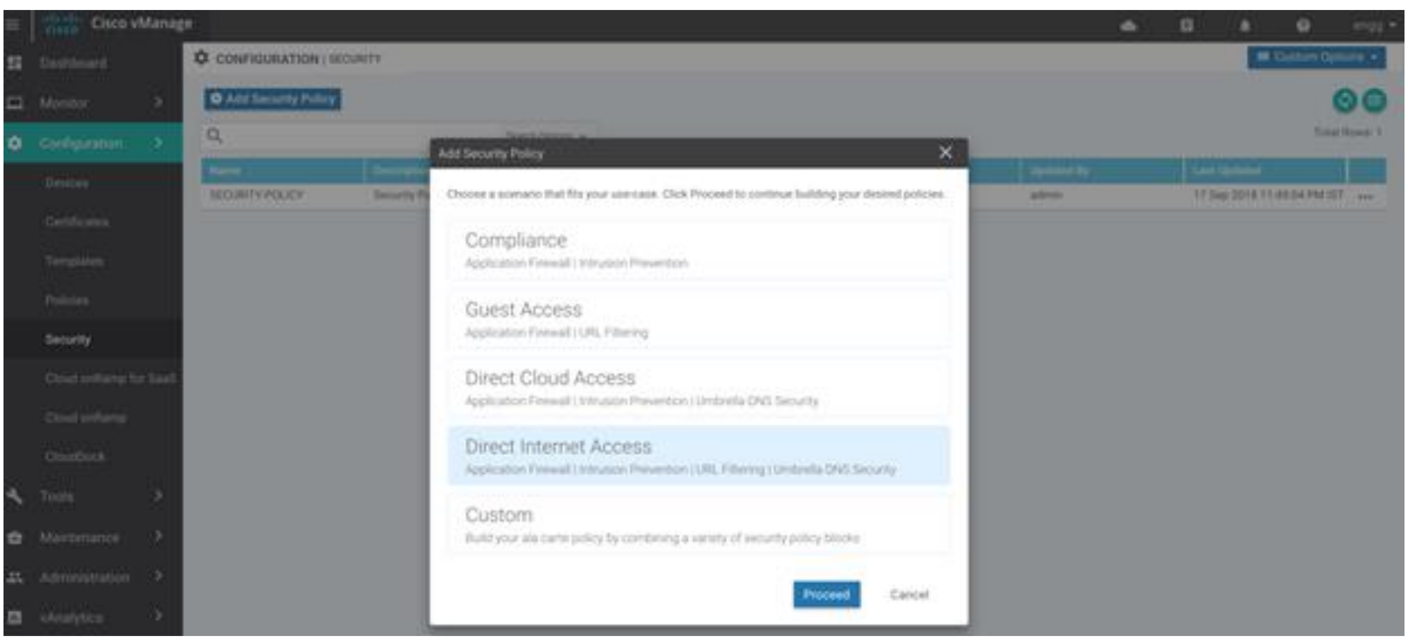
## URL Filtering Configuration

To configure URL Filtering through Security, use the vManage security configuration wizard:

1. In Cisco vManage, select the Configuration ► Security tab in the left side panel.



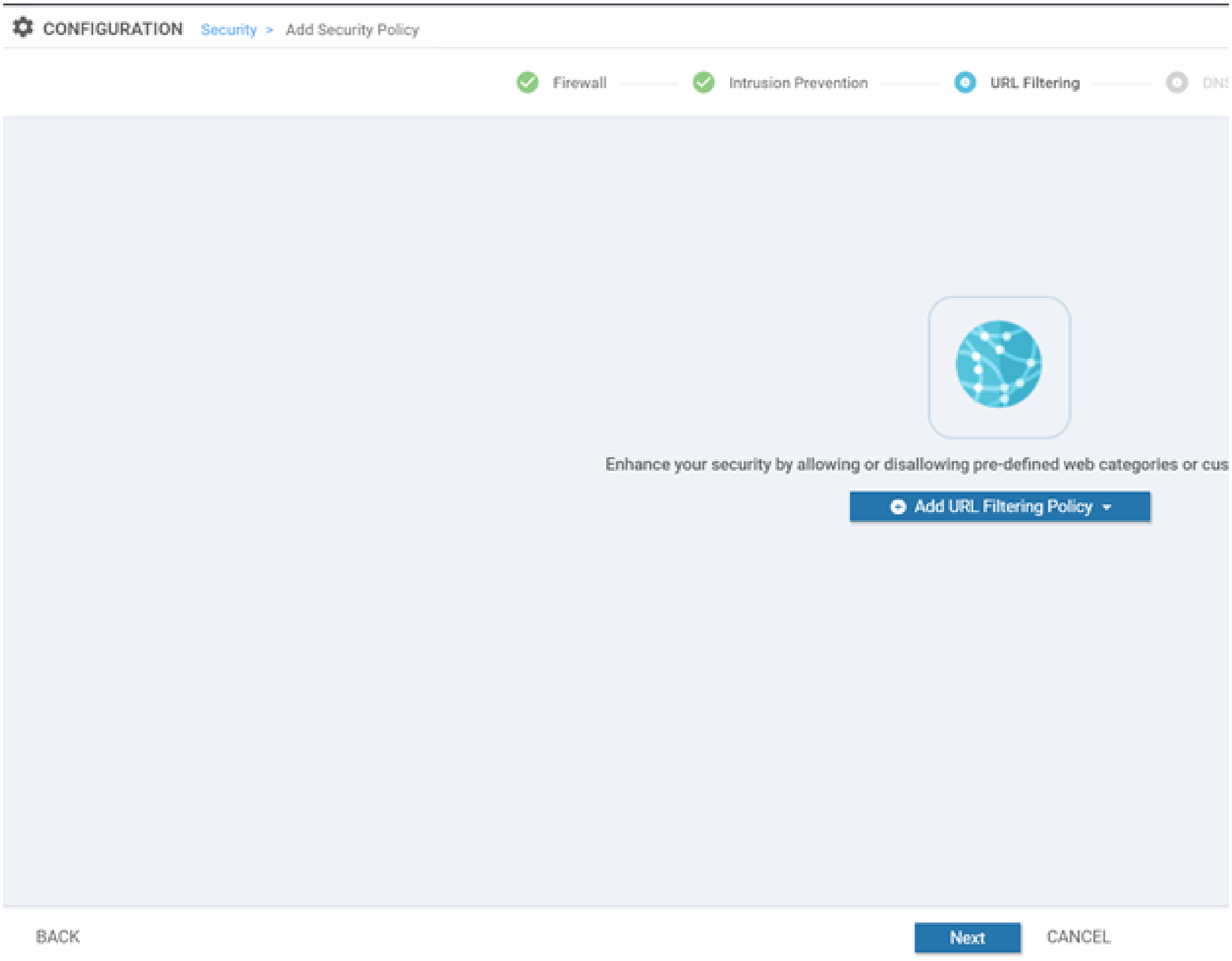

2. Click Add Security Policy. The Add Security Policy wizard appears and various use-case scenarios display.



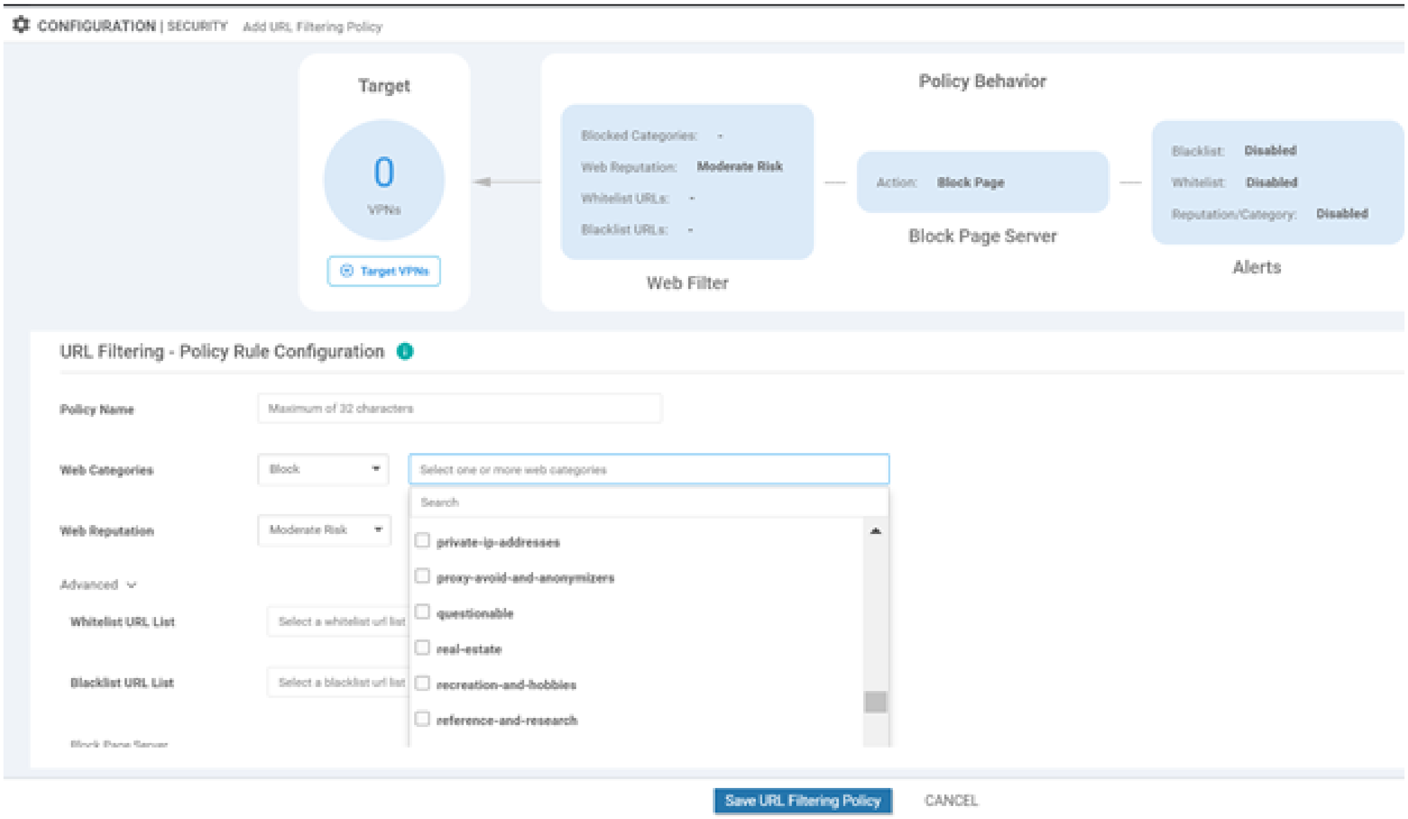

3. In Add Security Policy, select Direct Internet Access.

4. Click Proceed to add an Intrusion Prevention policy in the wizard.

5. In the Add Security Policy wizard, select URL Filtering tab to create a new URL Filtering Policy.




6. Click the Add URL Filtering Policy drop-down, select Create New to create a new policy. A URL Filtering - Policy Rule Configuration wizard appears.




7. Enter the policy name in Policy Name field.

8. Choose one of the following options from the Web Categories drop-down:

- Block—Block websites that match the categories that you select
- Allow—Allow websites that match the categories that you select

9. Select one or more categories to block or allow from the Web Categories list.

10. Select the Web Reputation from the drop-down. The options are:

- High Risk
- Suspicious
- Moderate Risk
- Low Risk
- Trustworthy

11. From the **Advanced** tab, choose one or more existing allowed URL lists or create new ones as needed from the **Whitelist URL List** drop-down.

Items on the allowed-list are not subject to domain filtering. If the same item is configured under both the allowed list and the blocked list, the traffic is allowed.

To create a new URL list, click **New Whitelist URL List** at the bottom of the drop-down. In the Whitelist URL List Name field, enter a list name consisting of up to 32 characters (letters, numbers, hyphens and underscores only). In the Add Whitelist URL field, enter URLs to include in the list, separated with commas. You also can use the Import button to add allowed lists from an accessible storage location. Click Save when you are finished.

12. From the **Advanced** tab, choose one or more existing blocked URL lists or create new ones as needed from the **Blacklist URL List** drop-down.

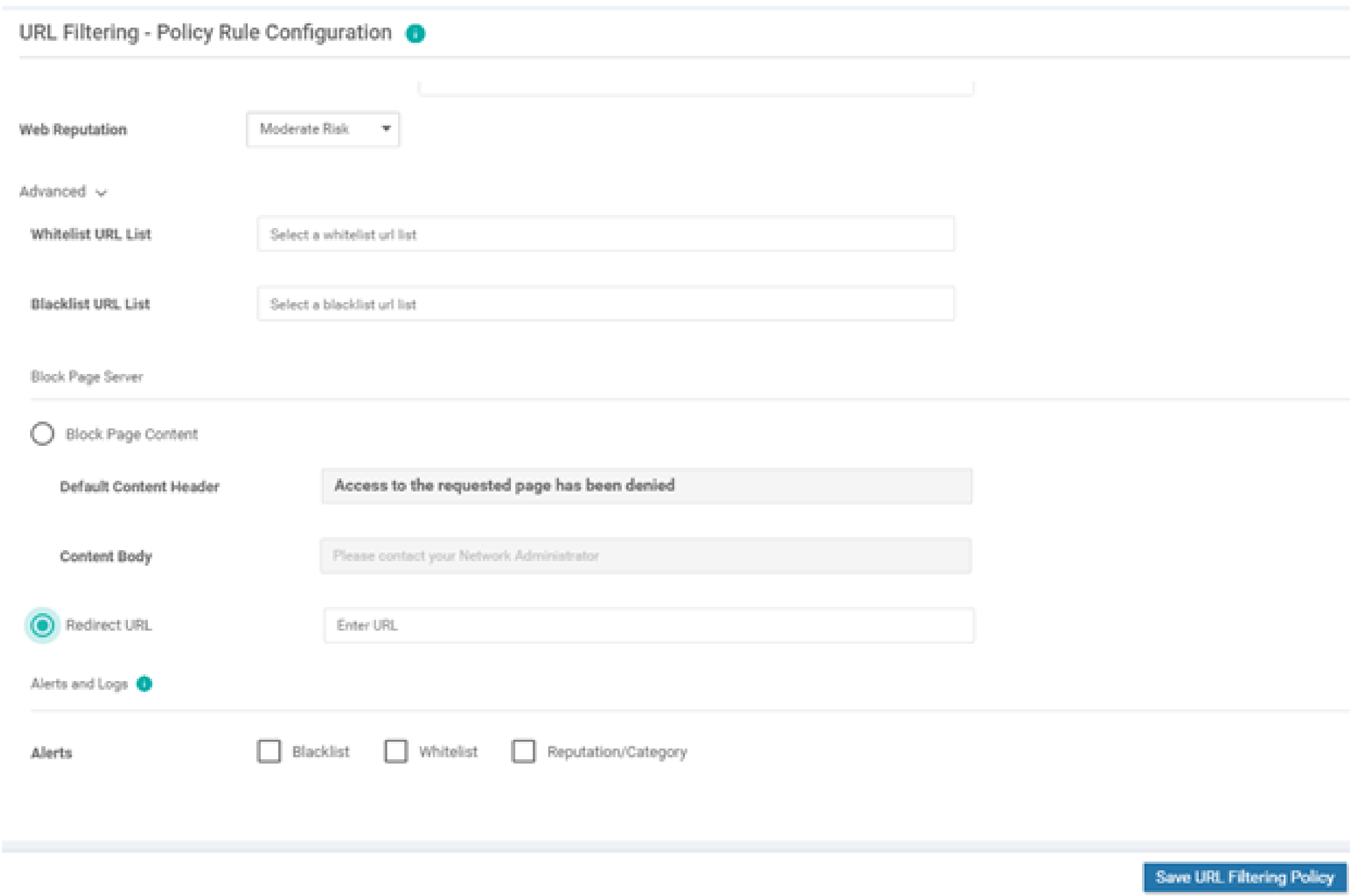
    Items on the blocked list are subject to domain filtering. If the same item is configured under both the allowed list and the blocked list, the traffic is allowed.

    To create a new URL list, click **New Blacklist URL List** at the bottom of the drop-down. In the Blacklist URL List Name field, enter a list name consisting of up to 32 characters (letters, numbers, hyphens and underscores only). In the Add Blacklist URL field, enter URLs to include in the list, separated with commas. You also can use the Import button to add blocked lists from an accessible storage location. Click Save when you are finished.

    You also can create or manage blocked URL lists by selecting the **Configuration ► Security** tab in the left side panel, choosing Lists from the Custom Options drop-down at the top right of the page, and then selecting Blacklist URLs in the left panel.

    To remove a URL list from the Blacklist URL List field, click the “X” next to the list name in the field.

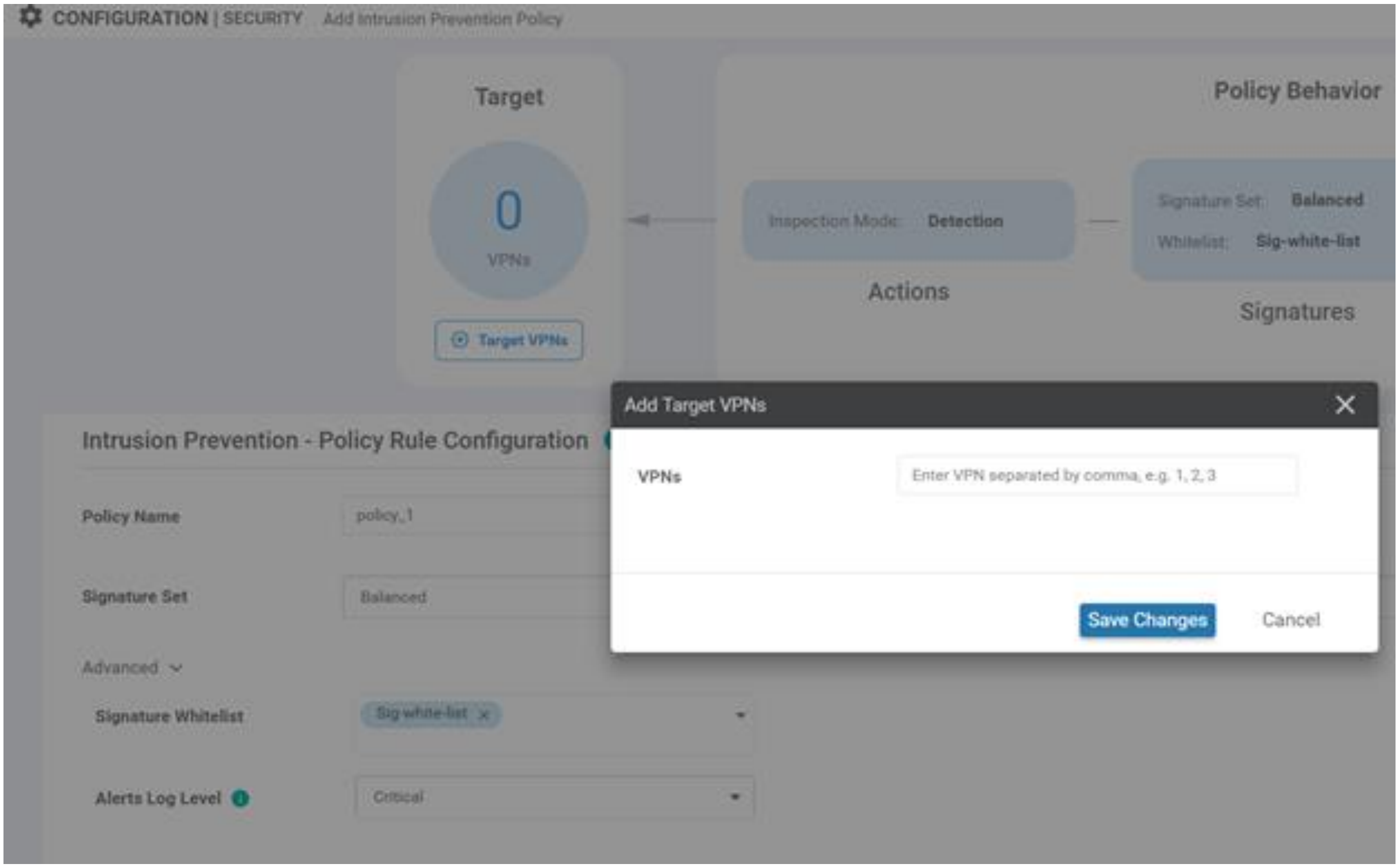
13. In the Block Page Server pane, choose an option to designate what happens when a user visits a URL that is blocked. Choose Block Page Content to display a message that access to the page has been denied, or choose Redirect URL to display another page.




14. In the Alerts and Logs pane, select the alert type from the following options:

- Blacklist—Exports an alert as a Syslog message if a user tries to access a URL that is configure in the Blacklist URL List
- Whitelist—Exports an alert as a Syslog message if a user tries to access a URL that is configure in the Whitelist URL List
- Reputation/Category—Exports an alert as a Syslog message if a user tries to access a URL that has a reputation that is configured in the Web Reputation field or that matches a blocked or allowed web category

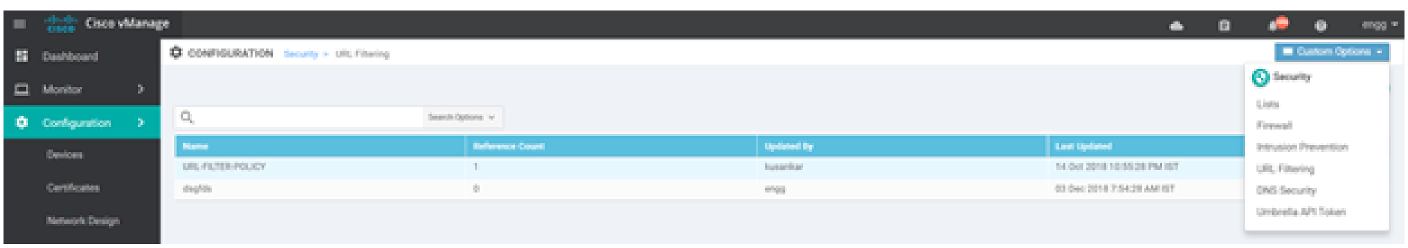
15. Click on Target VPNs to add required number of VPNs in Add Target VPNs wizard.




16. Click Save Changes to add target VPNs.

17. Click Save URL Filtering Policy to configure URL Filtering.

18. You can edit the existing URL Filtering policy by clicking on Custom Options in the right-side panel of vManage ▶ Configuration ▶ Security wizard.




## Monitoring URL Filtering Feature

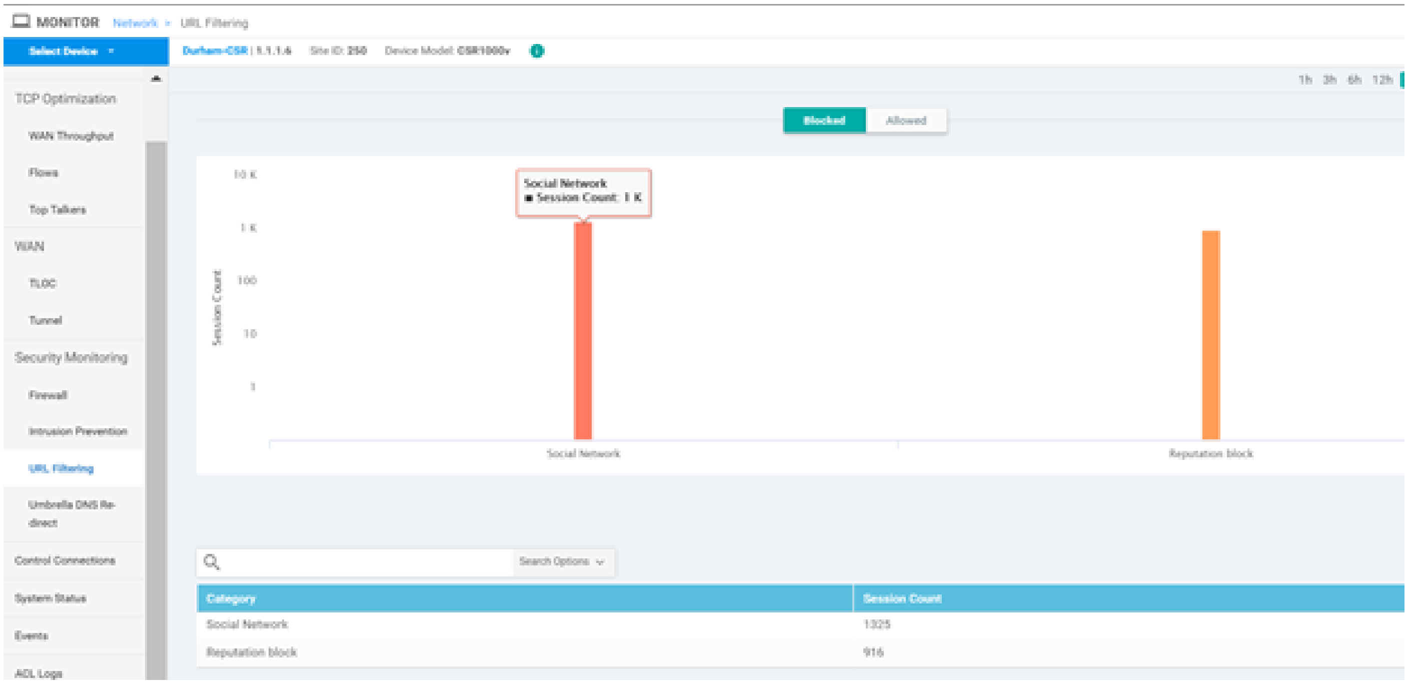
You can monitor the URL Filtering for a device by web categories using the following steps.

To monitor the URLs that are blocked or allowed on an IOS XE SD-WAN device:

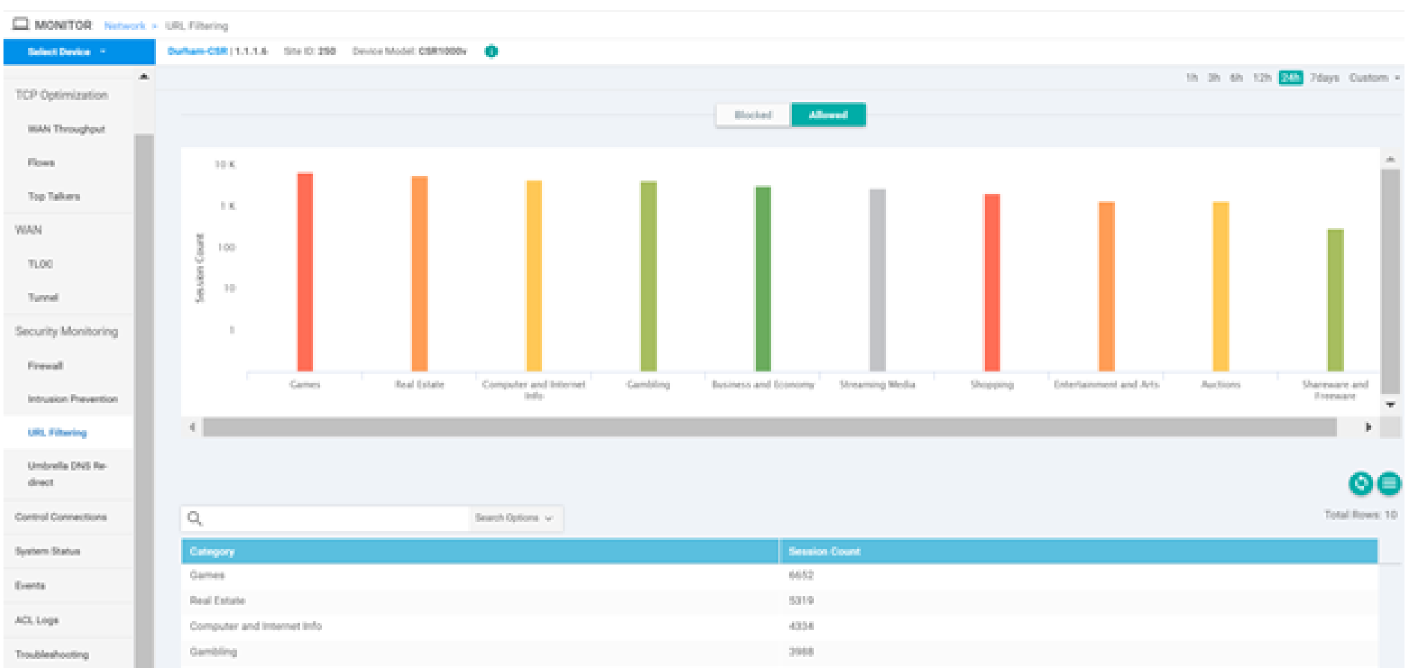
1. From the Monitor ▶ Network screen, select a device.

2. In the left panel, under Security Monitoring, select URL Filtering tab. The URL Filtering wizard displays.

3. Click on Blocked tab, and the session count on a blocked URL appears as shown in the following screenshot.




4. Click on Allowed tab, the session count on allowed URLs appear as shown in the following screenshot.




How to configure URL Filtering on a vManage

# VPN Interface NAT Pool

## Create NAT Pool Interfaces in a VPN

Use the VPN Interface NAT Pool template for all vEdge routers, to create Network Address Translation (NAT) pools of IP addresses in virtual private networks (VPNs).
To configure NAT pool interfaces in a VPN using vManage templates:

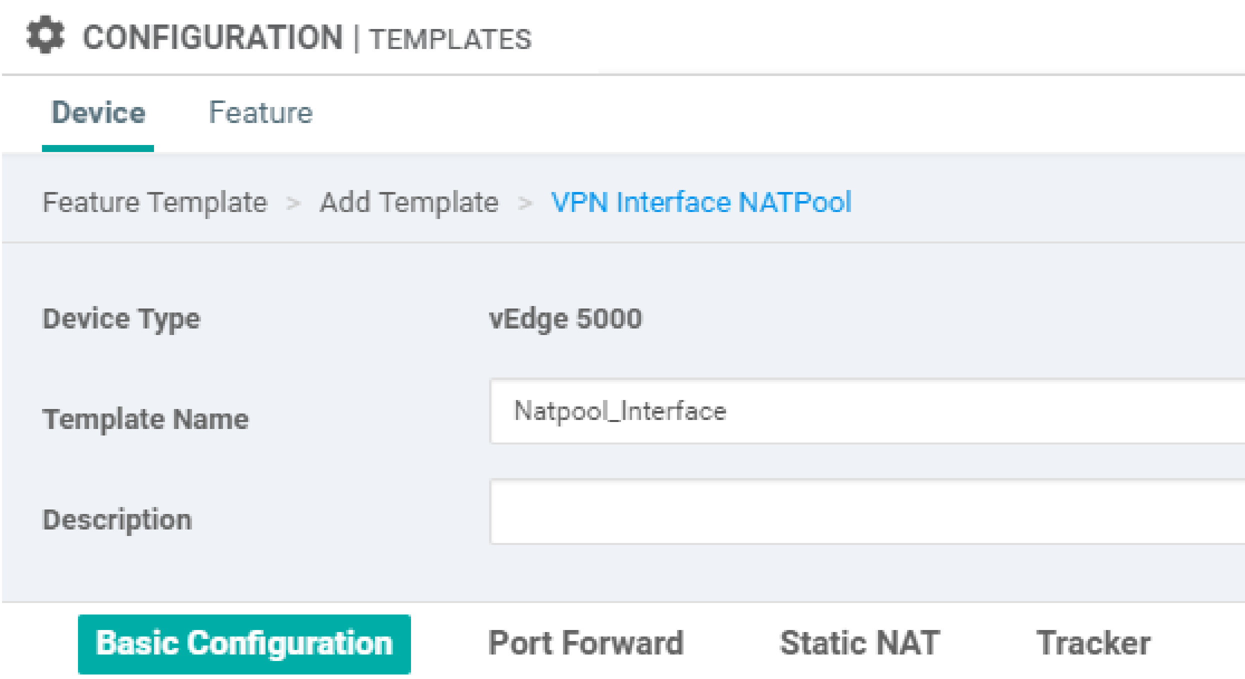
1. Create a VPN Interface NAT Pool template to configure Ethernet interface parameters, as described in this article.
2. Create a VPN feature template to configure parameters for a service-side VPN. See the VPN help topic.
3. Optionally, create a data policy to direct data traffic to a service-side NAT. See Create a Device Template.

## Create and Name a VPN Interface NAT Pool Template

You can open a new VPN Interface NAT Pool template from the Service VPN section of a device template.

1. From the vManage menu, select Configuration > Templates.
2. Click **Feature** .
3. Click **Add Template** .
4. Select a vEdge device from the list.
5. From the VPN section, click **VPN Interface NATPool** .

The VPN Interface NATPool template form displays. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN Interface NAT Pool parameters.




6. In the required 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 optional Template Description field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

## Parameter Menus and Options

Parameter Menus and Options

When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a ), 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:

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

## Configure a NAT Pool Interface

To configure a NAT pool interface, configure the following parameters. Parameters marked with an asterisk are required to configure the interface.

## Basic Configuration

Enter the following basic configuration parameters:

**Parameter Name**

**Values**

**Description**

Shutdown*

Yes

No

Click **No** to enable the interface.

Interface Name (1…31)*

1-31

Enter a number for the NAT pool interface to use for service-side NAT. For example, *natpool22* .

Description

Enter a description for the interface.

IPv4 Address*

Enter the IPv4 address of the interface. The address length determines the number of NAT addresses that the router use at the same time. A vEdge router can support a maximum of 250 NAT IP addresses.

Refresh Mode

Select how NAT mappings are refreshed:

bi-directional

Keep active the NAT mappings for inbound and outbound traffic.

outbound

Keep active the NAT mappings for outbound traffic. This is the default.

UDP Timeout

1-65536 minutes

Enter the time when NAT translations over UDP sessions time out.
*Default:* 1 minute

TCP Timeout

1-65536 minutes

Enter the time when NAT translations over TCP sessions time out.
*Default:* 60 minutes (1 hour)

Block ICMP

On

Off

Select whether a vEdge router that is acting as a NAT device should receive inbound ICMP error messages. By default, the router blocks these error messages. Click **Off** to receive the ICMP error messages.

Direction

Select the direction in which the NAT interface performs address translation:

inside

Translate the source IP address of packets that are coming from the service side of the vEdge router and that are destined to transport side of the router. This is the default.

outside

Translate the source IP address of packets that are coming to the vEdge router from the transport side of the vEdge router and that are destined to a service-side device.

Overload

Yes

No

Click **No** to disable dynamic NAT. By default, dynamic NAT is enabled.

## Tracker

1. To create one or more tracker interfaces, select the Tracker tab and click New Tracker.
2. Select one or more interfaces to track the status of service interfaces.
3. To save the tracker interfaces, click Add. To save the feature template, click Save.

## CLI Equivalent Commands

Use the following commands to configure NAT Pool interfaces.

```
vpn vpn-id
  interface natpoolnumber
    ip address prefix/length
    nat
      tracker tracker-name1 tracker-name2, tracker-name3
      direction (inside | outside)
      [no] overload
      refresh (bi-directional | outbound)
      static source-ip ip-address1 translate-ip ip-address2 (inside | outside)
      tcp-timeout minutes
      udp-timeout minutes
    [no] shutdown
```

# Configure Port-Forwarding Rules

To create port-forwarding rules to allow requests from an external network to reach devices on the internal network:

1. Select the Port Forward tab.
2. Click **New Port Forwarding Rule** , and configure the following parameters. You can create up to 128 rules.

**Parameter Name**

**Values**

**Description**

Port Start Range

Enter the starting port number. This number must be less than or equal to the ending port number.

Port End Range

Enter the ending port number. To apply port forwarding to a single port, specify the same port number for the starting and ending numbers. When applying port forwarding to a range of ports, the range includes the two port numbers that you specify.

Protocol

TCP

UDP

Select the protocol to apply the port-forwarding rule to. To match the same ports for both TCP and UDP traffic, configure two rules.

VPN

0-65535

Private VPN in which the internal server resides.

Private IP

Enter an IP address to use within the firewall. A best practice is to specify the IP address of a service-side VPN.

3. To save the rule, click **Add** .

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

## CLI Equivalent Commands

```
vpn vpn-id
  interface natpoolnumber
    nat
      port-forward port-start port-number1 port-end port-number2 proto (tcp | udp)
        private-ip-address ip address private-vpn vpn-id
```

# Configure Static NAT

To configure a static NAT of service-side source IP addresses:

1. Select the Static NAT tab. Then click **New Static NAT** and configure the following parameters to add a static NAT mapping:

**Parameter Name**

**Values**

**Description**

Mark as Optional Row

Check **Mark as Optional Row** to mark this configuration as device-specific. To include this configuration for a device, enter the requested variable values when you attach a device template to a device, or create a template variables spreadsheet to apply the variables. See Create a Template Variables Spreadsheet .

Source IP

Enter the NAT private source IP address.

Translate IP

To map a public IP address to a private source address, enter the public IP address.

Static NAT Direction

Select the direction in which to perform network address translation.

inside

Translate the IP address of packets that are coming from the service side of the vEdge router and that are destined for the transport side of the router.

outside

Translate the IP address of packets that are coming to the vEdge router from the transport side of the vEdge router and that are destined for a service-side device.

2. To save the NAT mapping, click **Add** .

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

### CLI Equivalent Commands

```
vpn vpn-id
  interface natpoolnumber
    nat
      port-forward port-start port-number1 port-end port-number2 proto (tcp | udp)
        private-ip-address ip address private-vpn vpn-id
```

## Release Information

Introduced in vManage NMS Release 16.3.
In Release 17.2.2, add support for tracker interface status.
In Release 18.4, updated images; add support for multiple tracker interfaces.

## Enterprise Firewall with Application Awareness

Cisco's Enterprise Firewall with Application Awareness uses a flexible and easily understood zone-based model for traffic inspection, compared to the older interface-based model.

A firewall policy is a type of localized security policy that allows stateful inspection of TCP, UDP, and ICMP data traffic flows. Traffic flows that originate in a given zone are allowed to proceed to another zone based on the policy between the two zones. A zone is a grouping of one or more VPNs. Grouping VPNs into zones allows you to establish security boundaries in your overlay network so that you can control all data traffic that passes between zones.

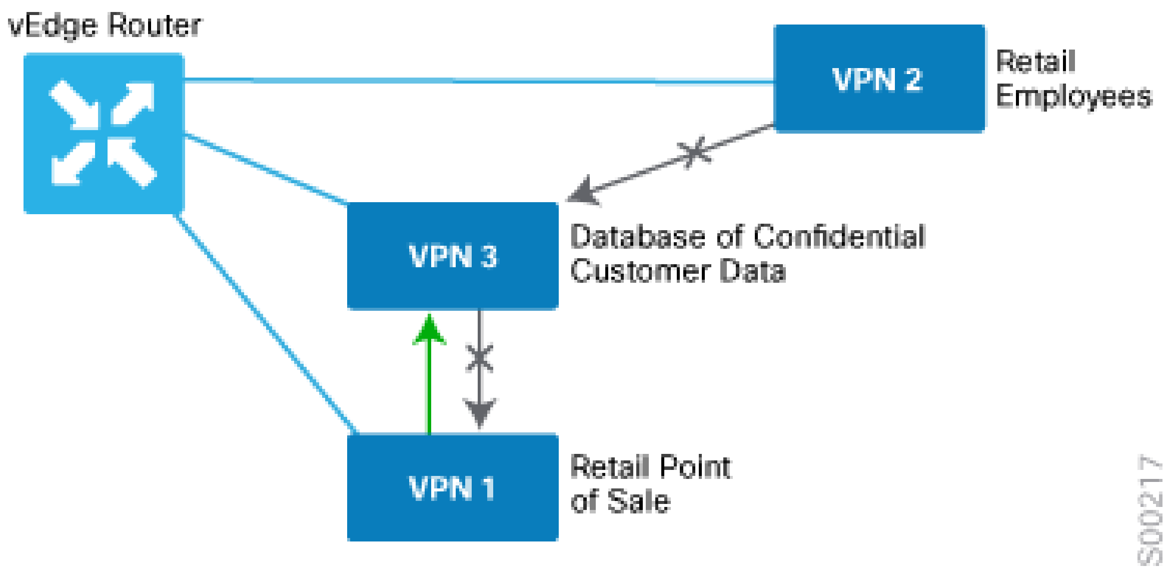
Zone configuration consists of the following components:

- Source zone—A grouping of VPNs where the data traffic flows originate. A VPN can be part of only one zone.
- Destination zone—A grouping of VPNs where the data traffic flows terminate. A VPN can be part of only one zone.
- Firewall policy—A security policy, similar to a localized security policy, that defines the conditions that the data traffic flow from the source zone must match to allow the flow to continue to the destination zone. Firewall policies can match IP prefixes, IP ports, the protocols TCP, UDP, and ICMP, and applications. Matching flows for prefixes, ports, and protocols can be accepted or dropped, and the packet headers can be logged. Nonmatching flows are dropped by default. Matching applications are denied.
- Zone pair—A container that associates a source zone with a destination zone and that applies a firewall policy to the traffic that flows between the two zones.

Matching flows that are accepted can be processed in two different ways:

- Inspect—The packet's header can be inspected to determine its source address and port.
- Pass—Allow the packet to pass to the destination zone without inspecting the packet's header at all.

The following figure shows a simple scenario in which three VPNs are configured on a XE SD-WAN Router. One of the VPNs, VPN 3, has shared resources that you want to restrict access to. These resources could be printers or confidential customer data. For the remaining two VPNs in this scenario, only users in one of them, VPN 1, are allowed to access the resources in VPN 3, while users in VPN 2 are denied access to these resources. In this scenario, we want data traffic to flow from VPN 1 to VPN 3, but we do not want traffic to flow in the other direction, from VPN 3 to VPN 1.




Firewall policies perform stateful inspection of TCP, UDP, and ICMP flows between zones. They examine the source and destination IP addresses and ports in the packet headers, as well as the packet's protocol. Then, based on the configured zone-based policy, they allow traffic to pass between the zones or they drop the traffic.

The implementation of firewall policies varies slightly to that of localized security policy. Where you configure and apply localized security policy based only on VPNs, you configure and apply firewall policies to one or more VPNs that have been grouped into a zone. You activate localized security policy by applying it to individual interfaces on the XE SD-WAN Routers. When you activate firewall policies, they apply to the specific VPNs in the zones, without regard to any specific interfaces.

## Application Firewall

The Application Firewall inspects and blocks traffic based on applications or application-family. This application-aware firewall feature provides the following benefits:

- Application visibility and granular control
- Classification of 1400+ layer 7 applications
- Blocks traffic by application or application-family

You can create lists of individual applications or application families. A sequence that contains a specified application or application family list can be inspected. This inspect action is a Layer 4 action. Matching applications are blocked/denied.

vEdge Router provides Application Layer Gateway (ALG) FTP support with Network Address Translation – Direct Internet Access (NAT-DIA), Service NAT, and Enterprise Firewall. Service NAT support is added for FTP ALG on the client and not on the FTP Server.

## Additional Information

Configuring Firewall Policies
Configuring Localized Data Policy

Firewall policies are a type of localized security policy that allows stateful inspection of TCP, UDP, and ICMP data traffic flows.

## Configuring Firewall Policies

This article provides procedures for configuring firewall policies on XE SD-WAN Routers. You provision firewall policies to direct traffic between two zones, which are referred to as a source zone and a destination zone. Each zone consists of one or more VPNs in the overlay network.

In vManage NMS, you configure firewall policies from the Configuration ► Security screen, using a policy configuration wizard. In the CLI, you configure these firewalls on the XE SD-WAN Router.

## Configuration Components

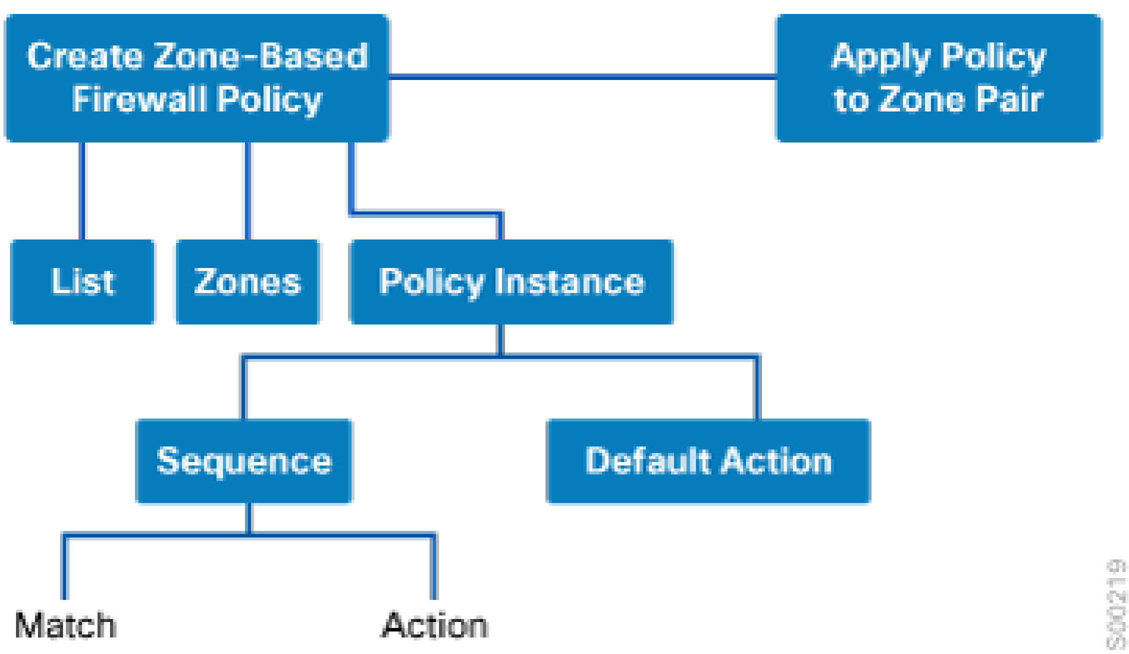
For firewall policies, you configure zones and a policy to apply to those zones.

Each zone consists of one of more VPNs in the overlay network. You define a source zone, which identifies the VPNs from which data traffic originates, and a destination zone, which identifies the VPNs to which the traffic is being sent.

The firewall policy consists of a series of numbered (ordered) sequences of match–action pairs that are evaluated in order, from lowest sequence number to highest sequence number. When a data packet matches the match conditions, the associated action or actions are taken and policy evaluation on that packet stops. Keep this process in mind as you design your policies to ensure that the desired actions are taken on the items subject to policy.

If a packet matches no parameters in any of the policy sequences, you define a default action to be taken on the packet.

The following figure illustrates the configuration components for firewall policies:




To create a firewall policy, you include the following components in the configuration for a XE SD-WAN Router:

| Component | Description | vManage Configuration | CLI Configuration Command |
|---|---|---|---|

| | | | |
|---|---|---|---|
| Lists | Groupings of related items that you reference in the match portion of the zone-based firewall configuration. | Configuration ▶ Security ▶ Custom Options ▶ Lists ▶ Data Prefix<br><br>Configuration ▶ Security ▶ Custom Options ▶ Lists ▶ Zones | **policy lists**<br><br>**policy zone** |
| Firewall policy | Container for a firewall policy. | Configuration ▶ Security ▶ Add Security Policy ▶ < *Scenario* > ▶ Add Firewall Policy | **policy zone-based-policy** |
| Numbered sequences of match–action pairs | Sequences establish the order in which the policy components are applied. | Configuration ▶ Security ▶ Add Security Policy ▶ < *Scenario* > ▶ Add Firewall Policy ▶ Sequence Rule | **policy zone-based-policy sequence** |
| L3/4 Match parameters | Conditions that packets must match to be considered for a data policy. | Configuration ▶ Security ▶ Add Security Policy ▶ < *Scenario* > ▶ Add Firewall Policy ▶ Sequence Rule ▶ Match | **policy zone-based-policy sequence match** |
| Actions | Whether to accept or reject matching packets, and how to process matching items. | Configuration ▶ Security ▶ Add Security Policy ▶ < *Scenario* > ▶ Add Firewall Policy ▶ Sequence Rule ▶ Action | **policy zone-based-policy sequence action** |
| Default action | Action to take if a packet matches none of the match parameters in any of the sequences. By default, nonmatching packets are dropped. | Configuration ▶ Security ▶ Add Security Policy ▶ < *Scenario* > ▶ Add Firewall Policy | **policy zone-based-policy default-action** |
| Apply firewall policy to a zone pair | For a firewall policy to take effect, you include it in the definition of a zone pair. | Configuration ▶ Security ▶ Add Security Policy ▶ < *Scenario* > ▶ Apply Policy | **policy zone-pair** |

To create an application firewall policy, you include the following components in the configuration for a XE SD-WAN Router:

| Component | Description | vManage Configuration | CLI Configuration Command |
|---|---|---|---|
| Lists | Groupings of related items that you reference in the match portion of the firewall policy configuration. | Configuration ▶ Security ▶ Custom Options ▶ Lists ▶ Application<br><br>Configuration ▶ Security ▶ Custom Options ▶ Lists ▶ Zones | **policy lists** |
| Firewall policy | Container for a firewall policy. | Configuration ▶ Security ▶ Add Security Policy ▶ < *Scenario* > ▶ Add Firewall Policy | **policy zone-based-policy** |
| Numbered sequences of match–action pairs | Sequences establish the order in which the policy components are applied. | Configuration ▶ Security ▶ Add Security Policy ▶ < *Scenario* > ▶ Add Firewall Policy ▶ Sequence Rule | **policy zone-based-policy sequence** |
| Application Match parameters | Conditions that packets must match to be considered for a security policy. | Configuration ▶ Security ▶ Add Security Policy ▶ <*Scenario*> ▶ Add Firewall Policy ▶ Sequence Rule ▶ Match ▶ Application/Application Family List | **policy zone-based-policy sequence match app-list** |
| Actions | For a sequence that contains an application or application family list, packets can be inspected. Matching applications are blocked/denied. | Configuration ▶ Security ▶ Add Security Policy ▶ <*Scenario*> ▶ Add Firewall Policy ▶ Sequence Rule ▶ Actions ▶ Inspect | **policy zone-based-policy sequence action inspect** |

| | | | |
|---|---|---|---|
| Default action | Action to take if a packet matches none of the match parameters in any of the sequences. By default, nonmatching packets are dropped. | Configuration ▶ Security ▶ Add Security Policy ▶< *Scenario* > ▶ Add Firewall Policy ▶ Sequence Rule ▶ Actions | **policy zone-based-policy default-action drop** |
| Apply firewall policy to a zone pair | For a firewall policy to take effect, you include it in the definition of a zone pair. | Configuration ▶ Security ▶ Add Security Policy ▶< *Scenario* > ▶Apply Policy | **policy zone-pair** |

## General vManage Configuration Procedure

To configure firewall policies, use the vManage policy configuration wizard. The wizard is a UI policy builder that lets you configure policy components:

- Create Lists—Create lists that group together related items and that you call in the match condition of a firewall policy.
- Firewall Policy—Define the match and action conditions of the firewall policy.
- Apply Configuration—Define zone pairs.

You must configure all these components to create a firewall policy. If you are modifying an existing firewall, you can skip a component by clicking the Next button at the bottom of the screen. To return to a component, click the Back button at the bottom of the screen.

### Step 1: Create Lists

To create lists:

1. In vManage NMS, select the Configure ▶ Security screen.
2. In the Title bar, click the Custom Options drop-down.
3. Select Lists. The Define Lists screen displays.
4. Select the list type to create. The following table describes the lists you can create for firewall policies.

List Type

Procedure

Application

1. In the left pane, click Application.
2. Click New Application List.
3. Enter a name for the list.
4. Select individual applications or application families.
5. Click Add.

Data Prefix

1. In the left pane, click Data Prefix.
2. Click New Data Prefix List.
3. Enter a name for the list.

4. Enter one or more IP prefixes.
5. Click Add.

Zones

1. In the left pane, click Zones.
2. Click New Zone List.
3. Enter a name for the zone list.
4. In the Add VPN field, enter the number or numbers of the VPN in the zone. Separate numbers with commas.
5. Click Add.
4. To edit, copy, or delete an existing list, click the Edit, Copy, or Trash Bin icon in the Action column.

## Step 2: Start the Policy Configuration Wizard

To start the policy configuration wizard:

1. In vManage NMS, select the Configure ► Security screen.
2. Click Add Security Policy.

The Add Security Policy configuration wizard opens, and various use-case scenarios display.

## Step 3: Select a Use-Case Scenario

In Add Security Policy, select a policy based on use-case scenarios, or build your own custom policy.

1. Select a security policy use-case scenario. The following table describes the use-case scenarios.

- Compliance – Applies application firewall and intrusion prevention.
- Guest Access – Applies application firewall and URL filtering.
- Direct Cloud Access – Applies application firewall, URL filtering, and DNS Umbrella security.
- Direct Internet Access – Applies application firewall, intrusion prevention, URL filtering, and DNS Umbrella security.
- Custom – Build your own security policy by combining various security policy blocks.

2. Click Proceed to add a firewall policy in the wizard.

## Step 4: Configure Firewall Policy

1. Click the Add Firewall Policy drop-down.
2. To create a new firewall policy:
    a. Select Create New.
    b. Enter a name and description for the policy.
    c. Go to Step 4.

3. To import an existing zone-based firewall policy:

    a. Select Copy from Existing. The Copy from Existing Firewall Policy dialog box appears.

    b. From the Policy drop-down, select the policy to copy.

    c. In the Policy Name field, accept the default name ( *policy_name* _copy) or enter a new name.

    d. In the Policy Description field, enter a description.

    e. Click Copy.

    f. To modify the policy, click the More Actions icon to at the far right of the policy and select Edit. Go to Step 4.

Otherwise, click Next to move to the next security block in the configuration wizard.

4. In the left pane, click Sequence Rule to create a single sequence in the firewall policy. The Match tab is selected by default.

5. Click a match condition:

- Source Data Prefix
- Source Port
- Destination Data Prefix
- Destination Port
- Protocol
- Application/Application Family List

You can select and configure more than one match condition in a sequence.

6. Enter the values for the match condition.

**Note** : If you selected an Application or Application Family List, you must select at least one other match condition.

7. Click the Actions tab.

8. Enter the action or actions to take if the traffic matches.

**Note** : If a match condition contains an Application or Application Family List, the action must be Inspect. This inspect action is a Layer 4 action. The action for a specific application is block/deny.

9. Click Save Match and Actions to save match-action pair.

10. Repeat Steps 4 through 9 to add match–action pairs to the firewall policy.

11. To rearrange match–action pairs in the policy, drag them to the desired position.

12. To edit, copy, or delete a sequence rule, in the right pane, click the edit, copy, or delete icon to the right of the sequence rule.

13. If no packets match any of the policy sequence rules, the default action is to drop the packets. To change the default action:

    a. Click the Pencil icon.

    b. Change the default action to Inspect or Pass.

    c. Click Save Match and Actions.

## Step 5: Apply Policy to a Zone Pair

1. At the top of the page, click Apply Zone-Pairs.

2. In the Source Zone field, select the zone that is the source of the data packets.

3. In the Destination Zone field, select the zone that is the destination of the data packets.

   You can select the same zone for both source and destination. However, if the packet's source and destination use the same physical interface (resulting in U-turn traffic), a firewall session is not created and traffic passes.

4. Click the plus (+) icon to add zone pairs.

5. Click Save.

6. At the bottom of the page, click Save Firewall Policy to save the policy.

7. To edit or delete a firewall policy, in the right pane, click the More Actions icon to the far right of the policy and select the desired option.

8. Click Next to configure the next security block in the wizard.

- **Intrusion Prevention**
- **URL Filtering**
- **DNS Security**

## Policy Summary

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

2. Enter a description for the security policy. This field is mandatory.

3. If you configured an application firewall policy, uncheck the “Bypass firewall policy and allow all Internet traffic to/from VPN 0” checkbox in the Additional Security Policy Settings area.

4. Click Save Policy to save the security policy.

## Apply a Security Policy to an XE SD-WAN Router

1. In vManage NMS, select the Configuration ► Templates screen.

2. If you are creating a new device template:

   a. In the Device tab, click Create Template.

   b. From the Create Template drop-down, select From Feature Template.

   c. From the Device Model drop-down, select one of the XE SD-WAN Router.

   d. In the Template Name field, enter a name for the device template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores (_). It cannot contain spaces or any other characters.

   e. In the Description field, enter a description for the device template. This field is mandatory, and it can contain any characters and spaces.

   f. Continue with Step 4.

3. If you are editing an existing device template:
    a. In the Device tab, click the More Actions icon to the right of the desired template, and click the pencil icon.
    b. Click the Additional Templates tab. The screen scrolls to the Additional Templates section.
    c. From the Policy drop-down, select the name of a policy that you have configured.
4. Click the Additional Templates tab located directly beneath the Description field. The screen scrolls to the Additional Templates section.
5. From the Security Policy drop-down, select the name of the security policy you configured in the above procedure.
6. Click Create (for a new template) or Update (for an existing template).

## Additional Information

[Enterprise Firewall with Application Awareness]
[Configuring Unified Threat Defense]

## Configuring Unified Threat Defense

This article provides procedures for configuring Unified Threat Defense (UTD) security mechanisms on IOS XE routers. You can configure the following UTD security mechanisms:

- Intrusion prevention and detection (IPS/IDS)
- Umbrella DNS security
- URL filtering

You provision zone-based firewall policies to define the data traffic that is subject to the UTD security mechanisms.

In vManage NMS, you configure UTD from the Configuration ► Security screen, using a policy configuration wizard.

## Configuration Components

UTD security policy components consist of the following:

- Zone-based firewall—Allows you to filter data packets, to match allows data traffic and drop unwanted traffic. You must configure one or more zone-based firewalls for any type of security policy. Zone configuration consists of the following components:
    - Source zone—A grouping of VPNs where the data traffic flows originate. A VPN can be part of only one zone.
    - Destination zone—A grouping of VPNs where the data traffic flows terminate. A VPN can be part of only one zone.
    - Zone pair—A container that associates a source zone with a destination zone and that applies a zone-based firewall policy to the traffic that flows between the two zones.
    - Zone-based firewall policy—A data policy, similar to a localized data policy, that defines the conditions that the data traffic flow from the source zone must match to allow the flow to continue to the destination zone. Zone-based firewalls can match IP prefixes, IP ports, and the protocols TCP, UDP, and ICMP. Matching flows can be accepted or dropped, and the packet headers can be logged. Nonmatching flows are dropped by default.
    - Zone pair—A container that associates a source zone with a destination zone and that applies a zone-based firewall policy to the traffic that flows between the two zones.
- Intrusion prevention policy—Protects against malicious attacks on data traffic by using signature sets and inspection mode. Intrusion detection passes all packets flowing between service-side and transport-side (WAN or internet) interfaces, and between VLANs, through

an intrusion detection engine, generating alerts for traffic that is identified as malicious, and logging these alerts via syslog. Intrusion prevention blocks traffic that is identified as malicious.

- URL filtering policy—Allows and disallows access to specific URLs and webpage categories. URL filtering allows you to control access to Internet websites by permitting or denying access to specific websites based on allowed lists, blocked lists, categories, and reputations. For example, when a client sends a HTTP or HTTPS request, the router inspects the traffic. If, for example, the request matches the blocked list, either it is blocked by a blocked page response or it is redirected to a different URL. If, for example, the HTTP or HTTPS request matches the allowed list, the traffic is allowed without further URL filtering inspection.
- DNS security policy—Directs traffic from your network to the cloud-based Cisco Umbrella secure internet gateway. Umbrella using DNS to stop threads over all ports and protocols and over direct-to-IP connections.

## Configure Compliance Security

A compliance security policy implements both intrusion prevention and intrusion detection. Intrusion prevention policy protects against malicious attacks on data traffic by using signature sets and inspection mode. Intrusion detection passes all packets flowing between service-side and transport-side (WAN or internet) interfaces, and between VLANs, through an intrusion detection engine, generating alerts for traffic that is identified as malicious, and logging these alerts via syslog. Intrusion prevention blocks traffic that is identified as malicious.

To configure intrusion prevention and detection, you use the Compliance policy option of the security policy configuration wizard.

### Step 1: Start the Security Policy Wizard

To start the security policy configuration wizard:

1. In vManage NMS, select the Configure ► Security screen.
2. Click Add Policy.
3. From the Add Security Policy popup, select Compliance Policy.
4. Click Proceed.

The security policy configuration wizard opens, and the Firewall screen displays.

### Step 2: Configure Application Firewall Policy

To create a new application firewall policy:

1. In the Firewall screen, click the Add Firewall Policy drop-down.
2. Select Create New. The Add Firewall Policy screen displays.
3. In the Name field, enter a name for the firewall policy. The name can be up to 128 characters and can contain only alphanumeric characters.
4. In the Description field, enter a description of the firewall policy. The description can be up to 2048 characters and can contain only alphanumeric characters.
5. Create a zone pair or apply an existing zone pair to the firewall policy:
    a. Click Apply Zone Pairs. The Apply Zone Pairs popup displays.
    b. In Source Zone, select an existing zone. Or to create a new zone, click Create New Zone List. Then enter a name for the list and the VPNs in the zone, and click Save.

c. In Destination Zone, select an existing zone. Or to create a new zone, click Create New Zone List. Then enter a name for the list and the VPNs in the zone, and click Save.

6. Create one or more security policy sequence rules to apply to the traffic that flows from the source zones to the destination zones:

    a. Click Add Sequence Rule.

    b. Click Match to add a match condition. You can match the following:
    - Application/Application Family List
    - Destination Data Prefix
    - Destination Port
    - Protocol
    - Source Data Prefix
    - Source Port

    c. Click Actions to define the actions to take when a match occurs. By default, the packet is dropped. You can take these other actions:
    - Inspect: Inspect the packet's header to determine its source address and port. The address and port are used by the NAT device to allow traffic to be returned from the destination to the sender.
    - Log: Log the packet headers.
    - Pass: Allow the packet to pass to the destination zone without inspecting the packet's header at all. With this action, the NAT device blocks return traffic that is addressed to the sender.

    d. Click Save Match and Actions.

    e. Add additional sequence rules as needed.

    f. Drag and drop the rules to arrange them in the desired sequence. Rules are applied to data packets in the order in which that are defined in the policy.

7. Click Save Firewall Policy.

8. Click Next.

To copy an existing firewall policy into the compliance security policy:

1. In the Firewall screen, click the Add Firewall Policy drop-down.

2. Select Copy from Existing.

3. In the Copy from Existing Firewall popup:

    a. In the Policy field, select a policy.

    b. In the Policy Name field, select a policy name.

    c. In the Policy Description field, enter a description of the firewall policy. The description can be up to 2048 characters and can contain only alphanumeric characters.

    d. Click Copy. The copied policy is listed in the Security Policy Firewall table.

4. Click Next. Depending on the security policy type you are configuring, one of the following screens displays:

- Intrusion prevention policy
- Umbrella DNS policy
- URL-filtering policy

## Step 3: Configure Intrusion Prevention and Detection

To create a new intrusion prevention and detection policy:

1. In the Intrusion Prevention screen, click the Add Intrusion Prevention Policy drop-down.
2. Click Create New. The Add Intrusion Prevention Policy screen displays.
3. In the Policy Name field, enter a name for the firewall policy. The name can be up to 32 characters and can contain only alphanumeric characters.
4. In the Signature Set field, select the desired signature set:

- Balanced (default)—Contains rules that are from the current year and the previous two years, are for vulnerabilities with a Common Vulnerability Scoring System (CVSS) score of 9 or greater, and are in one of the following categories:
  - Blacklist—Rules for URIs, user agents, DNS hostnames, and IP addresses that have been determined to be indicators of malicious activity.
  - Exploit-kit—Rules that are designed to detect exploit kit activity.
  - Malware-CNC—Rules for known malicious command and control activity for identified botnet traffic. These include call home, downloading of dropped files, and ex-filtration of data.
  - SQL Injection—Rules that are designed to detect SQL Injection attempts.
- Connectivity—Contains rules from the current year and the previous two years for vulnerabilities with a CVSS score of 10.
- Security—Contains rules that are from the current year and the previous three years, are for vulnerabilities with a CVSS score of 8 or greater, and are in one of the following categories:
  - App-detect—Rules that look for and control the traffic of certain applications that generate network activity.
  - Blacklist—Rules for URIs, user agents, DNS hostnames, and IP addresses that have been determined to be indicators of malicious activity.
  - Exploit-kit—Rules that are designed to detect exploit kit activity.
  - Malware-CNC—Rules for known malicious command and control activity for identified botnet traffic. These include call home, downloading of dropped files, and ex-filtration of data.
  - SQL Injection—Rules that are designed to detect SQL Injection attempts.

5. In the Inspection Mode field, select the desired inspection mode:

- Detection—In intrusion detection mode, traffic is accepted or blocked based on the rules defined by the signature set that you choose.
- Protection—In intrusion prevention mode, malicious traffic is automatically blocked, based on the intrusion prevention policy rules.

6. In the Advanced ► Signature Whitelist field, select the desired signature list.
7. In the Advanced ► Alerts Log Level field, select the desired log level for alerts. The level can be Emergency, Alert, Critical, Error, Warning, Notice, Info, and Debug. The default is Error.
8. Configure the VPNs to which to apply the intrusion prevention policy:
   a. In the Target field, click Add Target VPNs.
   b. Enter the VPN numbers to which to apply the intrusion prevention policy. To specify multiple VPNs, separate the numbers with commas.
   c. Click Save Changes.
9. Click Save Intrusion Prevention Policy. The intrusion prevention policy is then listed in the policy table.

10. Click Next. The Policy Summary screen displays.

To copy an existing intrusion prevention policy into the compliance security policy:

1. In the Intrusion Prevention screen, click the Add Intrusion Prevention Policy drop-down.
2. Select Copy from Existing.
3. In the Copy from Existing Intrusion Prevention Policy popup:
    a. In the Policy field, select a policy.
    b. In the Policy Name field, select a policy name.
    c. In the Policy Description field, enter a description of the firewall policy. The description can be up to 2048 characters and can contain only alphanumeric characters.
    d. Click Copy. The copied policy is listed in the Security Policy Firewall table.
4. Click Next. The Policy Summary screen displays.

## Step 4: Configure Additional Policy Settings

In the Policy Summary screen:

1. In the Security Policy Name field, enter the name of the security policy. The name can be up to 32 characters and can contain only alphanumeric characters, hyphens (-), and underscores (_).
2. In the Security Policy Description field,
3. In the Description field, enter a description of the security policy. The description can be up to 2048 characters and can contain only alphanumeric characters.
4. If you do not include VPN 0 in any of the zones that you configure in a zone-based firewall, by default, packets are able to reach destination zones that are accessible only over the public internet. To disallow this traffic, uncheck the Firewall ► Direct Internet Applications box.
5. To configure the number of TCP SYN packets that the router can receive while establishing a TCP connection to use for a zone-based firewall before the router shuts down the connection, move the Firewall ► TCP SYN Flood Limit slider to Enabled. Then enter a limit value from 1 through 2147483647 packets. The default limit is 2000 SYN packets.
6. By default, system logging (syslog) in enabled for intrusion detection. To disable syslog messages, move the Intrusion Prevention and/or URL Filtering ► Syslog slider to Disabled.
7. In the Intrusion Prevention and/or URL Filtering ► External Server field, configure an external syslog server. In the VPN field, specify the VPN through which the server can be reached. In the Server IP field, specify the IP address of the syslog server.
8. In the Intrusion Prevention and/or URL Filtering ► Failure Mode field, configure how the router handles traffic when the URL database update from the cloud fails. When you configure category-based or reputation-based URL filtering, as described above, a URL database is downloaded from the cloud. Incremental updates are automatically downloaded every 15 minutes. If connectivity to the cloud is lost for more than 24 hours, the database is invalidated. For the Failure Mode field, the default is Close, which drops all traffic destined for URL filtering when cloud connectivity is lost. To not drop traffic destined for URL filter, select Open.
9. To view the CLI commands that correspond to the compliance security policy configuration, click Preview.
10. Click Save Policy. The policy is listed in the table on the Configuration ► Policy screen.

### Step 5: Apply the Security Policy to an IOS XE Router

1. In vManage NMS, select the Configuration ► Templates screen.
2. If you are creating a new device template:
   a. In the Device tab, click Create Template.
   b. From the Create Template drop-down, select From Feature Template.
   c. From the Device Model drop-down, select one of the vEdge devices.
   d. In the Template Name field, enter a name for the device template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores (_). It cannot contain spaces or any other characters.
   e. In the Description field, enter a description for the device template. This field is mandatory, and it can contain any characters and spaces.
   f. Continue with Step 4.
3. If you are editing an existing device template:
   a. In the Device tab, click the More Actions icon to the right of the desired template, and click the pencil icon.
   b. Click the Additional Templates tab. The screen scrolls to the Additional Templates section.
   c. From the Policy drop-down, select the name of a policy that you have configured.
4. Click the Additional Templates tab located directly beneath the Description field. The screen scrolls to the Additional Templates section.
5. From the Security Policy drop-down, select the name of the zone-based firewall you configured in the above procedure.
6. Click Create (for a new template) or Update (for an existing template).

## Configure Guest Access

A guest access security policy uses URL filtering policy, which allows and disallows access to specific URLs and webpage categories. URL filtering allows you to control access to Internet websites by permitting or denying access to specific websites based on allowed lists, blocked lists, categories, and reputations. For example, when a client sends a HTTP or HTTPS request, the router inspects the traffic. If, for example, the request matches the blocked list, either it is blocked by a blocked page response or it is redirected to a different URL. If, for example, the HTTP or HTTPS request matches the allowed list, the traffic is allowed without further URL filtering inspection.

To configure URL filter, you use the Guest Access policy option of the security policy configuration wizard.

### Step 1: Start the Security Policy Wizard

To start the security policy configuration wizard:

1. In vManage NMS, select the Configure ► Security screen.
2. Click Add Policy.
3. From the Add Security Policy popup, select Guest Access Policy.
4. Click Proceed.

The security policy configuration wizard opens, and the Firewall screen displays.

## Step 2: Configure Application Firewall Policy

To create a new application firewall policy:

1. In the Firewall screen, click the Add Firewall Policy drop-down.
2. Select Create New. The Add Firewall Policy screen displays.
3. In the Name field, enter a name for the firewall policy. The name can be up to 128 characters and can contain only alphanumeric characters.
4. In the Description field, enter a description of the firewall policy. The description can be up to 2048 characters and can contain only alphanumeric characters.
5. Create a zone pair or apply an existing zone pair to the firewall policy:
    a. Click Apply Zone Pairs. The Apply Zone Pairs popup displays.
    b. In Source Zone, select an existing zone. Or to create a new zone, click Create New Zone List. Then enter a name for the list and the VPNs in the zone, and click Save.
    c. In Destination Zone, select an existing zone. Or to create a new zone, click Create New Zone List. Then enter a name for the list and the VPNs in the zone, and click Save.
6. Create one or more security policy sequence rules to apply to the traffic that flows from the source zones to the destination zones:
    a. Click Add Sequence Rule.
    b. Click Match to add a match condition. You can match the following:
    - Application/Application Family List
    - Destination Data Prefix
    - Destination Port
    - Protocol
    - Source Data Prefix
    - Source Port
    c. Click Actions to define the actions to take when a match occurs. By default, the packet is dropped. You can take these other actions:
    - Inspect: Inspect the packet's header to determine its source address and port. The address and port are used by the NAT device to allow traffic to be returned from the destination to the sender.
    - Log: Log the packet headers.
    - Pass: Allow the packet to pass to the destination zone without inspecting the packet's header at all. With this action, the NAT device blocks return traffic that is addressed to the sender.
    d. Click Save Match and Actions.
    e. Add additional sequence rules as needed.
    f. Drag and drop the rules to arrange them in the desired sequence. Rules are applied to data packets in the order in which that are defined in the policy.
7. Click Save Firewall Policy.
8. Click Next.

To copy an existing firewall policy into the compliance security policy:

1. In the Firewall screen, click the Add Firewall Policy drop-down.
2. Select Copy from Existing.
3. In the Copy from Existing Firewall popup:

a. In the Policy field, select a policy.

b. In the Policy Name field, select a policy name.

c. In the Policy Description field, enter a description of the firewall policy. The description can be up to 2048 characters and can contain only alphanumeric characters.

d. Click Copy. The copied policy is listed in the Security Policy Firewall table.

4. Click Next. Depending on the security policy type you are configuring, one of the following screens displays:

- Intrusion prevention policy
- Umbrella DNS policy
- URL-filtering policy

## Step 3: Configure URL Filtering

To create a new URL-filtering policy:

1. In the URL Filtering screen, click the Add URL Filtering Policy drop-down.

2. Click Create New. The Add URL Filtering Policy screen displays.

3. In the Policy Name field, enter a name for the firewall policy. The name can be up to 32 characters and can contain only alphanumeric characters.

4. In the Web Categories field:

   a. In the Block drop-down, define the action to take if a URL matches a website category. Select Block (the default) to block access to the website category, or select Allow to allow access to the website category.

   b. In the Web Category field, select one or more webpage categories to block or accept. A category defines websites that contain a certain type of content.
   When you configure category-based or reputation-based URL filtering, a URL database is downloaded from the cloud. Incremental updates are automatically downloaded every 15 minutes. If connectivity to the cloud is lost for more than 24 hours, the database is invalidated. To check a website's reputation, use the Webroot BrightCloud URL/IP Lookup tool.

5. In the Web Reputation field, select the reputation level of the website to block or accept. Each URL has a reputation score associated with it. The score ranges from 0 through 100 and is labeled as follows:

- High Risk—Reputation score 0 through 20
- Suspicious—Reputation score 0 through 40
- Moderate Risk—Reputation score 0 through 60. This is the default reputation setting.
- Low Risk—Reputation score 0 through 80.
- Trustworthy—Reputation score 0 through 100.

6. In the Advanced ► Whitelist URL List field, select a URL list to include in the URL filtering policy. An allowed URL list allows the specified URLs and blocks URLs not included in the list. For each URL filtering policy, you can configure only one allowed URL list. To create a new list of URLs to allow:

   a. Click in he Advanced ► Whitelist URL List field.

   b. Click Add New Whitelist URL List.

   c. In the Whitelist URL List Name field, enter a name for the allowed list.

d. In the Add Whitelist URL field, enter one or more URLs to allow. You can specify the full URL, or you can use regular expressions, such as **.*\.cisco\.com** .

e. To import a list of URL into the allowed list, click the Upload arrow and then select the file to import.

f. Click Save.

7. In the Advanced ► Blacklist URL List field, select one or more blocked URL lists to include in the URL filtering policy. A URL blocked list blocks the specified URLs and allows URLs not included in the list. For each URL filtering policy, you can configure only one blocked URL list. To create a new list of URLs to block:

    a. Click in the Advanced ► Blacklist URL List field.

    b. Click Add New Blacklist URL List.

    c. In the Blacklist URL List Name field, enter a name for the blocked list.

    d. In the Add Whitelist URL field, enter one or more URLs to allow. You can specify the full URL, or you can use regular expressions, such as **.*\.cisco\.com** .

    e. To import a list of URL into the allowed list, click the Upload arrow and then select the file to import.

    f. Click Save.

8. In the Advanced ► Block Page Server section, configure how to handle blocked HTTP URLs. For blocked HTTPS websites, no blocking or redirection is performed. Instead, all traffic is dropped.

    a. To block and not display the content of a webpage, click Block Page Content. Then, type the message to display to the user indicated why the webpage is not displayed. This is the default method for handling blocked URLs. In the Default Content Header field, type the title of the message, which is displayed in bold letters. The default header is, "Access to the requested page has been denied." In the Content Body field, type the content of the blocked page message. The default message is, "Please contact your network administrator".

    b. To redirect to another URL, click Redirect URL. Then, enter the URL to which to redirect the user.

9. In the Advanced ► Alerts and Logs section, configure when to send alerts and syslog messages:

    a. Click Blacklist to send alerts when a blocked-list URL is blocked.

    b. Click Whitelist to send alerts when a allowed-list URL is allowed.

    c. Click Reputation/Category to send alerts when a URL is blocked because of its category or reputation.

10. Configure the VPNs to which to apply the URL filtering policy:

    a. In the Target field, click Add Target VPNs.

    b. Enter the VPN numbers to which to apply the URL filtering policy. To specify multiple VPNs, separate the numbers with commas.

    c. Click Save Changes.

11. Click Save URL Filtering Policy. The URL filtering policy is then listed in the policy table.

12. Click Next. The Policy Summary screen displays.

To copy an existing URL filtering policy into the guest access policy:

1. In the URL Filtering screen, click the Add URL Filtering Policy drop-down.

2. Select Copy from Existing.

3. In the Copy from Existing URL Filtering Policy popup:

a. In the Policy field, select a policy.

b. In the Policy Name field, select a policy name.

c. In the Policy Description field, enter a description of the firewall policy. The description can be up to 2048 characters and can contain only alphanumeric characters.

d. Click Copy. The copied policy is listed in the URL Filtering table.

4. Click Next. The Policy Summary screen displays.

## Step 4: Configure Additional Policy Settings

In the Policy Summary screen:

1. In the Security Policy Name field, enter the name of the security policy. The name can be up to 32 characters and can contain only alphanumeric characters, hyphens (-), and underscores (_).

2. In the Security Policy Description field,

3. In the Description field, enter a description of the security policy. The description can be up to 2048 characters and can contain only alphanumeric characters.

4. If you do not include VPN 0 in any of the zones that you configure in a zone-based firewall, by default, packets are able to reach destination zones that are accessible only over the public internet. To disallow this traffic, uncheck the Firewall ► Direct Internet Applications box.

5. To configure the number of TCP SYN packets that the router can receive while establishing a TCP connection to use for a zone-based firewall before the router shuts down the connection, move the Firewall ► TCP SYN Flood Limit slider to Enabled. Then enter a limit value from 1 through 2147483647 packets. The default limit is 2000 SYN packets.

6. By default, system logging (syslog) in enabled for intrusion detection. To disable syslog messages, move the Intrusion Prevention and/or URL Filtering ► Syslog slider to Disabled.

7. In the Intrusion Prevention and/or URL Filtering ► External Server field, configure an external syslog server. In the VPN field, specify the VPN through which the server can be reached. In the Server IP field, specify the IP address of the syslog server.

8. In the Intrusion Prevention and/or URL Filtering ► Failure Mode field, configure how the router handles traffic when the URL database update from the cloud fails. When you configure category-based or reputation-based URL filtering, as described above, a URL database is downloaded from the cloud. Incremental updates are automatically downloaded every 15 minutes. If connectivity to the cloud is lost for more than 24 hours, the database is invalidated. For the Failure Mode field, the default is Close, which drops all traffic destined for URL filtering when cloud connectivity is lost. To not drop traffic destined for URL filter, select Open.

9. To view the CLI commands that correspond to the compliance security policy configuration, click Preview.

10. Click Save Policy. The policy is listed in the table on the Configuration ► Policy screen.

## Step 5: Apply the Security Policy to an IOS XE Router

1. In vManage NMS, select the Configuration ► Templates screen.

2. If you are creating a new device template:

    a. In the Device tab, click Create Template.

    b. From the Create Template drop-down, select From Feature Template.

    c. From the Device Model drop-down, select one of the vEdge devices.

d. In the Template Name field, enter a name for the device template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores (_). It cannot contain spaces or any other characters.

e. In the Description field, enter a description for the device template. This field is mandatory, and it can contain any characters and spaces.

f. Continue with Step 4.

3. If you are editing an existing device template:

   a. In the Device tab, click the More Actions icon to the right of the desired template, and click the pencil icon.

   b. Click the Additional Templates tab. The screen scrolls to the Additional Templates section.

   c. From the Policy drop-down, select the name of a policy that you have configured.

4. Click the Additional Templates tab located directly beneath the Description field. The screen scrolls to the Additional Templates section.

5. From the Security Policy drop-down, select the name of the zone-based firewall you configured in the above procedure.

6. Click Create (for a new template) or Update (for an existing template).

## Configure Direct Cloud Access

A direct cloud access policy uses intrusion prevention and detection and Umbrella DNS security to control access from the local device the cloud devices.

Intrusion prevention policy protects against malicious attacks on data traffic by using signature sets and inspection mode. Intrusion detection passes all packets flowing between service-side and transport-side (WAN or internet) interfaces, and between VLANs, through an intrusion detection engine, generating alerts for traffic that is identified as malicious, and logging these alerts via syslog. Intrusion prevention blocks traffic that is identified as malicious.

DNS security policy directs traffic from your network to the cloud-based Cisco Umbrella secure internet gateway. Umbrella using DNS to stop threads over all ports and protocols and over direct-to-IP connections.

To configure this, you use the Direct Cloud Access option of the security policy configuration wizard.

### Step 1: Start the Security Policy Wizard

To start the security policy configuration wizard:

1. In vManage NMS, select the Configure ► Security screen.

2. Click Add Policy.

3. From the Add Security Policy popup, select Guest Access Policy.

4. Click Proceed.

The security policy configuration wizard opens, and the Firewall screen displays.

### Step 2: Configure Application Firewall Policy

To create a new application firewall policy:

1. In the Firewall screen, click the Add Firewall Policy drop-down.

2. Select Create New. The Add Firewall Policy screen displays.

3. In the Name field, enter a name for the firewall policy. The name can be up to 128 characters and can contain only alphanumeric characters.

4. In the Description field, enter a description of the firewall policy. The description can be up to 2048 characters and can contain only alphanumeric characters.

5. Create a zone pair or apply an existing zone pair to the firewall policy:

    a. Click Apply Zone Pairs. The Apply Zone Pairs popup displays.

    b. In Source Zone, select an existing zone. Or to create a new zone, click Create New Zone List. Then enter a name for the list and the VPNs in the zone, and click Save.

    c. In Destination Zone, select an existing zone. Or to create a new zone, click Create New Zone List. Then enter a name for the list and the VPNs in the zone, and click Save.

6. Create one or more security policy sequence rules to apply to the traffic that flows from the source zones to the destination zones:

    a. Click Add Sequence Rule.

    b. Click Match to add a match condition. You can match the following:
    - Application/Application Family List
    - Destination Data Prefix
    - Destination Port
    - Protocol
    - Source Data Prefix
    - Source Port

    c. Click Actions to define the actions to take when a match occurs. By default, the packet is dropped. You can take these other actions:
    - Inspect: Inspect the packet's header to determine its source address and port. The address and port are used by the NAT device to allow traffic to be returned from the destination to the sender.
    - Log: Log the packet headers.
    - Pass: Allow the packet to pass to the destination zone without inspecting the packet's header at all. With this action, the NAT device blocks return traffic that is addressed to the sender.

    d. Click Save Match and Actions.

    e. Add additional sequence rules as needed.

    f. Drag and drop the rules to arrange them in the desired sequence. Rules are applied to data packets in the order in which that are defined in the policy.

7. Click Save Firewall Policy.

8. Click Next.

To copy an existing firewall policy into the compliance security policy:

1. In the Firewall screen, click the Add Firewall Policy drop-down.

2. Select Copy from Existing.

3. In the Copy from Existing Firewall popup:

    a. In the Policy field, select a policy.

    b. In the Policy Name field, select a policy name.

    c. In the Policy Description field, enter a description of the firewall policy. The description can be up to 2048 characters and can contain only alphanumeric characters.

d. Click Copy. The copied policy is listed in the Security Policy Firewall table.

4. Click Next. Depending on the security policy type you are configuring, one of the following screens displays:

- Intrusion prevention policy
- Umbrella DNS policy
- URL-filtering policy

## Step 3: Configure Intrusion Prevention and Detection

To create a new intrusion prevention and detection policy:

1. In the Intrusion Prevention screen, click the Add Intrusion Prevention Policy drop-down.
2. Click Create New. The Add Intrusion Prevention Policy screen displays.
3. In the Policy Name field, enter a name for the firewall policy. The name can be up to 32 characters and can contain only alphanumeric characters.
4. In the Signature Set field, select the desired signature set:

- Balanced (default)—Contains rules that are from the current year and the previous two years, are for vulnerabilities with a Common Vulnerability Scoring System (CVSS) score of 9 or greater, and are in one of the following categories:
  – Blacklist—Rules for URIs, user agents, DNS hostnames, and IP addresses that have been determined to be indicators of malicious activity.
  – Exploit-kit—Rules that are designed to detect exploit kit activity.
  – Malware-CNC—Rules for known malicious command and control activity for identified botnet traffic. These include call home, downloading of dropped files, and ex-filtration of data.
  – SQL Injection—Rules that are designed to detect SQL Injection attempts.
- Connectivity—Contains rules from the current year and the previous two years for vulnerabilities with a CVSS score of 10.
- Security—Contains rules that are from the current year and the previous three years, are for vulnerabilities with a CVSS score of 8 or greater, and are in one of the following categories:
  – App-detect—Rules that look for and control the traffic of certain applications that generate network activity.
  – Blacklist—Rules for URIs, user agents, DNS hostnames, and IP addresses that have been determined to be indicators of malicious activity.
  – Exploit-kit—Rules that are designed to detect exploit kit activity.
  – Malware-CNC—Rules for known malicious command and control activity for identified botnet traffic. These include call home, downloading of dropped files, and ex-filtration of data.
  – SQL Injection—Rules that are designed to detect SQL Injection attempts.

5. In the Inspection Mode field, select the desired inspection mode:

- Detection—In intrusion detection mode, traffic is accepted or blocked based on the rules defined by the signature set that you choose.
- Protection—In intrusion prevention mode, malicious traffic is automatically blocked, based on the intrusion prevention policy rules.

6. In the Advanced ► Signature Whitelist field, select the desired signature list.

7. In the Advanced ► Alerts Log Level field, select the desired log level for alerts. The level can be Emergency, Alert, Critical, Error, Warning, Notice, Info, and Debug. The default is Error.
8. Configure the VPNs to which to apply the intrusion prevention policy:
    a. In the Target field, click Add Target VPNs.
    b. Enter the VPN numbers to which to apply the intrusion prevention policy. To specify multiple VPNs, separate the numbers with commas.
    c. Click Save Changes.
9. Click Save Intrusion Prevention Policy. The intrusion prevention policy is then listed in the policy table.
10. Click Next. The Policy Summary screen displays.

To copy an existing intrusion prevention policy into the compliance security policy:

1. In the Intrusion Prevention screen, click the Add Intrusion Prevention Policy drop-down.
2. Select Copy from Existing.
3. In the Copy from Existing Intrusion Prevention Policy popup:
    a. In the Policy field, select a policy.
    b. In the Policy Name field, select a policy name.
    c. In the Policy Description field, enter a description of the firewall policy. The description can be up to 2048 characters and can contain only alphanumeric characters.
    d. Click Copy. The copied policy is listed in the Security Policy Firewall table.
4. Click Next. The Policy Summary screen displays.

## Step 4: Configure Umbrella DNS

To create a new Umbrella DNS policy:

1. In the Add Security Policy screen, click the Add DNS Security Policy drop-down.
2. Click Create New. The Add DNS Security Policy screen displays.
3. In the Policy Name field, enter a name for the firewall policy. The name can be up to 32 characters and can contain only alphanumeric characters.
4. In the Umbrella Registration Status field:
    a. Click Manage Umbrella Registration.
    b. In the Manage Umbrella Registration pop-up, enter your Umbrella registration token.
    c. Click Save Changes.
5. By default, the DNS security policy applies to all VPNs, so the Match All VPN field is selected. To apply the DNS security policy to a custom set of VPNs:
    a. Select the Custom VPN Configuration field.
    b. In the Target field, click Add Target VPNs.

   c. Enter the VPN numbers to which to apply the intrusion prevention policy. To specify multiple VPNs, separate the numbers with commas.

   d. Click Save Changes.

6. In the Local Domain Bypass List field, select the web domain list that lists the websites domains that are allowed by bypass DNS lookups. To create a domain list:

   a. Click in the Local Domain Bypass List field and then click Add New Domain List.

   b. In the Domain List Name field, enter a name for the domain list.

   c. In the Domain field, enter one or more web domains. Examples of website domains are cisco.com and *.cisco.com. Separate lists with a comma. The first item in the list cannot start with an asterisk (*).

   d. Click Save.

7. In the DNS Server IP field, select the IP address of the DNS server. By default, traffic using Umbrella as the DNS server. To use a different DNS server, select Custom DNS and enter the IP address of the DNS server.

6. In the Advanced ► DNSCrypt field, configure the encryption of DNS traffic. By default, encryption is enabled. To disable DNS traffic encryption, move the slider to the left.

7. Click Save DNS Security Policy. The intrusion prevention policy is then listed in the policy table.

8. Click Next. The Policy Summary screen displays.

To copy an existing intrusion prevention policy into the compliance security policy:

1. In the Add Security Policy screen, click the Add DNS Security Policy drop-down.

2. Select Copy from Existing.

3. In the Copy from Existing DNS Security Policy popup:

   a. In the Policy field, select a policy.

   b. In the Policy Name field, select a policy name.

   c. Click Copy. The copied policy is listed in the Security Policy Firewall table.

4. Click Next. The Policy Summary screen displays.

## Step 5: Configure Additional Policy Settings

In the Policy Summary screen:

1. In the Security Policy Name field, enter the name of the security policy. The name can be up to 32 characters and can contain only alphanumeric characters, hyphens (-), and underscores (_).

2. In the Security Policy Description field,

3. In the Description field, enter a description of the security policy. The description can be up to 2048 characters and can contain only alphanumeric characters.

4. If you do not include VPN 0 in any of the zones that you configure in a zone-based firewall, by default, packets are able to reach destination zones that are accessible only over the public internet. To disallow this traffic, uncheck the Firewall ► Direct Internet Applications box.

5. To configure the number of TCP SYN packets that the router can receive while establishing a TCP connection to use for a zone-based firewall before the router shuts down the connection, move the Firewall ▶ TCP SYN Flood Limit slider to Enabled. Then enter a limit value from 1 through 2147483647 packets. The default limit is 2000 SYN packets.

6. By default, system logging (syslog) in enabled for intrusion detection. To disable syslog messages, move the Intrusion Prevention and/or URL Filtering ▶ Syslog slider to Disabled.

7. In the Intrusion Prevention and/or URL Filtering ▶ External Server field, configure an external syslog server. In the VPN field, specify the VPN through which the server can be reached. In the Server IP field, specify the IP address of the syslog server.

8. In the Intrusion Prevention and/or URL Filtering ▶ Failure Mode field, configure how the router handles traffic when the URL database update from the cloud fails. When you configure category-based or reputation-based URL filtering, as described above, a URL database is downloaded from the cloud. Incremental updates are automatically downloaded every 15 minutes. If connectivity to the cloud is lost for more than 24 hours, the database is invalidated. For the Failure Mode field, the default is Close, which drops all traffic destined for URL filtering when cloud connectivity is lost. To not drop traffic destined for URL filter, select Open.

9. To view the CLI commands that correspond to the compliance security policy configuration, click Preview.

10. Click Save Policy. The policy is listed in the table on the Configuration ▶ Policy screen.

## Step 6: Apply the Security Policy to an IOS XE Router

1. In vManage NMS, select the Configuration ▶ Templates screen.

2. If you are creating a new device template:

    a. In the Device tab, click Create Template.

    b. From the Create Template drop-down, select From Feature Template.

    c. From the Device Model drop-down, select one of the vEdge devices.

    d. In the Template Name field, enter a name for the device template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores (_). It cannot contain spaces or any other characters.

    e. In the Description field, enter a description for the device template. This field is mandatory, and it can contain any characters and spaces.

    f. Continue with Step 4.

3. If you are editing an existing device template:

    a. In the Device tab, click the More Actions icon to the right of the desired template, and click the pencil icon.

    b. Click the Additional Templates tab. The screen scrolls to the Additional Templates section.

    c. From the Policy drop-down, select the name of a policy that you have configured.

4. Click the Additional Templates tab located directly beneath the Description field. The screen scrolls to the Additional Templates section.

5. From the Security Policy drop-down, select the name of the zone-based firewall you configured in the above procedure.

6. Click Create (for a new template) or Update (for an existing template).

# Configure Direct Internet Access

A direct internet access policy uses intrusion prevention and detection, URL filtering, and Umbrella DNS security to control access from the local device the internet.

Intrusion prevention policy protects against malicious attacks on data traffic by using signature sets and inspection mode. Intrusion detection passes all packets flowing between service-side and transport-side (WAN or internet) interfaces, and between VLANs, through an intrusion detection engine, generating alerts for traffic that is identified as malicious, and logging these alerts via syslog. Intrusion prevention blocks traffic that is identified as malicious.

URL filtering policy allows and disallows access to specific URLs and webpage categories. URL filtering allows you to control access to Internet websites by permitting or denying access to specific websites based on allowed lists, blocked lists, categories, and reputations. For example, when a client sends a HTTP or HTTPS request, the router inspects the traffic. If, for example, the request matches the blocked list, either it is blocked by a blocked page response or it is redirected to a different URL. If, for example, the HTTP or HTTPS request matches the allowed list, the traffic is allowed without further URL filtering inspection.

DNS security policy directs traffic from your network to the cloud-based Cisco Umbrella secure internet gateway. Umbrella using DNS to stop threads over all ports and protocols and over direct-to-IP connections.

To configure this, you use the Direct Cloud Access option of the security policy configuration wizard.

## Step 1: Start the Security Policy Wizard

To start the security policy configuration wizard:

1. In vManage NMS, select the Configure ► Security screen.
2. Click Add Policy.
3. From the Add Security Policy popup, select Guest Access Policy.
4. Click Proceed.

The security policy configuration wizard opens, and the Firewall screen displays.

## Step 2: Configure Application Firewall Policy

To create a new application firewall policy:

1. In the Firewall screen, click the Add Firewall Policy drop-down.
2. Select Create New. The Add Firewall Policy screen displays.
3. In the Name field, enter a name for the firewall policy. The name can be up to 128 characters and can contain only alphanumeric characters.
4. In the Description field, enter a description of the firewall policy. The description can be up to 2048 characters and can contain only alphanumeric characters.
5. Create a zone pair or apply an existing zone pair to the firewall policy:
    a. Click Apply Zone Pairs. The Apply Zone Pairs popup displays.
    b. In Source Zone, select an existing zone. Or to create a new zone, click Create New Zone List. Then enter a name for the list and the VPNs in the zone, and click Save.
    c. In Destination Zone, select an existing zone. Or to create a new zone, click Create New Zone List. Then enter a name for the list and the VPNs in the zone, and click Save.
6. Create one or more security policy sequence rules to apply to the traffic that flows from the source zones to the destination zones:
    a. Click Add Sequence Rule.

b. Click Match to add a match condition. You can match the following:
- Application/Application Family List
- Destination Data Prefix
- Destination Port
- Protocol
- Source Data Prefix
- Source Port

c. Click Actions to define the actions to take when a match occurs. By default, the packet is dropped. You can take these other actions:
- Inspect: Inspect the packet's header to determine its source address and port. The address and port are used by the NAT device to allow traffic to be returned from the destination to the sender.
- Log: Log the packet headers.
- Pass: Allow the packet to pass to the destination zone without inspecting the packet's header at all. With this action, the NAT device blocks return traffic that is addressed to the sender.

d. Click Save Match and Actions.

e. Add additional sequence rules as needed.

f. Drag and drop the rules to arrange them in the desired sequence. Rules are applied to data packets in the order in which that are defined in the policy.

7. Click Save Firewall Policy.

8. Click Next.

To copy an existing firewall policy into the compliance security policy:

1. In the Firewall screen, click the Add Firewall Policy drop-down.

2. Select Copy from Existing.

3. In the Copy from Existing Firewall popup:

   a. In the Policy field, select a policy.

   b. In the Policy Name field, select a policy name.

   c. In the Policy Description field, enter a description of the firewall policy. The description can be up to 2048 characters and can contain only alphanumeric characters.

   d. Click Copy. The copied policy is listed in the Security Policy Firewall table.

4. Click Next. Depending on the security policy type you are configuring, one of the following screens displays:

- Intrusion prevention policy
- Umbrella DNS policy
- URL-filtering policy

## Step 3: Configure Intrusion Prevention and Detection

To create a new intrusion prevention and detection policy:

1. In the Intrusion Prevention screen, click the Add Intrusion Prevention Policy drop-down.

2. Click Create New. The Add Intrusion Prevention Policy screen displays.

3. In the Policy Name field, enter a name for the firewall policy. The name can be up to 32 characters and can contain only alphanumeric characters.

4. In the Signature Set field, select the desired signature set:

- Balanced (default)—Contains rules that are from the current year and the previous two years, are for vulnerabilities with a Common Vulnerability Scoring System (CVSS) score of 9 or greater, and are in one of the following categories:
  - Blacklist—Rules for URIs, user agents, DNS hostnames, and IP addresses that have been determined to be indicators of malicious activity.
  - Exploit-kit—Rules that are designed to detect exploit kit activity.
  - Malware-CNC—Rules for known malicious command and control activity for identified botnet traffic. These include call home, downloading of dropped files, and ex-filtration of data.
  - SQL Injection—Rules that are designed to detect SQL Injection attempts.
- Connectivity—Contains rules from the current year and the previous two years for vulnerabilities with a CVSS score of 10.
- Security—Contains rules that are from the current year and the previous three years, are for vulnerabilities with a CVSS score of 8 or greater, and are in one of the following categories:
  - App-detect—Rules that look for and control the traffic of certain applications that generate network activity.
  - Blacklist—Rules for URIs, user agents, DNS hostnames, and IP addresses that have been determined to be indicators of malicious activity.
  - Exploit-kit—Rules that are designed to detect exploit kit activity.
  - Malware-CNC—Rules for known malicious command and control activity for identified botnet traffic. These include call home, downloading of dropped files, and ex-filtration of data.
  - SQL Injection—Rules that are designed to detect SQL Injection attempts.

5. In the Inspection Mode field, select the desired inspection mode:

- Detection—In intrusion detection mode, traffic is accepted or blocked based on the rules defined by the signature set that you choose.
- Protection—In intrusion prevention mode, malicious traffic is automatically blocked, based on the intrusion prevention policy rules.

6. In the Advanced ► Signature Whitelist field, select the desired signature list.

7. In the Advanced ► Alerts Log Level field, select the desired log level for alerts. The level can be Emergency, Alert, Critical, Error, Warning, Notice, Info, and Debug. The default is Error.

8. Configure the VPNs to which to apply the intrusion prevention policy:
   a. In the Target field, click Add Target VPNs.
   b. Enter the VPN numbers to which to apply the intrusion prevention policy. To specify multiple VPNs, separate the numbers with commas.
   c. Click Save Changes.

9. Click Save Intrusion Prevention Policy. The intrusion prevention policy is then listed in the policy table.

10. Click Next. The Policy Summary screen displays.

To copy an existing intrusion prevention policy into the compliance security policy:

1. In the Intrusion Prevention screen, click the Add Intrusion Prevention Policy drop-down.

2. Select Copy from Existing.
3. In the Copy from Existing Intrusion Prevention Policy popup:
    a. In the Policy field, select a policy.
    b. In the Policy Name field, select a policy name.
    c. In the Policy Description field, enter a description of the firewall policy. The description can be up to 2048 characters and can contain only alphanumeric characters.
    d. Click Copy. The copied policy is listed in the Security Policy Firewall table.
4. Click Next. The Policy Summary screen displays.

## Step 4: Configure URL Filtering

To create a new URL-filtering policy:

1. In the URL Filtering screen, click the Add URL Filtering Policy drop-down.
2. Click Create New. The Add URL Filtering Policy screen displays.
3. In the Policy Name field, enter a name for the firewall policy. The name can be up to 32 characters and can contain only alphanumeric characters.
4. In the Web Categories field:
    a. In the Block drop-down, define the action to take if a URL matches a website category. Select Block (the default) to block access to the website category, or select Allow to allow access to the website category.
    b. In the Web Category field, select one or more webpage categories to block or accept. A category defines websites that contain a certain type of content.
    When you configure category-based or reputation-based URL filtering, a URL database is downloaded from the cloud. Incremental updates are automatically downloaded every 15 minutes. If connectivity to the cloud is lost for more than 24 hours, the database is invalidated. To check a website's reputation, use the Webroot BrightCloud URL/IP Lookup tool.
5. In the Web Reputation field, select the reputation level of the website to block or accept. Each URL has a reputation score associated with it. The score ranges from 0 through 100 and is labeled as follows:

- High Risk—Reputation score 0 through 20
- Suspicious—Reputation score 0 through 40
- Moderate Risk—Reputation score 0 through 60. This is the default reputation setting.
- Low Risk—Reputation score 0 through 80.
- Trustworthy—Reputation score 0 through 100.

6. In the Advanced ► Whitelist URL List field, select a URL list to include in the URL filtering policy. An allowed URL list allows the specified URLs and blocks URLs not included in the list. For each URL filtering policy, you can configure only one allowed URL list. To create a new list of URLs to allow:
    a. Click in he Advanced ► Whitelist URL List field.
    b. Click Add New Whitelist URL List.
    c. In the Whitelist URL List Name field, enter a name for the allowed list.

d. In the Add Whitelist URL field, enter one or more URLs to allow. You can specify the full URL, or you can use regular expressions, such as **.*\.cisco\.com** .

e. To import a list of URL into the allowed list, click the Upload arrow and then select the file to import.

f. Click Save.

7. In the Advanced ► Blacklist URL List field, select one or more blocked URL lists to include in the URL filtering policy. A blocked URL list blocks the specified URLs and allows URLs not included in the list. For each URL filtering policy, you can configure only one blocked URL list. To create a new list of URLs to block:

    a. Click in the Advanced ► Blacklist URL List field.

    b. Click Add New Blacklist URL List.

    c. In the Blacklist URL List Name field, enter a name for the blocked list.

    d. In the Add Whitelist URL field, enter one or more URLs to allow. You can specify the full URL, or you can use regular expressions, such as **.*\.cisco\.com** .

    e. To import a list of URL into the allowed list, click the Upload arrow and then select the file to import.

    f. Click Save.

8. In the Advanced ► Block Page Server section, configure how to handle blocked HTTP URLs. For blocked HTTPS websites, no blocking or redirection is performed. Instead, all traffic is dropped.

    a. To block and not display the content of a webpage, click Block Page Content. Then, type the message to display to the user indicated why the webpage is not displayed. This is the default method for handling blocked URLs. In the Default Content Header field, type the title of the message, which is displayed in bold letters. The default header is, "Access to the requested page has been denied." In the Content Body field, type the content of the blocked page message. The default message is, "Please contact your network administrator".

    b. To redirect to another URL, click Redirect URL. Then, enter the URL to which to redirect the user.

9. In the Advanced ► Alerts and Logs section, configure when to send alerts and syslog messages:

    a. Click Blacklist to send alerts when a blocked-list URL is blocked.

    b. Click Whitelist to send alerts when a allowed-list URL is allowed.

    c. Click Reputation/Category to send alerts when a URL is blocked because of its category or reputation.

10. Configure the VPNs to which to apply the URL filtering policy:

    a. In the Target field, click Add Target VPNs.

    b. Enter the VPN numbers to which to apply the URL filtering policy. To specify multiple VPNs, separate the numbers with commas.

    c. Click Save Changes.

11. Click Save URL Filtering Policy. The URL filtering policy is then listed in the policy table.

12. Click Next. The Policy Summary screen displays.

To copy an existing URL filtering policy into the guest access policy:

1. In the URL Filtering screen, click the Add URL Filtering Policy drop-down.

2. Select Copy from Existing.

3. In the Copy from Existing URL Filtering Policy popup:

a. In the Policy field, select a policy.

b. In the Policy Name field, select a policy name.

c. In the Policy Description field, enter a description of the firewall policy. The description can be up to 2048 characters and can contain only alphanumeric characters.

d. Click Copy. The copied policy is listed in the URL Filtering table.

4. Click Next. The Policy Summary screen displays.

## Step 5: Configure Umbrella DNS

To create a new Umbrella DNS policy:

1. In the Add Security Policy screen, click the Add DNS Security Policy drop-down.
2. Click Create New. The Add DNS Security Policy screen displays.
3. In the Policy Name field, enter a name for the firewall policy. The name can be up to 32 characters and can contain only alphanumeric characters.
4. In the Umbrella Registration Status field:
    a. Click Manage Umbrella Registration.
    b. In the Manage Umbrella Registration pop-up, enter your Umbrella registration token.
    c. Click Save Changes.
5. By default, the DNS security policy applies to all VPNs, so the Match All VPN field is selected. To apply the DNS security policy to a custom set of VPNs:
    a. Select the Custom VPN Configuration field.
    b. In the Target field, click Add Target VPNs.
    c. Enter the VPN numbers to which to apply the intrusion prevention policy. To specify multiple VPNs, separate the numbers with commas.
    d. Click Save Changes.
6. In the Local Domain Bypass List field, select the web domain list that lists the websites domains that are allowed by bypass DNS lookups. To create a domain list:
    a. Click in the Local Domain Bypass List field and then click Add New Domain List.
    b. In the Domain List Name field, enter a name for the domain list.
    c. In the Domain field, enter one or more web domains. Examples of website domains are cisco.com and *.cisco.com. Separate lists with a comma. The first item in the list cannot start with an asterisk (*).
    d. Click Save.
7. In the DNS Server IP field, select the IP address of the DNS server. By default, traffic using Umbrella as the DNS server. To use a different DNS server, select Custom DNS and enter the IP address of the DNS server.

6. In the Advanced ► DNSCrypt field, configure the encryption of DNS traffic. By default, encryption is enabled. To disable DNS traffic encryption, move the slider to the left.

7. Click Save DNS Security Policy. The intrusion prevention policy is then listed in the policy table.

8. Click Next. The Policy Summary screen displays.

To copy an existing intrusion prevention policy into the compliance security policy:

1. In the Add Security Policy screen, click the Add DNS Security Policy drop-down.
2. Select Copy from Existing.
3. In the Copy from Existing DNS Security Policy popup:
    a. In the Policy field, select a policy.
    b. In the Policy Name field, select a policy name.
    c. Click Copy. The copied policy is listed in the Security Policy Firewall table.
4. Click Next. The Policy Summary screen displays.

## Step 6: Configure Additional Policy Settings

In the Policy Summary screen:

1. In the Security Policy Name field, enter the name of the security policy. The name can be up to 32 characters and can contain only alphanumeric characters, hyphens (-), and underscores (_).
2. In the Security Policy Description field,
3. In the Description field, enter a description of the security policy. The description can be up to 2048 characters and can contain only alphanumeric characters.
4. If you do not include VPN 0 in any of the zones that you configure in a zone-based firewall, by default, packets are able to reach destination zones that are accessible only over the public internet. To disallow this traffic, uncheck the Firewall ► Direct Internet Applications box.
5. To configure the number of TCP SYN packets that the router can receive while establishing a TCP connection to use for a zone-based firewall before the router shuts down the connection, move the Firewall ► TCP SYN Flood Limit slider to Enabled. Then enter a limit value from 1 through 2147483647 packets. The default limit is 2000 SYN packets.
6. By default, system logging (syslog) in enabled for intrusion detection. To disable syslog messages, move the Intrusion Prevention and/or URL Filtering ► Syslog slider to Disabled.
7. In the Intrusion Prevention and/or URL Filtering ► External Server field, configure an external syslog server. In the VPN field, specify the VPN through which the server can be reached. In the Server IP field, specify the IP address of the syslog server.
8. In the Intrusion Prevention and/or URL Filtering ► Failure Mode field, configure how the router handles traffic when the URL database update from the cloud fails. When you configure category-based or reputation-based URL filtering, as described above, a URL database is downloaded from the cloud. Incremental updates are automatically downloaded every 15 minutes. If connectivity to the cloud is lost for more than 24 hours, the database is invalidated. For the Failure Mode field, the default is Close, which drops all traffic destined for URL filtering when cloud connectivity is lost. To not drop traffic destined for URL filter, select Open.
9. To view the CLI commands that correspond to the compliance security policy configuration, click Preview.
10. Click Save Policy. The policy is listed in the table on the Configuration ► Policy screen.

## Step 7: Apply the Security Policy to an IOS XE Router

1. In vManage NMS, select the Configuration ► Templates screen.

2. If you are creating a new device template:
   a. In the Device tab, click Create Template.
   b. From the Create Template drop-down, select From Feature Template.
   c. From the Device Model drop-down, select one of the vEdge devices.
   d. In the Template Name field, enter a name for the device template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores (_). It cannot contain spaces or any other characters.
   e. In the Description field, enter a description for the device template. This field is mandatory, and it can contain any characters and spaces.
   f. Continue with Step 4.
3. If you are editing an existing device template:
   a. In the Device tab, click the More Actions icon to the right of the desired template, and click the pencil icon.
   b. Click the Additional Templates tab. The screen scrolls to the Additional Templates section.
   c. From the Policy drop-down, select the name of a policy that you have configured.
4. Click the Additional Templates tab located directly beneath the Description field. The screen scrolls to the Additional Templates section.
5. From the Security Policy drop-down, select the name of the zone-based firewall you configured in the above procedure.
6. Click Create (for a new template) or Update (for an existing template).

## Configure a Custom UTD Security Policy

You can create a custom UTD security policy consisting of any of the standard UTD policy components.

To start the security policy configuration wizard:

1. In vManage NMS, select the Configure ► Security screen.
2. Click Add Policy.
3. From the Add Security Policy popup, select the Custom option.
4. Click Proceed.

The security policy configuration wizard opens, and the Firewall screen displays. Configure the desired security policy components.

## Additional Information

[Configuring Zone-Based Firewalls]
[Zone-Based Firewalls]
[Zone-Based Firewall Configuration Examples]

This article describes how to configure zone-base firewalls.

## Zone-based Firewall Configuration Examples

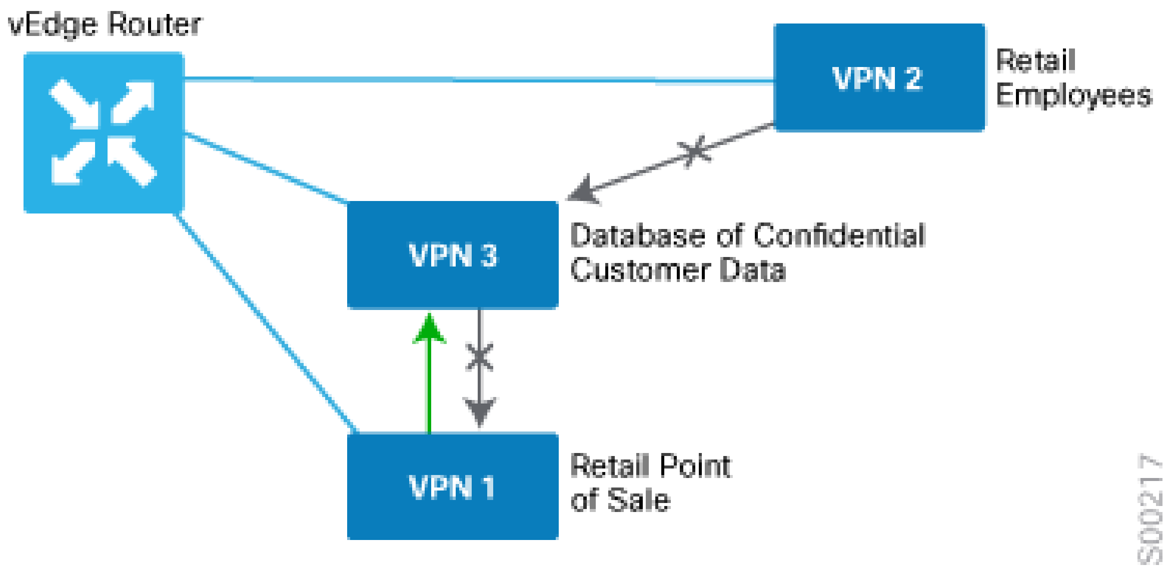
This articles provides an example of configuring a simple zone-based firewall.

## Isolating Two VPNs

In this zone-based firewall configuration example, we have a scenario where a vEdge router is connected to three service-side networks:

- Guest network that provides point-of-sale (PoS) services
- Employee network
- Network that provides shared services, including shared printers and the customer database

We want users in the employee and guest networks to be able to access the shared services, but we do not want any traffic to be exchanged between the employee and guest networks. Similarly, we do not want any traffic that originates in the shared services network to enter into either the employee network or the guest network. The following figure illustrates this scenario:




In this figure:

- VPN 1 is the guest network used for PoS services.
- VPN 2 is the network used by the enterprise's employees.
- VPN 3 contains the shared services, including printers and customer databases.

The configuration consists of three sections:

- Define the zones.
- Define the zone-based firewall policy.
- Apply the zone-based firewall policy to a source zone and destination zone pair.

### CLI Configuration

First, we define the zones for this scenario:

```
vEdge(config)# policy
vEdge(config-policy)# zone pos-zone vpn 1
```

```
vEdge(config-policy)# zone employee-zone vpn 2
vEdge(config-policy)# zone services-zone vpn 3
```

In this simple example, each zone corresponds to a single VPN. If you were to later add a second VPN for a discrete group of employees (let's say this is VPN 20) and you wanted this VPN to be subject to the same firewall policy, you could simply add this VPN to the employee zone:

```
vEdge(config-policy)# zone employee-zone vpn 20
vEdge(config-policy)# show full-configuration
policy
 zone employee-zone
  vpn 2
  vpn 20
 !
!
```

Next, we configure the zone-based firewall policy. The policy matches all traffic that is destined for VPN 3, which is the services zone, and which has an IP prefix of 10.2.2.0/24. Because we want the policy to allow traffic to flow from VPN 1 and VPN 2 to VPN 3, but we do not want traffic to flow in the reverse direction, we set the action to **pass** .

```
vEdge(config-policy)# zone-based-policy vpn-isolation-policy
vEdge(config-zone-based-policy)# sequence 10
vEdge(config-sequence)# match destination-ip 10.2.2.0/24
vEdge(config-sequence)# action pass
```

We want to drop any traffic that does not match the zone-based filrewall policy:

```
vEdge(config-zone-based-policy)# default-action drop
```

In the final step of the configuration process, we apply the zone-based firewall policy to the zones. Here is the zone pairing between the guest and PoS zone and the services zone:

```
vEdge(config-policy)# zone-pair pos-services-pairing
vEdge(config-zone-pair)# source-zone pos-zone
vEdge(config-zone-pair)# destination-zone services-zone
vEdge(config-zone-pair)# zone-policy vpn-isolation-policy
```

And here is the pairing between the employee zone and the services zone:

```
vEdge(config-policy)# zone-pair employee-services-pairing
vEdge(config-zone-pair)# source-zone employee-zone
vEdge(config-zone-pair)# destination-zone services-zone
vEdge(config-zone-pair)# zone-pair employee-services-pairing
```

Here is a view of the entire policy:

```
vEdge(config-policy)# show full-configuration
policy
 zone employee-zone
  vpn 2
 !
 zone pos-zone
  vpn 1
 !
 zone services-zone
  vpn 3
 !
 zone-pair employee-services-pairing
  source-zone      employee-zone
  destination-zone services-zone
  zone-policy      vpn-isolation-policy
 !
 zone-pair services-pairing
  source-zone      pos-zone
  destination-zone services-zone
  zone-policy      vpn-isolation-policy
 !
```

```
 zone-based-policy vpn-isolation-policy
  sequence 10
   match
    destination-ip 10.2.2.0/24
   !
   action pass
   !
  !
  default-action drop
 !
!
```

## vManage Configuration

To configure this zone-based firewall policy in vManage NMS:

1. Select Configuration ► Security.
2. Click Add Policy. The zone-based firewall configuration wizard opens.

Configure data prefix groups and zones in the Create Groups of Interest screen:

1. In the left pane, select Data Prefix.
2. In the right pane, click New Data Prefix List.
3. Enter a name for the list.
4. Enter the data prefix or prefixes to include in the list.
5. Click Add.

Configure zones in the Create Groups of Interest screen:

1. In the left pane, select Zones.
2. In the right pane, click New Zone List.
3. Enter a name for the list.
4. Enter the number of the zone or zones to include in the list. Separate numbers with a comma.
5. Click Add.

Click Next to move to Zone-Based Firewall in the zone-based firewall configuration wizard.

Configure zone-based firewall policies:

1. Click Add Configuration, and select Create New.
2. Enter a name and description for the policy.
3. In the left pane, click Add Sequence.
4. In the right pane, click Add Sequence Rule.
5. Select the desired match and action conditions.
6. Click Same Match and Actions.
7. In the left pane, click Default Action.

8. Select the desired default action.

9. Click Save Zone-Based Policy.

Click Next to move to the Apply Configuration in the zone-based firewall configuration wizard.

1. Enter a name and description for the zone-based firewall zone pair.

2. Click Add Zone Pair.

3. In the Source Zone drop-down, select the zone from which data traffic originates.

4. In the Destination Zone drop-down, select the zone to which data traffic is sent.

5. Click Add.

6. Click Save Policy. The Configuration ► Security screen is then displayed, and the zone-based firewalls table includes the newly created policy.

## Additional Information

Configuring Zone-Based Firewalls
Zone-Based Firewalls

# Revision 19.1 Topics

## EIGRP

Cisco release 19.1 supports Enhanced Interior Gateway Routing Protocol (EIGRP) on Cisco IOS XE devices. Cisco EIGRP is an open standard IGP routing protocol that provides advantages such as:

- Increased network width from 15 to 100 hops
- Fast convergence
- Incremental updates, minimizing bandwidth
- Protocol-independent neighbor discovery
- Easy scaling

**Note:** If your EIGRP network includes vEdge routers, you may need additional software. Refer to SD-WAN 19.1 release notes for configuration information.

To configure EIGRP routing protocol using vManage templates:

1. Create an EIGRP feature template to configure EIGRP parameters, as described in this article.

2. Create a VPN feature template to configure VPN parameters for service-side routing (any VPN other than VPN 0 or VPN 512). See VPN .

3. Create a device template and apply the templates to the correct devices. See Templates .

## Create and Name an EIGRP Template

1. From the vManage menu, select Configuration ► Templates.

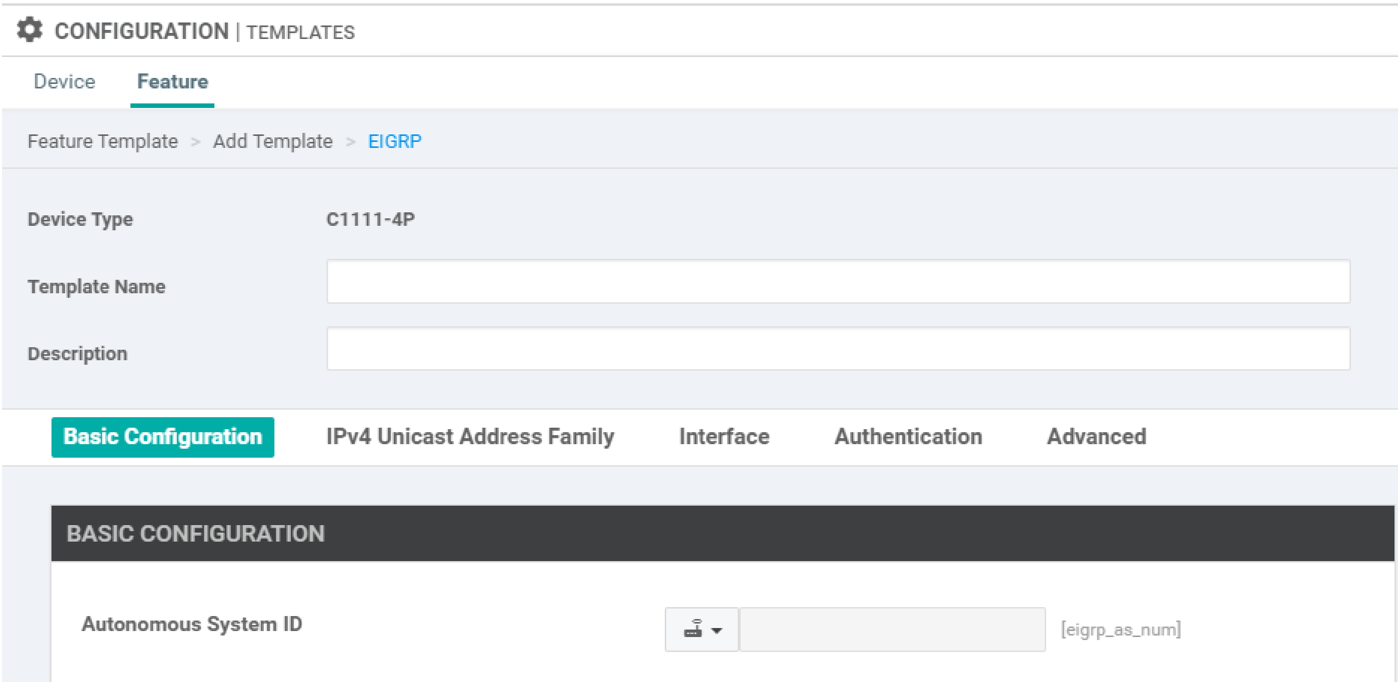
2. Click **Feature** .

3. Click Add Template.

4. Select a Cisco IOS XE device from the list.

5. From the Other Templates section, click **EIGRP** .

The EIGRP Feature template opens. The top of the form contains fields for naming the template, and the bottom contains fields for defining EIGRP parameters.

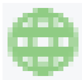



6. In the **Template Name** field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

7. In the **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 (a blue check), 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:

| Parameter Scope | Scope Description |
|---|---|
| **Device Specific**  | 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 template to a device .<br><br>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 .<br><br>To change the default key, type a new string and move the cursor out of the Enter Key box.<br><br>Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID. |

| | |
|---|---|
| **Global**  | Enter a value for the parameter, and apply that value to all devices.<br><br>Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs. |

## Basic Configuration

Click the Basic Configuration tab to configure the local autonomous system (AS) number for the template.

| Parameter Name | Description |
|---|---|
| **Autonomous System ID** * | Specify the local AS number.<br><br>*Range* : 1 -- 65,535<br>*Default* : No default |

### Equivalent CLI Commands

```
vpn vpn-id
   router
      eigrp name
         address-family ipv4 vrf vrf-name autonomous-system number
```

## IP4 Unicast Address Family

To configure the global EIGRP address family, click the **Unicast Address Family** tab.

### Redistribute tab

To redistribute routes from one protocol (routing domain) into a EIGRP routing domain, click **New Redistribute** and enter the following parameter values:

**Parameter Name**

**Value**

**Description**

**Mark as Optional Row**

Click **Optional** to mark this configuration as device-specific. To include this configuration for a device, enter the requested variable values when you attach a device template to a device, or create a template variables spreadsheet to apply the variables. See Create a Template Variables Spreadsheet .

**Protocol** *

Select the protocols from which to redistribute routes into EIGRP, for all EIGRP sessions.

**bgp**

Redistribute Border Gateway Protocol (BGP) routes into EIGRP.

**connected**

Redistribute connected routes into EIGRP.

**nat-route**

Redistribute network address translation (NAT) routes into EIGRP.

**omp**

Redistribute Overlay Management Protocol (OMP) routes into EIGRP.

**ospf**

Redistribute Open Shortest Path First (OSPF) routes into EIGRP.

**static**

Redistribute static routes into EIGRP.

**Route Policy** *

Enter the name of the route policy to apply to redistributed routes.

Click **Add** to save the redistribution information.

### Network tab

To advertise a prefix into the EIGRP routing domain, click the Network tab, and then click **New Network** and enter the following parameter values:

**Parameter Name**

**Description**

**Mark as Optional Row**

Click **Optional** to mark this configuration as device-specific. To include this configuration for a device, enter the requested variable values when you attach a device template to a device, or create a template variables spreadsheet to apply the variables. See Create a Template Variables Spreadsheet .

**Network Prefix** *

Enter the network prefix you want EIGRP to advertise in the format of *prefix/mask.*

Click **Add** to save the network prefix.

### Equivalent CLI Commands

```
vpn vpn-id
  router
    eigrp
      address-family ipv4-unicast
        maximum-paths paths number
        network prefix/mask
        redistribute (bgp | connected | nat-route | omp | ospf | static)
```

## Advanced Parameters

To configure advanced parameters for EIGRP, click the **Advanced** tab and configure the following parameter values:

| Parameter Name | Description |
|---|---|
| **Hold Time** (seconds) | Set the interval after which EIGRP considers a neighbor to be down. The local router then terminates the EIGRP session to that peer. This acts as the global hold time.<br><br>*Range* : 0 through 65535 seconds<br>*Default* : 15 seconds |
| **Hello Interval** (seconds) | Set the interval at which the router sends EIGRP hello packets.<br><br>*Range* : 0 to 65535 seconds<br>*Default* : 5 seconds |
| **Route Policy Name** | Enter the name of an EIGRP route policy. |

## Equivalent CLI Commands

```
vpn vpn-id
   router
      eigrp name
         address-family ipv4 vrf vrf-name autonomous-system number
            af-interface intf-name
               hello-interval seconds
               hold-time seconds
```

# Route Authentication Parameters

The IP Enhanced IGRP Route Authentication feature supports MD5 or HMAC-sha-256 authentication of routing updates from the EIGRP routing protocol. To configure authentication for EIGRP routes:

1. Click the Authentication tab
2. Click **Authentication** to open the Authentication Type field.
3. Select **Global** parameter scope.
4. From the drop-down list, select **md5** or **hmac-sha-256** .

Parameter

Option

Description

**MD5**

**MD5 Key ID**

Enter an MD5 key ID to compute an MD5 hash over the contents of the EIGRP packet using that value.

**MD5 Authentication Key**

Enter an MD5 authentication key to use an encoded MD5 checksum in the transmitted packet.

**HMAC SHA-256**

**Authentication Key**

A 256-byte unique piece of information that is used to compute the HMAC and is known both by the sender and the receiver of the message.

Click **Add** to save the authentication parameters.

**Note** : To use a preferred route map, specify both an MD5 key (ID or auth key) and a route map.

## Equivalent CLI Commands

```
vpn vpn-id
   router
      eigrp name
         address-family ipv4 vrf vrf-name autonomous-system number
            af-interface intf-name
               authentication key-chain keychain-name
               authentication mode {hmac-sha-256 | md5}
```

# Interface Parameters

To configure interface parameters for EIGRP routes, click the Interface tab, click **Interface** , and enter the following parameter values:

**Parameter Name**

**Description**

**Mark as Optional Row**

Click **Optional** to mark this configuration as device-specific. To include this configuration for a device, enter the requested variable values when you attach a device template to a device, or create a template variables spreadsheet to apply the variables. See Create a Template Variables Spreadsheet .

**Interface name**

Enter the interface name(s) on which EIGRP should run.

**Shutdown**

**No** (the default) enables the interface to run EIGRP.
**Yes** disables the interface.

Click **Add** to save the interfaces.

## Summary Addresses

To configure a summary IP address from the Interface tab:

1. Click **Interface** to open the Interface menu.
2. Click **Add Summary Address** .
3. If you have no configured summary addresses, click **Add Summary Address** from the pop-up message.
4. Enter the following parameters:

**Parameter Name**

**Description**

**Summary address prefix**

Enter the address prefix you want to apply to the summary address.

Click **Add** to add the summary address.

4. Click **Add** to save the interfaces.

Click **Save** to save the feature template.

## Equivalent CLI Commands

```
vpn vpn-id
   router
      eigrp name
         address-family ipv4 vrf vrf-name autonomous-system number
            af-interface intf-name
               summary-address prefix/mask
```

# VPN Interface Ethernet

Use the VPN Interface Ethernet template for all Viptela devices and Cisco IOS XE routers running the SD-WAN software.

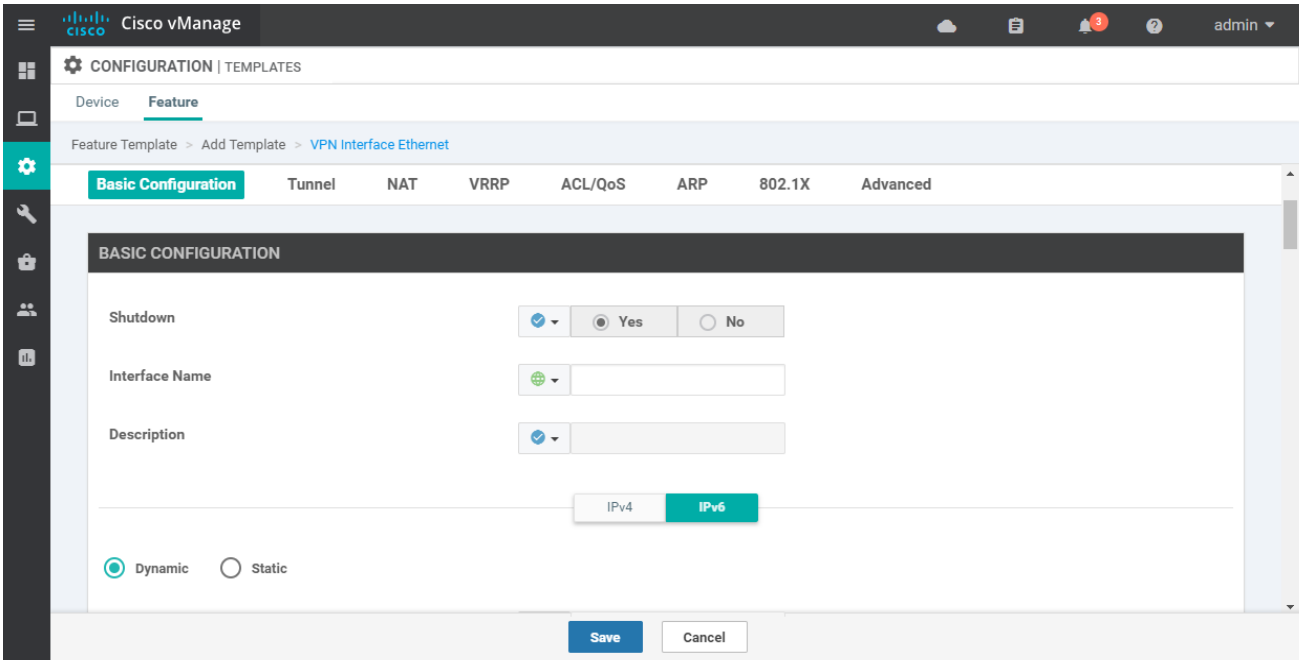
To configure the Ethernet interfaces in a VPN using vManage templates:

1. Create a VPN Interface Ethernet feature template to configure Ethernet interface parameters, as described in this article.
2. Create a VPN feature template to configure VPN parameters. See the VPN help topic.
3. Optionally, on vEdge routers, to enable DHCP server functionality on the interface, create a DHCP Server feature template. See the DHCP Server help topic.

## 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 template for VPN 0 or VPN 512:
   a. Click the Transport & Management VPN tab located directly beneath the Description field, or scroll to the Transport & Management VPN section.
   b. Under Additional VPN 0 Templates, located to the right of the screen, click VPN Interface.
   c. From the VPN Interface drop-down, click Create Template. The VPN Interface Ethernet template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN Interface Ethernet parameters.
6. To create a template for VPNs 1 through 511, and 513 through 65530:
   a. Click the Service VPN tab located directly beneath the Description field, or scroll to the Service VPN section.
   b. Click the Service VPN drop-down.
   c. Under Additional VPN templates, located to the right of the screen, click VPN Interface.

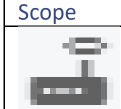
d. From the VPN Interface drop-down, click Create Template. The VPN Interface Ethernet template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN Interface Ethernet parameters.




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 (  ), 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:

| Parameter Scope | Scope Description |
|---|---|
|  Device Specific | 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** .<br><br>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 .<br><br>To change the default key, type a new string and move the cursor out of the Enter Key box.<br><br>Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID. |

| | |
|---|---|
| Global | Enter a value for the parameter, and apply that value to all devices.<br><br>Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs. |

## Configure Basic Interface Functionality

To configure basic interface functionality in a VPN, select the Basic Configuration tab and configure the following parameters. Parameters marked with an asterisk are required to configure an interface.

Parameter Name

IPv4 or IPv6

Options

Description

**Shutdown** *

Click **No** to enable the interface.

**Interface name** *

Enter a name for the interface.

For IOS XE routers, you must:

- Spell out the interface names completely (for example, GigabitEthernet0/0/0)
- Configure all the router's interfaces, even if you are not using them, so that they are configured in the shutdown state and so that all default values for them are configured.

**Description**

Enter a description for the interface.

**IPv4 / IPv6**

Click **IPv4** to configure an IPv4 VPN interface. Click **IPv6** to configure an IPv6 interface.

**Dynamic**

Click **Dynamic** to set the interface as a Dynamic Host Configuration Protocol (DHCP) client, so that the interface receives its IP address from a DHCP server.

**Both**

**DHCP Distance**

Optionally, enter an administrative distance value for routes learned from a DHCP server. Default is 1.

**IPv6**

**DHCP Rapid Commit**

Click **On** to.....WHAT?

Click **Off** to....What?

**Static**

Click **Static** to enter an IP address that doesn't change.

**IPv4**

**IPv4 Address**

Enter a static IPv4 address.

**IPv6**

**IPv6 Address**

Enter a static IPv6 address.

**Secondary IP Address**

**IPv4**

Click **Add** to enter up to four secondary IPv4 addresses for a service-side interface.

**IPv6 Address**

**IPv6**

Click **Add** to enter up to two secondary IPv6 addresses for a service-side interface.

**DHCP Helper**

**Both**

To designate the interface as a DHCP helper on a vEdge router, enter up to eight IP addresses, separated by commas, for DHCP servers in the network.  A DHCP helper interface forwards BootP (broadcast) DHCP requests that it receives from the specified DHCP servers.

**Block Non-Source IP**

**Yes** / **No**

Click **Yes** to have the interface forward traffic only if the source IP address of the traffic matches the interface's IP prefix range. Click **No** to allow other traffic.

**Bandwidth Upstream**

For vEdge routers and vManage NMSs:

For transmitted traffic, set the bandwidth above which to generate notifications.
*Range:* 1 through ($2^{32}$ / 2) – 1 kbps

**Bandwidth Downstream**

For vEdge routers and vManage NMSs:

For received traffic, set the bandwidth above which to generate notifications.
*Range:* 1 through ($2^{32}$ / 2) – 1 kbps

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

*CLI equivalent:*

```
vpn vpn-id
  interface interface-name
    bandwidth-downstream kbps
    bandwidth-upstream kbps
    block-non-source-ip
```

```
description text
dhcp-helper ip-address (on vEdge routers only)
(ip address ipv4-prefix/length| ip dhcp-client [dhcp-distance number])
(ipv6 address ipv6-prefix/length | ipv6 dhcp-client [dhcp-distance number] [dhcp-rapid-commit])
secondary-address ipv4-address
[no] shutdown
```

## Create a Tunnel Interface

On vEdge routers, you can configure up to four tunnel interfaces. This means that each vEdge router can have up to four TLOCs.

On vSmart controllers and vManage NMSs, you can configure one tunnel interface.

For the control plane to establish itself so that the overlay network can function, you must configure WAN transport interfaces in VPN 0.

To configure a tunnel interface, select the Interface Tunnel tab and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Tunnel Interface | Click On to create a tunnel interface. |
| Color | Select a color for the TLOC. |
| Control Connection (on vEdge routers) | If the vEdge router has multiple TLOCs, click No to have the tunnel not establish a TLOC. The default is On, which establishes a control connection for the TLOC. |
| Maximum Control Connections (on vEdge routers) | Specify the maximum number of vSmart controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0.<br><br>*Range:* 0 through 8<br>*Default:* 2 |
| vBond As Stun Server (on vEdge routers) | Click On to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the vEdge router is located behind a NAT. |
| Exclude Controller Group List (on vEdge routers) | Set the vSmart controllers that the tunnel interface is not allowed to connect to.<br>*Range:* 0 through 100 |
| vManage Connection Preference (on vEdge routers) | Set the preference for using a tunnel interface to exchange control traffic with the vManage NMS.<br>*Range:* 0 through 8<br>*Default:* 5 |
| Port Hop | Click On to enable port hopping, or click Off to disable it. If port hopping is enabled globally, you can disable it on an individual TLOC (tunnel interface). To control port hopping on a global level, use the System configuration template.<br>*Default:* Enabled (on vEdge routers); disabled (on vManage NMSs and vSmart controllers) |
| Low-Bandwidth Link (on vEdge routers) | Select to characterize the tunnel interface as a low-bandwidth link. |
| Allow Service | Select On or Off for each service to allow or disallow the service on the interface. |

To configure additional tunnel interface parameters, click Advanced Options:

| Parameter Name | Description |
|---|---|
| GRE (on vEdge routers) | Use GRE encapsulation on the tunnel interface. By default, GRE is disabled.<br><br>If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation. |

| | |
|---|---|
| IPsec (on vEdge routers) | Use IPsec encapsulation on the tunnel interface. By default, IPsec is enabled.<br><br>If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation. |
| IPsec Preference (on vEdge routers) | Specify a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value.<br><br>*Range:* 0 through 4294967295<br>*Default:* 0 |
| IPsec Weight (on vEdge routers) | Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel.<br><br>*Range:* 1 through 255<br>*Default:* 1 |
| Carrier | Select the carrier name or private network identifier to associate with the tunnel.<br><br>*Values:* carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default<br>*Default:* default |
| Bind Loopback Tunnel (on vEdge routers) | Enter the name of a physical interface to bind to a loopback interface. |
| Last-Resort Circuit (on vEdge routers) | Select to use the tunnel interface as the circuit of last resort. |
| NAT Refresh Interval | Enter the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection.<br>*Range:* 1 through 60 seconds<br>*Default:* 5 seconds |
| Hello Interval | Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection.<br>*Range:* 100 through 10000 milliseconds<br>*Default:* 1000 milliseconds (1 second) |
| Hello Tolerance | Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down.<br><br>*Range:* 12 through 60 seconds<br>*Default:* 12 seconds |

To save the feature template, click Save.

*CLI equivalent:*

```
vpn 0
  interface interface-name
    tunnel-interface
      allow-service service-name
      bind interface-name (on vEdge routers only)
      carrier carrier-name
      color color
      encapsulation (gre | ipsec) (on vEdge routers only)
        preference number
        weight number
      exclude-controller-group-list number (on vEdge routers only)
      hello-interval milliseconds
      hello-tolerance seconds
      last-resort-circuit (on vEdge routers only)
      low-bandwidth-link (on vEdge routers only)
      max-control-connections number (on vEdge routers only)
      nat-refresh-interval seconds
```

```
vbond-as-stun-server
vmanage-connection-preference number (on vEdge routers only)
```

## Configure the Interface as a NAT Device (on vEdge Routers)

To configure an interface to act as a NAT device for applications such as port forwarding, select the NAT tab, click On and configure the following parameters:

| Parameter Name | Description |
|---|---|
| NAT | Click On to have the interface act as a NAT device. |
| Refresh Mode | Select how NAT mappings are refreshed, either outbound or bidirectional (outbound and inbound).<br>*Default* : Outbound |
| UDP Timeout | Specify when NAT translations over UDP sessions time out.<br>*Range* : 1 through 65536 minutes<br>*Default* : 1 minutes |
| TCP Timeout | Specify when NAT translations over TCP sessions time out.<br>*Range* : 1 through 65536 minutes<br>*Default* : 60 minutes (1 hour) |
| Block ICMP | Select On to block inbound ICMP error messages. By default, a vEdge router acting as a NAT device receives these error messages.<br>*Default* : Off |
| Respond to Ping | Select On to have the vEdge router respond to ping requests to the NAT interface's IP address that are received from the public side of the connection. |

To create a port forwarding rule, click Add New Port Forwarding Rule and configure the following parameters. You can define up to 128 port-forwarding rules to allow requests from an external network to reach devices on the internal network.

| Parameter Name | Description |
|---|---|
| Port Start Range | Enter a port number to define the port or first port in the range of interest.<br>*Range:* 0 through 65535 |
| Port End Range | Enter the same port number to apply port forwarding to a single port, or enter a larger number to apply it to a range of ports.<br>*Range:* 0 through 65535 |
| Protocol | Select the protocol to which to apply the port-forwarding rule, either TCP or UDP. To match the same ports for both TCP and UDP traffic, configure two rules. |
| VPN | Specify the private VPN in which the internal server resides. This VPN is one of the VPN identifiers in the overlay network.<br>*Range:* 0 through 65530 |
| Private IP | Specify the IP address of the internal server to which to direct traffic that matches the port-forwarding rule. |

To save a port forwarding rule, click Add.

To save the feature template, click Save.

*CLI equivalent:*

```
vpn vpn-id
  interface interface-name
    nat
      block-icmp-error
```

```
port-forward port-start port-number1 port-end port-number2 proto (tcp | udp)
  private-ip-address ip-address private-vpn vpn-id
refresh (bi-directional | outbound)
respond-to-ping
tcp-timeout minutes
udp-timeout minutes
```

## Configure VRRP (on vEdge Routers)

To have an interface run the Virtual Router Redundancy Protocol (VRRP), which allows multiple routers to share a common virtual IP address for default gateway redundancy, select the VRRP tab. Then click Add New VRRP and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Group ID | Enter the virtual router ID, which is a numeric identifier of the virtual router. You can configure a maximum of 24 groups.<br>*Range:* 1 through 255 |
| Priority | Enter the priority level of the router. There router with the highest priority is elected as primary. If two vEdge routers have the same priority, the one with the higher IP address is elected as primary.<br>*Range:* 1 through 254<br>*Default:* 100 |
| Timer | Specify how often the VRRP primary sends VRRP advertisement messages. If subordinate routers miss three consecutive VRRP advertisements, they elect a new primary.<br>*Range:* 1 through 3600 seconds<br>*Default:* 1 second |
| Track OMP<br>Track Prefix List | By default, VRRP uses of the state of the service (LAN) interface on which it is running to determine which vEdge router is the primary virtual router. if a vEdge router loses all its WAN control connections, the LAN interface still indicates that it is up even though the router is functionally unable to participate in VRRP. To take WAN side connectivity into account for VRRP, configure one of the following:<br><br>Track OMP—Click On for VRRP to track the Overlay Management Protocol (OMP) session running on the WAN connection. If the primary VRRP router loses all its OMP sessions, VRRP elects a new default gateway from those that have at least one active OMP session.<br><br>Track Prefix List—Track both the OMP session and a list of remote prefixes, which is defined in a prefix list configured on the local router. If the primary VRRP router loses all its OMP sessions, VRRP failover occurs as described for the Track OMP option. In addition, if reachability to one of the prefixes in the list is lost, VRRP failover occurs immediately, without waiting for the OMP hold timer to expire, thus minimizing the amount of overlay traffic is dropped while the vEdge routers determine the VRRP primary. |
| IP Address | Enter the IP address of the virtual router. This address must be different from the configured interface IP addresses of both the local vEdge router and the peer running VRRP. |

*CLI equivalent:*

```
vpn vpn-id
  interface geslot/port[.subinterface]
    vrrp group-number
      ipv4 ip-address
      priority number
      timer seconds
      (track-omp | track-prefix-list list-name)
```

## Apply Access Lists and QoS Parameters (on vEdge Routers)

To configure a shaping rate to a router interface and to apply a QoS map, a rewrite rule, access lists, and policers to a router interface, select the ACL/QoS tab and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Shaping rate | Configure the aggregate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps). |
| QoS Map | Specify the name of the QoS map to apply to packets being transmitted out the interface. |
| Rewrite Rule | Click On, and specify the name of the rewrite rule to apply on the interface. |
| Ingress ACL – IPv4 | Click On, and specify the name of the access list to apply to IPv4 packets being received on the interface. |
| Egress ACL – IPv4 | Click On, and specify the name of the access list to apply to IPv4 packets being transmitted on the interface. |
| Ingress ACL – IPv6 | Click On, and specify the name of the access list to apply to IPv6 packets being received on the interface. |
| Egress ACL – IPv6 | Click On, and specify the name of the access list to apply to IPv6 packets being transmitted on the interface. |
| Ingress Policer | Click On, and specify the name of the policer to apply to packets received on the interface. |
| Egress Policer | Click On, and specify the name of the policer to apply to packets being transmitted on the interface. |

To save the feature template, click Save.

*CLI equivalent:*

```
vpn vpn-id
  interface interface-name
    access-list acl-list (in | out)
    policer policer-name (in |out)
    qos-map name
    rewrite-rule name
    shaping-rate name
```

## Add ARP Table Entries

To configure static Address Resolution Protocol (ARP) table entries on the interface, select the ARP tab. Then click Add New ARP and configure the following parameters:

| Parameter Name | Description |
|---|---|
| IP Address | Enter the IP address for the ARP entry in dotted decimal notation or as a fully qualified host name. |
| MAC Address | Enter the MAC address in colon-separated hexadecimal notation. |

To save the ARP configuration, click Add.

To save the feature template, click Save.

*CLI equivalent:*

```
vpn vpn-id
  interface interface-name
    arp
      ip ip-address mac mac-address
```

## Configure IEEE 802.1X Authentication for WANs

To configure IEEE 802.1X authentication for WANs on the interface, select the 802.1X tab, and click On:

| Parameter Name | Description |
|---|---|
| 802.1X | Click On to enable IEEE 802.1X on the interface. |
| RADIUS Server | Enter the tag of the RADIUS server to use for 802.1X authentication. It can be from 4 through 16 characters long. You configure the tag in the **AAA feature template** . |
| Account Interim Interval | Enter how often to send 802.1X interim accounting updates to the RADIUS server.<br>*Range:* 0 through 7200 seconds<br>*Default:* 0 (no interim accounting updates are sent) |
| NAS Identifier | Enter the NAS identifier of the local router. It can be a string from 1 to 255 characters long. This identifier is sent to the RADIUS server. |
| NAS IP | Enter the NAS IP address of the local router. This address is sent to the RADIUS server. |
| Wake On LAN | Enable a client to be powered up when the router receives an Ethernet magic packet frame. |
| Control Direction | Select how an 802.1X interface that is using wake on LAN handles packets from unauthorized clients:<br>• In and Out—Send and receive packets with unauthorized clients. This is the default<br>• In Only—Send but do not receive packets with unauthorized clients. |
| Reauthentication | Enter how often to reauthenticate 802.1X clients. By default, no reauthentication attempts are made after the initial LAN access request.<br>*Range:* 0 through 1440 minutes |
| Inactivity | Enter how long to wait before revoking an 802.1X client's network access.<br>*Range:* 0 through 1440 minutes (24 hours)<br>*Default:* 60 minutes (1 hour) |
| Host Mode | Select whether an 802.1X interface grants access to a single client or to multiple clients:<br>• Multi Auth—Grant access to one client on a voice VLAN and multiple clients on data VLANs.<br>• Multi Host—Grant access to multiple clients<br>• Single Host—Grant access only to the first authenticated client. This is the default. |

To configure other IEEE 802.1X authentication properties, click Advanced Options and configure the following parameters:

Parameter Name

Description

Authentication Order

Set the order of authentication methods to use when authenticating devices for connection to the 802.1X WAN. The default authentication order is RADIUS, then MAC authentication bypass (MAB).

**VLAN**

Authentication Fail VLAN

Configure network access when RADIUS authentication or the RADIUS server fails. An authentication-fail VLAN is similar to a critical VLAN.

Guest VLAN

Configure a guest VLAN to provide limited services 50 802.1X–compliant clients.

Authentication Reject VLAN

Configure limited services to 802.1X–compliant clients that failed RADIUS authentication. An authentication-reject VLAN is similar to a restricted VLAN.

Default VLAN

Configure network access for 802.1X–compliant clients that are successfully authenticated by the RADIUS server. If you do not configure a default VLAN on the router, successfully authenticated clients are placed into VLAN 0, which is the VLAN associated with an untagged bridge.

**Dynamic Authentication Server**

DAS Port

Configure the UDP port number to listen for CoA requests from the RADIUS server.
*Range:* 1 through 65535
*Default:* 3799

Client

Set the IP address of the RADIUS or other authentication server from which to accept CoA requests.

Secret Key

Set the password that the RADIUS or other authentication server uses to access the router's 802.1X interface.

Time Window

Set how long a CoA request is valid.
*Range:* 0 through 1000 seconds
*Default:* 300 seconds (5 minutes)

Require Timestamp

Enable to require the DAS client to timestamp CoA messages.

VPN

Set the VPN through which the RADIUS or other authentication server is reachable.

**MAC Authentication Bypass**

Server

Select to enable MAC authentication bypass (MAB) on the RADIUS server and to authentication non-802.1X–compliant clients using a RADIUS server.

Allow

Specify the MAC addresses of one or more devices so that authentication checks for these devices are performed using the RADIUS server.

**Request Attributes**

Authentication

Click Authentication, then click Add New Authentication Entry to configure RADIUS authentication attribute–value (AV) pairs to send to the RADIUS server during an 802.1X session.

To save the entry, click Add.

Accounting

Click Accounting, then click Add New Accounting Entry to configure RADIUS accounting attribute–value (AV) pairs to send to the RADIUS server during an 802.1X session.

To save the entry, click Add.

To save the feature template, click Save.

*CLI equivalent:*

```
vpn 0
  interface interface-name
    dot1x
      accounting-interval minutes
      acct-req-attr attribute-number (integer integer | octet octet | string string)
      auth-fail-vlan vlan-id
      auth-order (mab | radius)
      auth-reject-vlan vlan-id
      auth-req-attr attribute-number (integer integer | octet octet | string string)
      control-direction direction
      das
        client ip-address
        port port-number
        require-timestamp
        secret-key password
        time-window seconds
        vpn vpn-id
      default-vlan vlan-id
      guest-vlan vlan-id
      host-mode (multi-auth | multi-host | single-host)
      mac-authentication-bypass
        allow mac-addresses
        server
      nas-identifier string
      nas-ip-address ip-address
      radius-servers tag
      reauthentication minutes
      timeout
        inactivity minutes
      wake-on-lan
```

## Configure Other Interface Properties

To configure other interface properties, select the Advanced tab and configure the following parameters:

| Parameter Name | Description |
|---|---|
| Duplex | Choose full or half to specify whether the interface runs in full-duplex or half-duplex mode.<br>*Default:* full |
| MAC Address | Specify a MAC address to associate with the interface, in colon-separated hexadecimal notation. |
| IP MTU | Specify the maximum MTU size of packets on the interface.<br>*Range:* 576 through 1804<br>*Default:* 1500 bytes |
| PMTU Discovery | Click On to enable path MTU discovery on the interface. PMTU determines the largest MTU size that the interface supports so that packet fragmentation does not occur. |

| | |
|---|---|
| Flow Control | Select a setting for bidirectional flow control, which is a mechanism for temporarily stopping the transmission of data on the interface.<br>*Values:* autonet, both, egress, ingress, none<br>*Default:* autoneg |
| TCP MSS | Specify the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented.<br>*Range:* 552 to 1460 bytes<br>*Default:* None |
| Speed | Specify the speed of the interface, for use when the remote end of the connection does not support autonegotiation.<br>*Values:* 10, 100, or 1000 Mbps<br>*Default:* Autonegotiate (10/100/1000 Mbps) |
| Clear-Dont-Fragment | Click On to clear the Don't Fragment (DF) bit in the IPv4 packet header for packets being transmitted out the interface. When the DF bit is cleared, packets larger than that interface's MTU are fragmented before being sent. |
| Static Ingress QoS (on vEdge routers) | Specify a queue number to use for incoming traffic.<br>*Range:* 0 through 7 |
| ARP Timeout (on vEdge routers) | Specify how long it takes for a dynamically learned ARP entry to time out.<br>*Range:* 0 through 2678400 seconds (744 hours)<br>*Default:* 1200 (20 minutes) |
| Autonegotiation | Click Off to turn off autonegotiation. By default, an interface runs in autonegotiation mode. |
| TLOC Extension | Enter the name of a physical interface on the same router that connects to the WAN transport. This configuration then binds this service-side interface to the WAN transport. A second router at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN.<br><br>Note that TLOC extension over L3 is only supported for Cisco IOS XE routers. If configuring TLOC extension over L3 for a Cisco IOS XE router, enter the IP address of the L3 interface. |
| Power over Ethernet (on vEdge 100m and vEdge 100wm routers) | Click On to enable PoE on the interface. |
| Tracker (on vEdge routers) | Enter the name of a tracker to track the status of transport interfaces that connect to the internet. |
| ICMP Redirect (on vEdge routers) | Click Disable to disable ICMP redirect messages on the interface. By default, an interface allows ICMP redirect messages. |
| GRE Tunnel Source IP (on IOS XE routers) | Enter the IP address of the extended WAN interface. |
| Xconnect (on IOS XE routers) | Enter the name of a physical interface on the same router that connects to the WAN transport. |

*CLI equivalent:*

```
vpn vpn-id
  interface interface-name
    arp-timeout seconds (on vEdge routers only)
    [no] autonegotiate
    clear-dont-fragment
    duplex (full | half)
    flow-control control
    icmp-redirect-disable (on vEdge routers only)
    mac-address mac-address
```

```
mtu bytes
pmtu
pppoe-client (on vEdge 100m and vEdge 100wm routers only)
  ppp-interface pppnumber
speed speed
static-ingress-qos number (on vEdge routers only)
tcp-mss-adjust bytes
tloc-extension interface-name (on vEdge routers only)
tracker tracker-name (on vEdge routers only)
```

## Release Information

Introduced in vManage NMS Release 15.2.
In Release 17.2.2, add support for tracker interface status.
In Release 18.2, add support for disabling ICMP redirect messages.

## Security Overview

***Security*** is a critical element of today's networking infrastructure. Network administrators and security officers are hard pressed to defend their network against attacks and breaches. As a result of hybrid clouds and remote employee connectivity, the security perimeter around networks is disappearing. There are multiple problems with the traditional ways of securing networks, including:

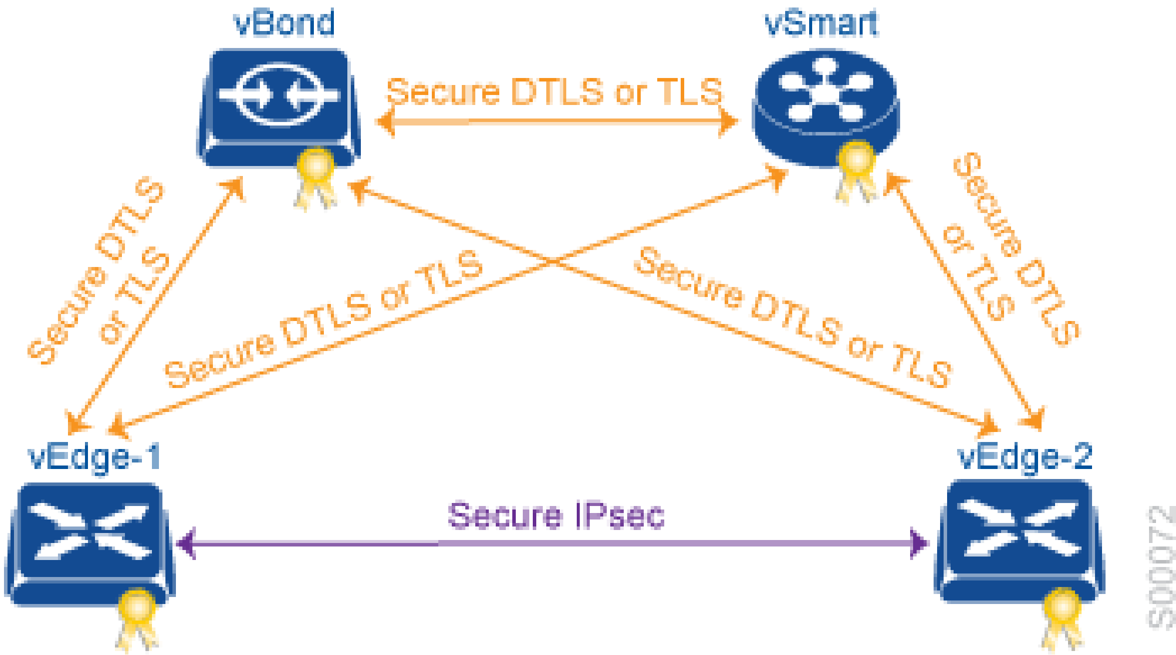
- Very little emphasis is placed on ensuring the authenticity of the devices involved in the communication.
- Securing the links between a pair of devices involves tedious and manual setup of keys and shared passwords.
- Scalability and high availability solutions are often at odds with each other.

## Viptela Security Components

The Viptela solution takes a fundamentally different approach to security, basing its core design around the following precepts:

- Authentication—The solution ensures that only authentic devices are allowed to send traffic to one another.
- Encryption—All communication between each pair of devices is automatically secure, completely eliminating the overhead involved in securing the links.
- Integrity—No group keys or key server issues are involved in securing the infrastructure.

These three components—authentication, encryption, and integrity—are key to securing the Viptela overlay network infrastructure.




The articles on Control Plane Security Overview and Data Plane Security Overview examine how authentication, encryption, and integrity are implemented throughout the Viptela overlay network. The security discussion refers to the following illustration of the components of the Viptela network—the vSmart controller, the vBond orchestrator, and the vEdge routers. The connections between these devices form the control plane (in orange) and the data plane (in purple), and it is these connections that need to be protected by appropriate measures to ensure the security of the network devices and all network traffic.

## Security Provided by NAT Devices

While the primary purpose of NAT devices is to allow devices with private IP addresses in a local-area network (LAN) to communicate with devices in public address spaces, such as the Internet, NAT devices also inherently provide a level of security, functioning as hardware firewalls to prevent unwanted data traffic from passing through the Viptela edge routers and to the LAN networks in the service-side networks connected to the vEdge router.

To enhance the security at branch sites, you can place the vEdge router behind a NAT device. The vEdge router can interact with NAT devices configured with the following Session Traversal Utilities for NAT (STUN) methods, as defined in RFC 5389 :

- Full-cone NAT, or one-to-one NAT—This method maps an internal address and port pair to an external address and port. Any external host can send packets to LAN devices behind the vEdge router by addressing them to the external address and port.
- Address-restricted cone NAT, or restricted-cone NAT—This method also maps an internal address and port to and external address and port. However, an external host can send packets to the internal device only if the external address (and any port at that address) has received a packet from the internal address and port.
- Port-restricted cone NAT—This method is a stricter version of restricted-cone NAT, in which an external host can send packets to the internal address and port only if the external address and port pair has received a packet from that internal address and port. The external device must send packets from the specific port to the specific internal port.
- Symmetric NAT—With this method, each request from the same internal IP address and port to an external IP address and port is mapped to a unique external source IP address and port. If the same internal host sends a packet with the same source address and port but to a different destination, the NAT device creates a different mapping. Only an external host that receives a packet from an internal host can send a packet back. vEdge routers support symmetric NAT only on one side of the WAN tunnel. That is, only one of the NAT devices at either end of the tunnel can use symmetric NAT.
  When a vEdge router operates behind a NAT device running symmetric NAT, only one of the NAT devices at either end of the tunnel can

use symmetric NAT. The vEdge router that is behind a symmetric NAT cannot establish a BFD tunnel with a remote vEdge router that is behind a symmetric NAT, an address-restricted NAT, or a port-restricted NAT.
To allow a vEdge router to function behind a symmetric NAT, you must configure the vManage NMS and vSmart controller control connections to use TLS. DTLS control connections do not work through a symmetric NAT.

## Security for Connections to External Devices

Viptela vEdge routers can use the standards-based Internet Key Exchange (IKE) protocol when establishing IPsec tunnels between a device within the overlay network and a device that is external to the overlay network, such as a cloud-hosted service or a remote user. The Viptela software supports IKE version 2, which performs mutual authentication and establishes and maintains security associations (SAs). IPsec provides confidentiality, data integrity, access control, and data source authentication for the traffic being exchanged over the IPsec tunnel.

## Additional Information

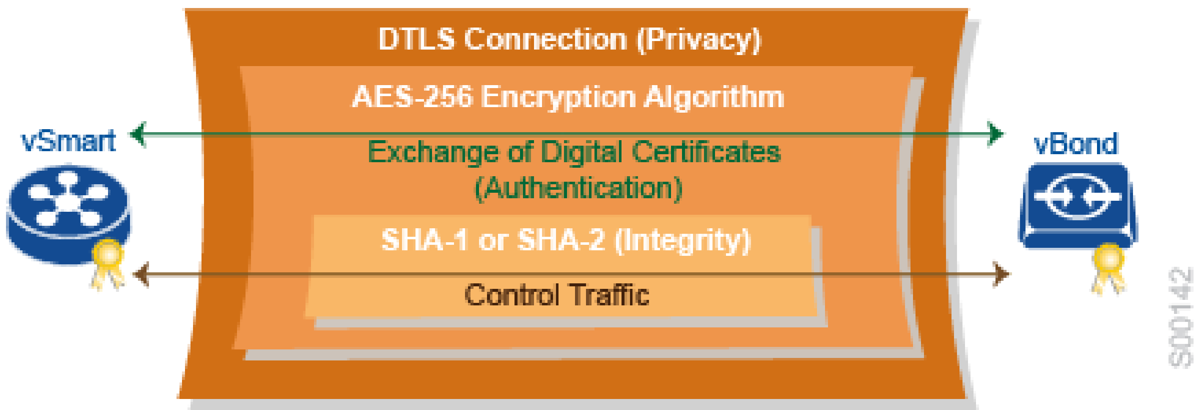
Configuring Security Parameters
Configuring IKE
Control Plane Security Overview
Data Plane Security Overview

## Control Plane Security Overview

The control plane of any network is concerned with determining the network topology and defining how to direct packets. In a traditional network, the control plane operations of building and maintaining routing and forwarding tables and directing packets towards their destination are handled by routing and switching protocols, which typically offer few or no mechanisms for authenticating devices or for encrypting routing updates and other control information. In addition, the traditional methods for providing security are highly manual and do not scale. As examples, certificates are typically installed manually rather than in an automated fashion, and using preshared keys is not a very secure approach for providing device security.

The Viptela control plane has been designed with network and device security in mind. The foundation of the control plane is one of two security protocols derived from SSL (Secure Sockets Layer)—the Datagram Transport Layer Security (DTLS) protocol and the Transport Layer Security (TLS) protocol. The vSmart controller, which is the centralized brain of the Viptela solution, establishes and maintains DTLS or TLS connections to all Viptela devices in the overlay network: to the vEdge routers, the vBond orchestrators, to vManage NMSs, and to other vSmart controllers. These connections carry control plane traffic. DTLS or TLS provides communication privacy between Viptela devices in the network, using the Advanced Encryption Standard (AES-256) encryption algorithm to encrypt all control traffic sent over the connections.

The privacy and encryption in the control plane offered by DTLS and TLS provide a safe and secure foundation for the other two security components, authentication and integrity. To perform authentication, the Viptela devices exchange digital certificates. These certificates, which are either installed by the software or hard-coded into the hardware, depending on the device, identify the device and allow the devices themselves to automatically determine which ones belong in the network and which are imposters. For integrity, the DTLS or TLS connections run SHA-1 or SHA-2, a cryptographic secure hash algorithm which ensures that all control and data traffic sent over the connections has not been tampered with.




The following are the control plane security components, which function in the privacy provided by DTLS or TLS connections:

- **AES-256** encryption algorithm provides encryption services.
- **Digital certificates** are used for authentication.
- **SHA-1 or SHA-2** is responsible for ensuring integrity.

## DTLS and TLS Infrastructure

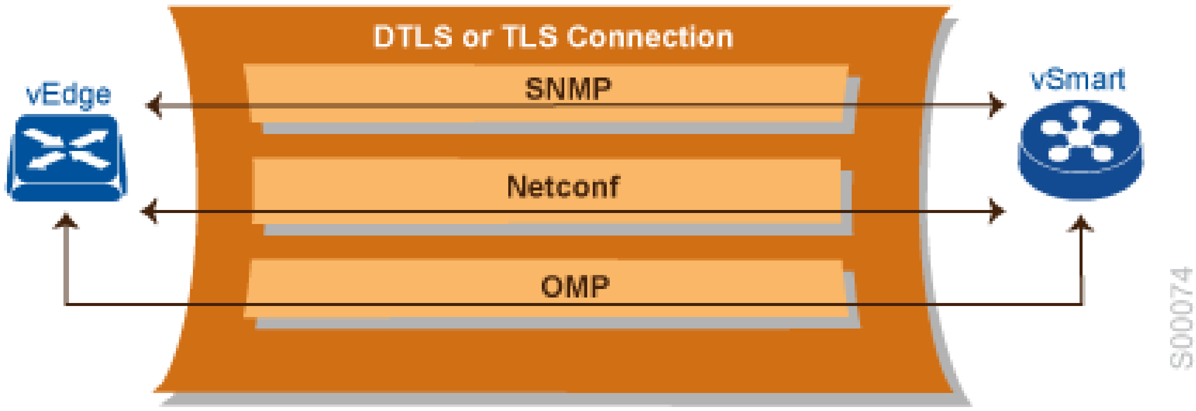
Security protocols derived from SSL provide the foundation for the Viptela control plane infrastructure.

The first is the DTLS protocol, which is a transport privacy protocol for connectionless datagram protocols such as UDP, provides the foundation for the Viptela control plane infrastructure. It is based on the stream-oriented Transport Layer Security (TLS) protocol, which provides security for TCP-based traffic. (TLS itself evolved from SSL.) The Viptela infrastructure design uses DTLS running over UDP to avoid some of the issues with TCP, including the delays associated with stream protocols and some security issues. However, because UDP performs no handshaking and sends no acknowledgments, DTLS has to handle possible packet re-ordering, loss of datagrams, and data larger than the datagram packet size.

The control plane infrastructure can also be configured to run over TLS. This might be desirable in situations where the protections of TCP outweigh its issues. For example, firewalls generally offer better protection for TCP servers than for UDP servers.

The Viptela software implements the standard version of DTLS with UDP, which is defined in RFC 6347 . DTLS for use with other protocols is defined in a number of other RFCs . For TLS, the Viptela software implements the standard version defined in RFC 5246 .


In the Viptela architecture, the Viptela devices use DTLS or TLS as a tunneling protocol, which is an application-level (Layer 4) tunneling protocol. When the vSmart controllers, vBond orchestrators, vManage NMSs, and vEdge routers join the network, they create provisional DTLS or TLS tunnels between them as part of the device authentication process. After the authentication process completes successfully, the provisional tunnels between the vEdge routers and vSmart controllers, and those between the vBond orchestrators and vSmart controllers, become permanent and remain up as long as the devices are active in the network. It is these authenticated, secure DTLS or TLS tunnels that are used by all the protocol applications running on the Viptela devices to transport their traffic. For example, an OMP session on a vEdge router communicates with an OMP session on a vSmart controller by sending plain IP traffic through the secure DTLS or TLS tunnel between the two devices. (The Overlay Management Protocol is the Viptela control protocol used to exchange routing, policy, and management information among Viptela devices, as described in [Overlay Routing Overview](#) .)




A Viptela daemon running on each vSmart controller and vEdge router creates and maintains the secure DTLS or TLS connections between the devices. This daemon is called vdaemon and is discussed later in this article. After the control plane DTLS or TLS connections are established between these devices, multiple protocols can create sessions to run and route their traffic over these connections—including OMP, Simple Network Management Protocol (SNMP), and Network Configuration Protocol (Netconf)—without needing to be concerned with any security-related issues. The session-related traffic is simply directed over the secure connection between the vEdge routers and vSmart controllers.

## Control Plane Authentication

The Viptela control plane uses digital certificates with 2048-bit RSA keys to authenticate the Viptela devices in the network. The digital certificates are created, managed, and exchanged by standard components of the public key infrastructure, or PKI:

- **Public keys** —These keys are generally known.
- **Private keys** —These keys are private. They reside on each Viptela device and cannot be retrieved from the device.
- **Certificates** signed by a root certification authority (CA)—The trust chain associated with the root CA needs to be present on all Viptela devices.

In addition to standard PKI components, the Viptela device serial numbers and the vEdge router chassis numbers are used in the authentication processes.

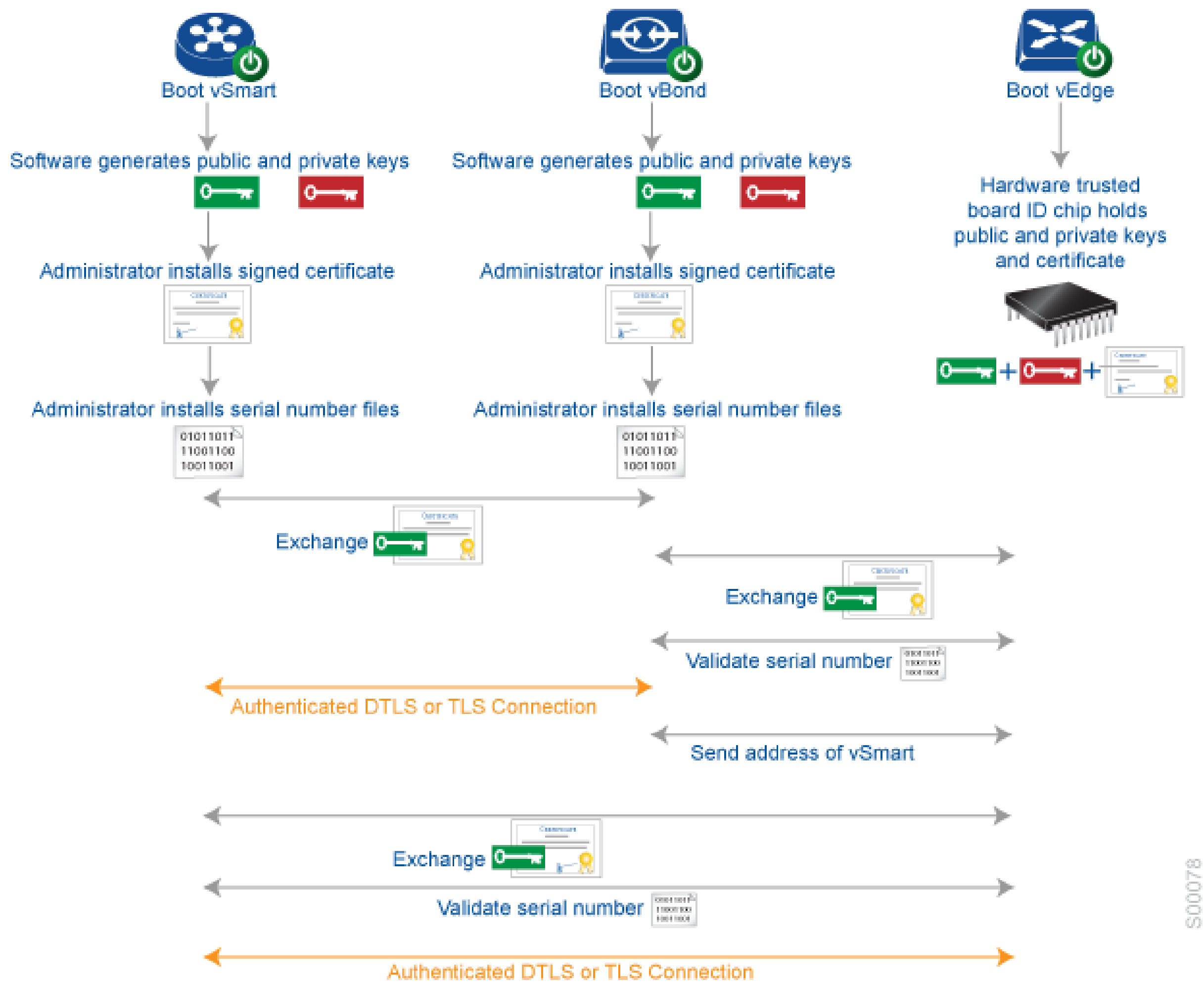
Let's first look at the PKI components that are involved in device authentication. On vEdge routers, the public and private keys and the certificates are managed automatically, by a Trusted Board ID chip that is built into the router. When the routers are manufactured, this chip is programmed with a signed certificate, which includes the device's public key and its serial number, and the device's private key. When the vEdge routers boot up and join the network, they exchange their certificates (including the device's public key and serial number) with other Viptela devices as part of the device authentication process. For networks with thousands or tens of thousands of vEdge routers, providing an automated process for managing keys and certificates greatly simplifies the task of maintaining security across the edge devices in the network. (Note that the vEdge router's private key always remains embedded in the router's Trusted Board ID chip, and it is never distributed, nor can it ever be retrieved from the device. In fact, any brute-force attempt to read the private key causes the Trusted Board ID chip to fail, thereby disabling all access to the router.)

For vSmart controllers, vBond orchestrators, and vManage NMS systems, the public and private keys and the certificates are managed manually. When you boot these devices for the first time, the Viptela software generates a unique private key–public key pair for each software image. The public key needs to be signed by the CA root. The network administrator then requests a signed certificate and manually installs it and the certificate chains on the vSmart controllers, vBond orchestrators, and vManage NMS systems. A typical network might have only a small handful of vSmart controllers, vBond orchestrators, and vManage NMSs, so the burden of manually managing the keys and certificates on these devices is small.

To augment these standard PKI components, the Viptela software uses the device serial numbers in performing automatic device authentication. Specifically, it uses the vEdge and vSmart serial numbers and the vEdge chassis numbers. When a batch of vEdge routers is shipped, the manufacturer sends a text file that lists the serial numbers of the vEdge routers and the corresponding chassis numbers. For the vSmart controllers, when the network administrator receives the signed certificate, they should extract the serial numbers from the certificates and place them into a single text file, one serial number per line. Then the network administrator manually installs these two files. The file received from the manufacturer that lists all valid vEdge serial and chassis numbers is uploaded and installed on vSmart controllers. Both the vEdge authorized serial number file and the file listing the vSmart serial numbers are uploaded and installed on vBond orchestrators. Then, during the automatic authentication process, as pairs of devices are establishing DTLS control connections between them, each device compares the serial numbers (and for vEdge routers, the chassis numbers) to those in the files installed on the device. A devices allows a connection to be established only if the serial number or serial–chassis number combination (for a vEdge router) matches.

You can display the installed vSmart authorized serial numbers using the **show control valid-vsmarts** command on a vSmart controller or a vEdge router and the **show orchestrator valid-vsmarts** command on a vBond orchestrator. You can display the installed vEdge authorized serial and chassis number associations using the **show control valid-vedges** command on a vSmart controller and the **show orchestrator valid-devices** command on a vBond orchestrator

Now, let's look at how the PKI authentication components and the device serial and chassis numbers are used to authenticate devices on the Viptela overlay network. When vSmart controllers, vBond orchestrators, and vEdge routers first boot up, they establish secure DTLS or TLS connections between them. Over these connections, the devices authenticate each other, using the public and private keys, the signed certificates, and the device serial numbers and performing a series of handshake operations to ensure that all the devices on the network are valid and not imposters. The following figure illustrates the key and certificate exchange that occurs when the Viptela devices boot. For details about the authentication that occurs during the bringup process, see Bringup Sequence of Events .




## Control Plane Encryption

Control plane encryption is done by either DTLS, which is based on the TLS protocol, or TLS. These protocol encrypt the control plane traffic that is sent across the connections between Viptela devices to validate the integrity of the data. TLS uses asymmetric cryptography for authenticating key exchange, symmetric encryption for confidentiality, and message authentication codes for message integrity.

A single Viptela device can have DTLS or TLS connections to multiple Viptela devices, so vdaemon creates a kernel route for each destination. For example, a vEdge router would typically have one kernel route, and hence one DTLS or TLS connection, for each vSmart controller. Similarly, a vSmart controller would have one kernel route and one DTLS or TLS connection for each vEdge router in its domain.

## Control Plane Integrity

The Viptela design implements control plane integrity by combining two security elements: SHA-1 or SHA-2 message digests, and public and private keys.

SHA-1 and SHA-2 are cryptographic hash functions that generate message digests (sometimes called simply digests) for each packet sent over a control plane connection. SHA-1 generates a 160-bit message digest. SHA-2 is a family that consists of six hash functions with digests that are 224, 256, 384, or 512 bits. The receiver then generates a digest for the packet, and if the two match, the packet is accepted as valid. Both SHA-1 and SHA-2 allow verification that the packet's contents have not been tampered with.

The second component of control plane integrity is the use of public and private keys. When a control plane connection is being established, a local Viptela device sends a challenge to a remote device. The remote device encrypts the challenge by signing it with its private key, and returns the signed challenge to the local device. The local device then uses the remote device's public key to verify that the received challenge matches the sent challenge.

Then, once a control plane connection is up, keys are used to ensure that packets have been sent by a trusted host and were not inserted midstream by an untrusted source. The authenticity of each packet is verified through encryption and decryption with symmetric keys that were exchanged during the process of establishing the control connection.

## Additional Information

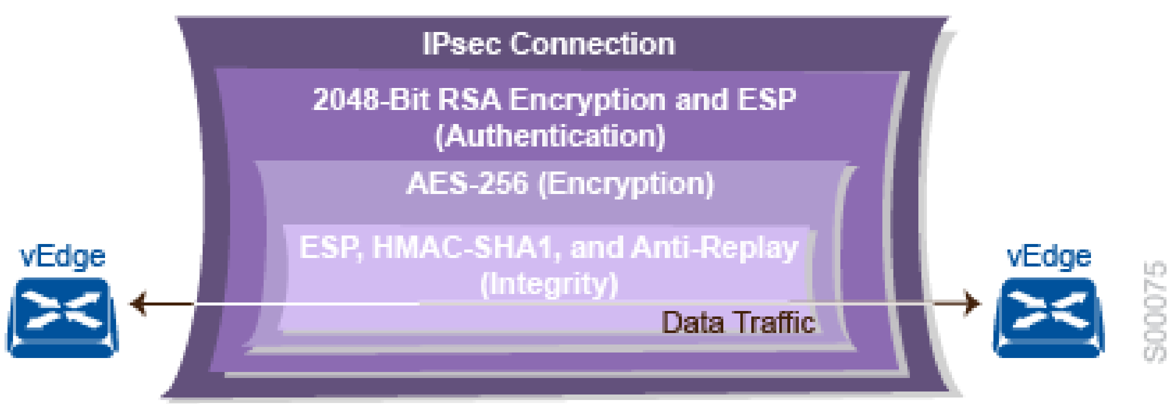
[Bringup Sequence of Events](#)
[Configuring Security Parameters](#)
[Data Plane Security Overview](#)
[Security Overview](#)

## Data Plane Security Overview

The data plane of any network is responsible for handling data packets that are transported across the network. (The data plane is also sometimes called the forwarding plane.) In a traditional network, data packets are typically sent directly over the Internet or another type of public IP cloud, or they could be sent through MPLS tunnels. If the vEdge routers in the Viptela overlay network were to send traffic over a public IP cloud, the transmission would be insecure. Anyone would be able to sniff the traffic, and it would be easy to implement various types of attacks, including man-in-the-middle (MITM) attacks.

The underlying foundation for security in the Viptela data plane is the security of the control plane. Because the control plane is secure—all devices are validated, and control traffic is encrypted and cannot be tampered with—we can be confident in using routes and other information learned from the control plane to create and maintain secure data paths throughout a network of vEdge routers.

The data plane provides the infrastructure for sending data traffic among the vEdge routers in the Viptela overlay network. Data plane traffic travels within secure Internet Security (IPsec) connections. The Viptela data plane implements the key security components of authentication, encryption, and integrity in the following ways:




- **Authentication** —As mentioned above, the Viptela control plane contributes the underlying infrastructure for data plane security. In addition, authentication is enforced by two other mechanisms:

- RSA encryption with 2048-bit keys.
- Two standard protocols from the IPsec security suite framework, Encapsulation Security Payload (ESP) and Authentication Header (AH), are used to authenticate the origin of data traffic.

- **Encryption** —The standard ESP protocol protects the data packet's payload, and the standard AH protocol protects both the payload and the non-mutable header fields. Key exchange encryption is done using the AES-256 cipher.
- **Integrity** —To guarantee that data traffic is transmitted across the network without being tampered with, the data plane implements several mechanisms from the IPsec security protocol suite:
  - The ESP protocol encapsulates the payload of data packets.
  - The HMAC-SHA1 algorithm, which is used by the IPsec AH protocol, combines a keyed-hash authentication code with SHA-1 cryptography to ensure data integrity. AH encapsulates the non-mutable fields in the outer IP header and the payload of data packets. You can configure the integrity methods supported on each vEdge router, and this information is exchanged in the router's TLOC properties. If two vEdge peers advertise different authentication types, they negotiate the type to use, choosing the strongest method.
  - The anti-replay scheme protects against attacks in which an attacker duplicates encrypted packets.

## Data Plane Authentication and Encryption

Before a pair of vEdge routers can exchange data traffic, they establish an IPsec connection between them, which they use as a secure communications channel, and then the routers authenticate each other over this connection. As with the control plane, the data plane uses keys to perform Viptela device authentication.

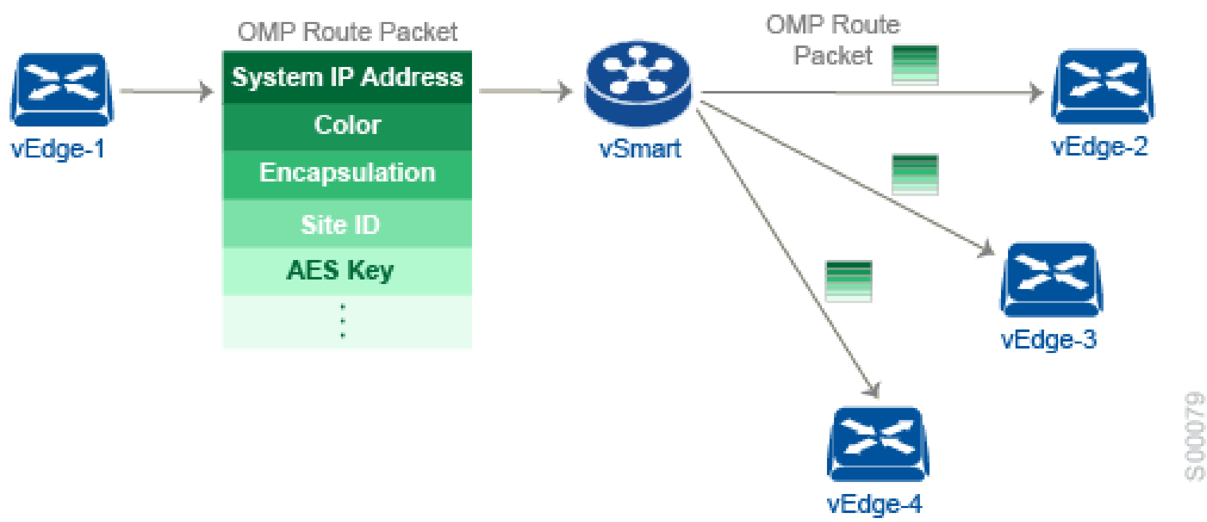
In a traditional IPsec environment, key exchange is handled by the Internet Key Exchange (IKE) protocol. IKE first sets up secure communications channels between devices and then establishes security associations (SAs) between each pair of devices that want to exchange data. IKE uses a Diffie-Hellman key exchange algorithm to generate a shared key that encrypts further IKE communication. To establish SAs, each device (n) exchanges keys with every other device in the network and creates per-pair keys, generating a unique key for each remote device. This scheme means that in a fully meshed network, each device has to manage $n^2$ key exchanges and (n-1) keys. As an example, in a 1,000-node network, 1,000,000 key exchanges are required to authenticate the devices, and each node is responsible for maintaining and managing 999 keys.

The discussion in the previous paragraph points out why an IKE-style key exchange does not scale as network size increases and why IKE could be a bottleneck in starting and in maintaining data exchange on a large network:

- The handshaking required to set up the communications channels is both time consuming and resource intensive.
- The processing required for the key exchange, especially in larger networks, can strain network resources and can take a long time.

The Viptela implementation of data plane authentication and encryption establishes SAs between each pair of devices that want to exchange data, but it dispenses with IKE altogether. Instead, to provide a scalable solution to data plane key exchange, the Viptela solution takes advantage of the fact that the DTLS control plane connections in the Viptela overlay network are known to be secure. Because the Viptela control plane establishes authenticated, encrypted, and tamperproof connections, there is no need in the data plane to set up secure communications channels to perform data plane authentication.

In the Viptela network, data plane encryption and key generation are done by AES-256, a symmetric-key algorithm that uses the same key to encrypt outgoing packets and to decrypt incoming packets. Each vEdge router periodically generates an AES key for its data path (specifically, one key per TLOC) and transmits this key to the vSmart controller in OMP route packets, which are similar to IP route updates. These packets contain information that the vSmart controller uses to determine the network topology, including the vEdge router's TLOC (a tuple of the system IP address and traffic color) and AES key. The vSmart controller then places these OMP route packets into reachability advertisements that it sends to the other vEdge routers in the network. In this way, the AES keys for all the vEdge routers are distributed across the network. Even though the key exchange is symmetric, Viptela devices use it in an asymmetric fashion. The result is a simple and scalable key exchange process that does not use per-pair keys.




If control policies configured on a vSmart controller limit the communications channels between network devices, the reachability advertisements sent by the vSmart controller contain information only for the vEdge routers that they are allowed to exchange data with. So, a vEdge router learns the keys only for those vEdge routers that they are allowed to communicate with.

To further strengthen data plane authentication and encryption, vEdge routers regenerate their AES keys aggressively (by default, every 24 hours). Also, the key regeneration mechanism ensures that no data traffic is dropped when keys change.

In the Viptela overlay network, the liveness of SAs between vEdge router peers is tracked by monitoring BFD packets, which are periodically exchanged over the IPsec connection between the peers. IPsec relays the connection status to the vSmart controllers. If data connectivity between two peers is lost, the exchange of BFD packets stops, and from this, the vSmart controller learns that the connection has been lost.

The Viptela IPsec software has no explicit SA idle timeout, which specifies the time to wait before deleting SAs associated with inactive peers. Instead, an SA remains active as long as the IPsec connection between two vEdge routers is up, as determined by the periodic exchange of BFD packets between them. Also, the frequency with which SA keys are regenerated obviates the need to implement an implicit SA idle timeout.

In summary, the Viptela data plane authentication offers the following improvements over IKE:

- Because only n +1 keypaths are required rather than the $n^2$ required by IKE, the Viptela solution scales better as the network grows large.
- Keys are generated and refreshed locally, and key exchange is performed over a secure control plane.
- No key server is required, and thus there is no need to worry about high availability requirements of a key server.

## Data Plane Integrity

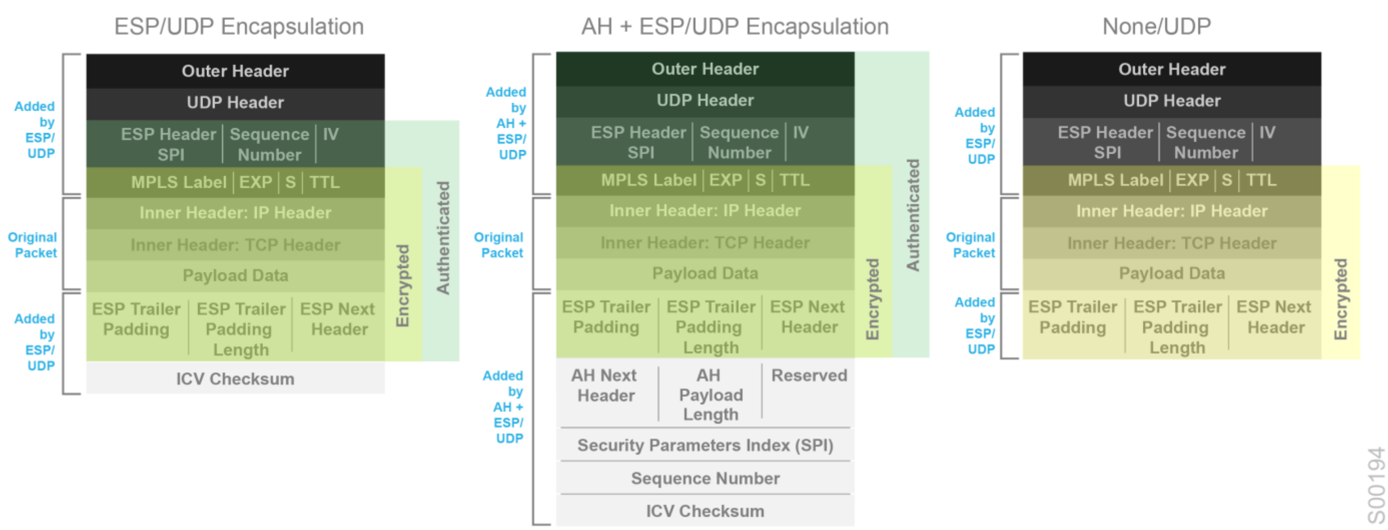
A number of components contribute to the integrity of data packets in the Viptela data plane:

- ESP, which is the standard IPsec encryption protocol, protects (via encryption and authentication) the inner header, data packet payload, and ESP trailer in all data packets.
- AH, which is the standard IPsec authentication protocol, protects (via authentication) the entire data packet, including the inner and outer headers, data packet payload, and ESP trailer.
- Anti-replay, which is also part of the standard IPsec software suite, provides a mechanism to number all data packets and to ensure that receiving routers accept only packets with unique numbers.

The first of these components, ESP, is the standard IPsec encryption protocol. ESP protects a data packet's payload and its inner IP header fields both by encryption, which occurs automatically, and authentication. For authentication, ESP performs a checksum calculation on the data packet's payload and inner header fields and places the resultant hash (also called a digest) into a 12-byte HMAC-SHA1 field at the end of the packet. (A hash is a one-way compression.) The receiving device performs the same checksum and compares its calculated hash with that in the packet. If the two checksums match, the packet is accepted. Otherwise, it is dropped. In the figure below, the left stack illustrates the ESP/UDP encapsulation. ESP encrypts and authenticates the inner headers, payload, MPLS label (if present), and ESP trailer fields, placing the HMAC-SHA1 hash in the ICV checksum field at the end of the packet. The outer header fields added by ESP/UDP are neither encrypted nor authenticated.

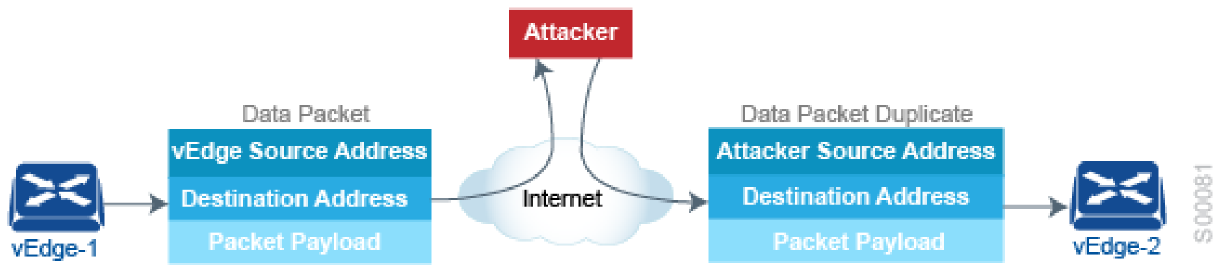
A second component that contributes to data packet integrity is AH, the standard IPsec authentication protocol, which protects all fields in a data packet via authentication. AH performs a checksum process similar to that done by ESP, except that instead of calculating the checksum over just the payload and inner IP header fields, it calculates it over all the fields in the packet—the payload, the inner header, and all the non-mutable fields in the outer IP header. AH places the resultant HMAC-SHA1 hash into the last field of the packet. As with ESP, AH on the receiving device performs the same checksum, and accepts packets whose checksums match. In the figure below, the center stack illustrates the encapsulation performed by AH, in combination with ESP. ESP again encrypts the inner headers, payload, MPLS label (if present), and ESP trailer fields, and now AH authenticates the entire packet—the outer IP and UDP headers, the ESP header, the MPLS label (if present), the original packet, and the ESP trailer—and places its calculated HMAC-SHA1 hash into the ICV checksum field at the end of the packet.

For situations in which data packet authentication is not required, you can disable data packet authentication altogether. In this case, data packets are processed just by ESP, which encrypts the original packet, the MPLS label (if present), and the ESP trailer. This scheme is illustrated in the right stack in the figure below.

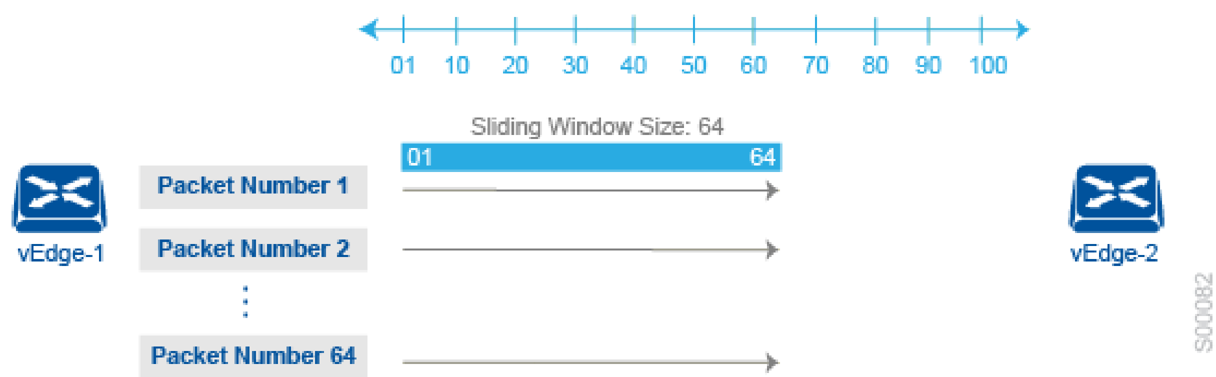



Note that Viptela devices exchange not only the encryption key (which is symmetric), but also the authentication key that is used to generate the HMAC-SHA1 digest. Both are distributed as part of the TLOC properties for a vEdge router.

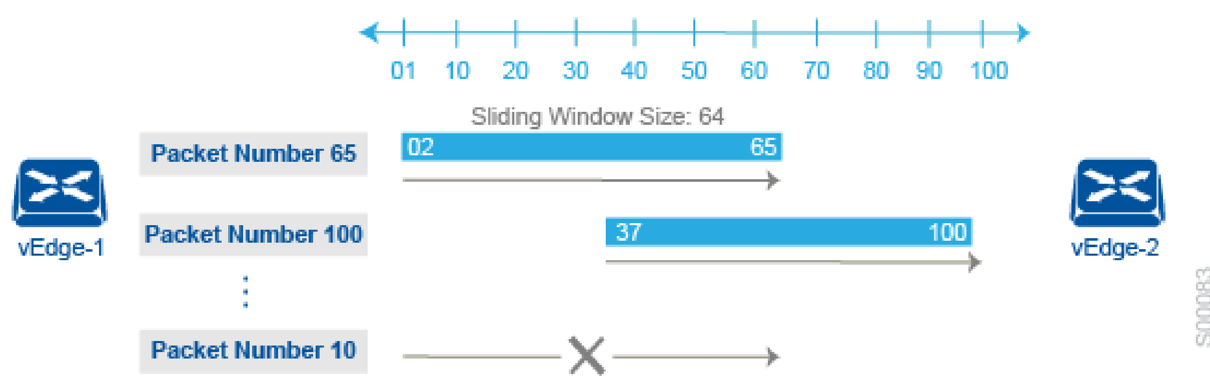
Even though the IPsec connections over which data traffic is exchanged are secure, they often travel across a public network space, such as the Internet, where it is possible for a hacker to launch a replay attack (also called a man-in-the-middle, or MITM, attack) against the IPsec connection. In this type of attack, an adversary tampers with the data traffic by inserting a copy of a message that was previously sent by the source. If the destination cannot distinguish the replayed message from a valid message, it may authenticate the adversary as the source or may incorrectly grant to the adversary unauthorized access to resources or services.



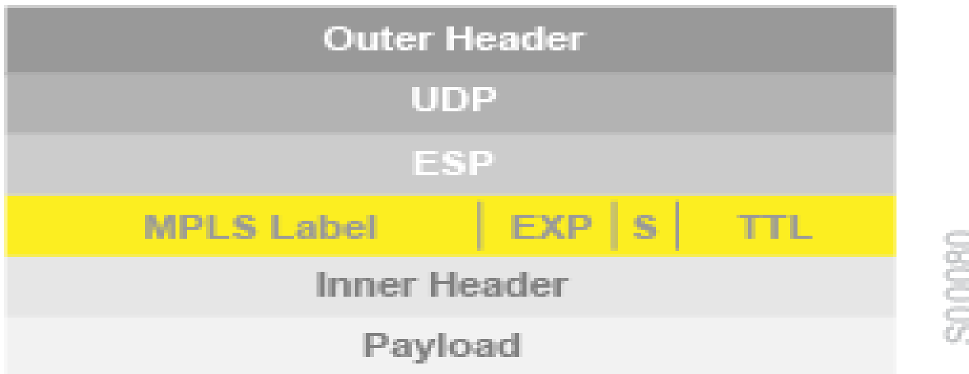

As a counter to such attacks, the Viptela overlay network software implements the IPsec anti-replay protocol. This protocol consists of two components, both of which protect the integrity of a data traffic stream. The first component is to associate sequence numbers with each data packets. The sender inserts a sequence number into each IPsec packet, and the destination checks the sequence number, accepting only packets with unique, non-duplicate sequence numbers. The second component is a sliding window, which defines a range of sequence numbers that are current. The sliding window has a fixed length. The destination accepts only packets whose sequence numbers fall within the current range of values in the sliding window, and it drops all others. A sliding window is used rather than accepting only packets whose sequence number is larger than the last known sequence number, because packets often do not arrive in order.




When the destination receives a packet whose sequence number is larger than the highest number in the sliding window, it slides the window to the right, thus changing the range of valid sequences numbers it will accept. This scheme protects against an MITM type of attack because, by choosing the proper window size, you can ensure that if a duplicate packet is inserted into the traffic stream, its sequence number will either be within the current range but will be a duplicate, or it will be smaller than the lowest current value of the sliding window. Either way, the destination will drop the duplicate packet. So, the sequence numbering combined with a sliding window provide protection against MITM type of attacks and ensure the integrity of the data stream flowing within the IPsec connection.



## Carrying VPN Information in Data Packets




For enterprise-wide VPNs, Viptela devices support MPLS extensions to data packets that are transported within IPsec connections. The figure to the right shows the location of the MPLS information in the data packet header. These extensions provide the security for the network segmentation (that is, for the VPNs) that is needed to support multi-tenancy in a branch or segmentation in a campus. The Viptela implementation uses IPsec UDP-based overlay network layer protocol encapsulation as defined in RFC 4023 . The security is provided by including the Initialization Vector (IV) at the beginning of the payload data in the ESP header. The IV value is calculated by the AES-256 cipher block chaining (CBC).

## Additional Information

Configuring Security Parameters
Control Plane Security Overview
Security Overview

## Umbrella Integration Using CLI

The Umbrella Integration feature enables cloud-based security service by inspecting the Domain Name System (DNS) query that is sent to the DNS server through the device. The security administrator configures policies on the Umbrella portal to either allow or deny traffic towards the fully qualified domain name (FQDN). The router acts as a DNS forwarder on the network edge, transparently intercepts DNS traffic, and forwards the DNS queries to the Umbrella cloud.

**Restrictions for Umbrella Integration**

- If an application or host uses IP address directly instead of DNS to query domain names, policy enforcement is not applied.
- When the client is connected to a web proxy, the DNS query does not pass through the device. In this case, the connector does not detect any DNS request and the connection to the web server bypasses any policy from the Umbrella portal.
- When the Umbrella Integration policy blocks a DNS query, the client is redirected to a Umbrella block page. HTTPS servers provide these block pages and the IP address range of these block pages is defined by the Umbrella portal.
- The type A, AAAA, and TXT queries are the only records that are redirected. Other types of query bypasses the connector. Umbrella Connector maintains a list of IP address that is known for malicious traffic. When the Umbrella roaming client detects the destination of packets to those addresses, it forwards those addresses to Umbrella cloud for further inspection.
- Only the IPv4 address of the host is conveyed in the EDNS option.
- A maximum of 64 local domains can be configured under bypass list, and the allowed domain name length is 100 characters.

**Prerequisites for Umbrella Integration**

Before you configure the Umbrella Integration feature, ensure that the following are met:

- The device has a security K9 license to enable Umbrella Integration.
- The device runs on the SD-WAN IOS XE 16.10 software image or later.
- SD-WAN Umbrella subscription license is available.
- The device is set as the default DNS server gateway and needs to ensure that the DNS traffic goes through the device.

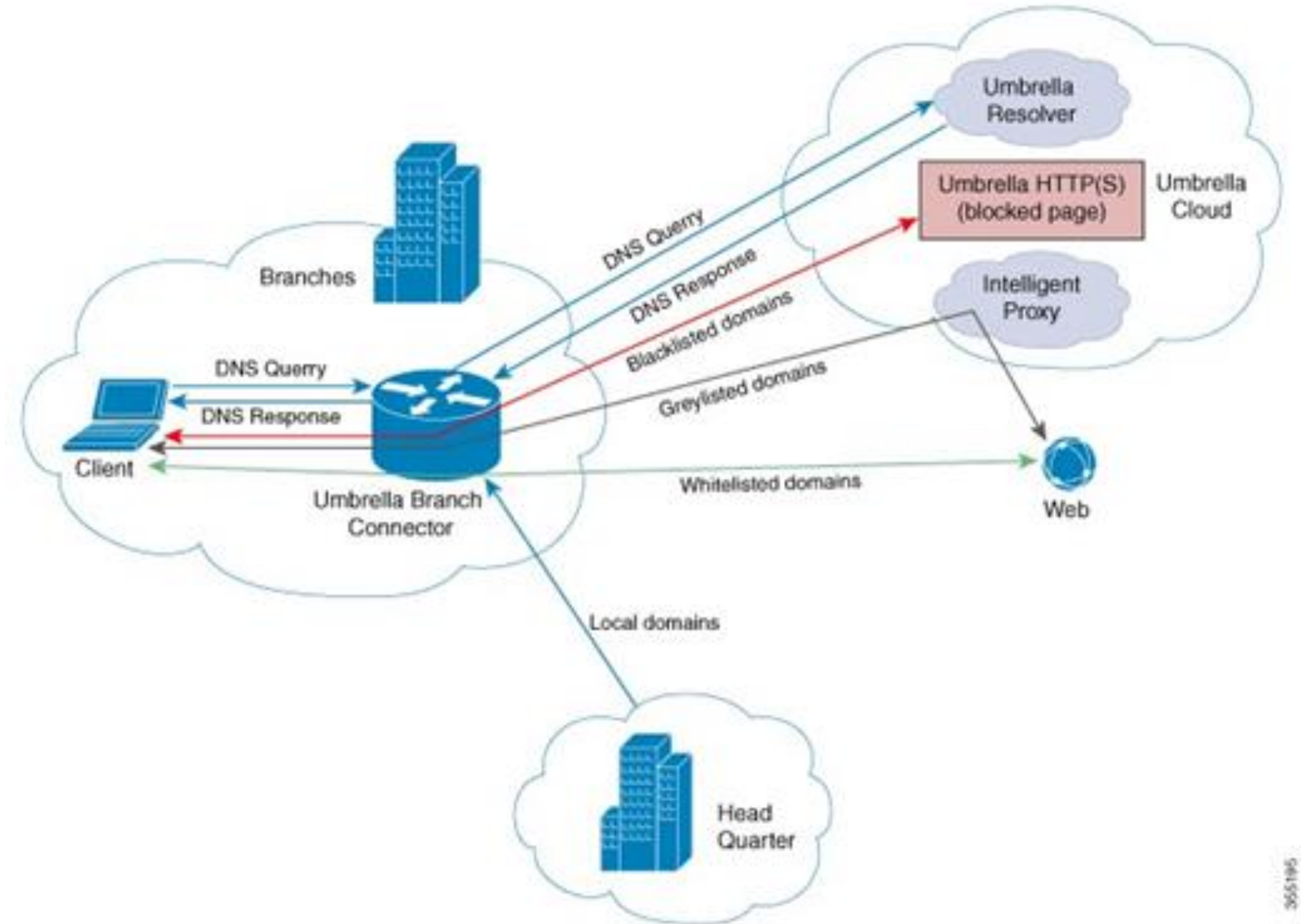
**Cloud-based Security Service Using Umbrella Integration**

The SD-WAN Umbrella Integration feature provides cloud-based security service by inspecting the DNS query that is sent to the DNS server through the device. When a host initiates the traffic and sends a DNS query, the Umbrella Connector in the device intercepts and inspects the DNS query. If the DNS query is for a local domain, it forwards the query without changing the DNS packet to the DNS server in the enterprise network. If it is for an external domain, it adds an Extended DNS (EDNS) record to the query and sends it to Umbrella Resolver. An EDNS record includes the device identifier information, organization ID and client IP. Based on this information, Umbrella Cloud applies different policies to the DNS query.

The Umbrella Integration cloud, based on the policies configured on the portal and the reputation of the DNS Fully Qualified Domain Name (FQDN) may take one of the following actions:

- If FQDN is found to be malicious or blocked by the customized Enterprise Security policy, then the IP address of the Umbrella Cloud's blocked landing page is returned in the DNS response. This is called a blocked list action at Umbrella Cloud.
- If FQDN is found to be non-malicious, then the IP address of the content provider is returned in the DNS response. This is called a allowed list action at Umbrella Cloud.
- If the FQDN is suspicious, then the intelligent proxy unicast IP addresses are returned in the DNS response. This is referred to as grey list action at Umbrella Cloud.

Figure 1: Umbrella Cloud




When the DNS response is received, the device forwards the response back to the host. The host will extract the IP address from the response and send the HTTP / HTTPS requests to this IP.

Note: The intelligent proxy option has to be enabled in the Umbrella dashboard for the Umbrella Resolver to return the intelligent proxy unicast IP addresses in the DNS response when an attempt is made to access the domains in the grey list.

**Handling HTTP and HTTPs Traffic**

With SD-WAN Umbrella Integration, HTTP and HTTPs client requests are handled in the following ways:

- If the Fully Qualified Domain Name (FQDN) in the DNS query is malicious (falls under blocked domains), Umbrella Cloud returns the IP address of the blocked landing page in the DNS response. When the HTTP client sends a request to this IP, Umbrella Cloud displays a page that informs the user that the requested page was blocked and the reason for blocking the page.
- If the FQDN in the DNS query is non-malicious (falls under allowed domains), Umbrella Cloud returns the IP address of the content provider. The HTTP client sends the request to this IP address and gets the desired content.
- If the FQDN in the DNS query falls under grey-listed domains, Umbrella Resolver returns the unicast IP addresses of intelligent proxy in the DNS response. All HTTP traffic from the host to the grey domain gets proxied through the intelligent proxy and undergo URL filtering.

One potential limitation in using intelligent proxy unicast IP addresses is the probability of the datacenter going down when the client is trying to send the traffic to the intelligent proxy unicast IP address. This is a scenario where a client has completed DNS resolution for a domain which falls under grey-listed domain and client's HTTP/(S) traffic is being sent to one of the obtained intelligent proxy unicast IP address. If that datacenter is down, then the client has no way of knowing it.

The Umbrella Connector does not act on the HTTP and HTTPS traffic. The connector does not redirect any web traffic or alter any HTTP/(S) packets.

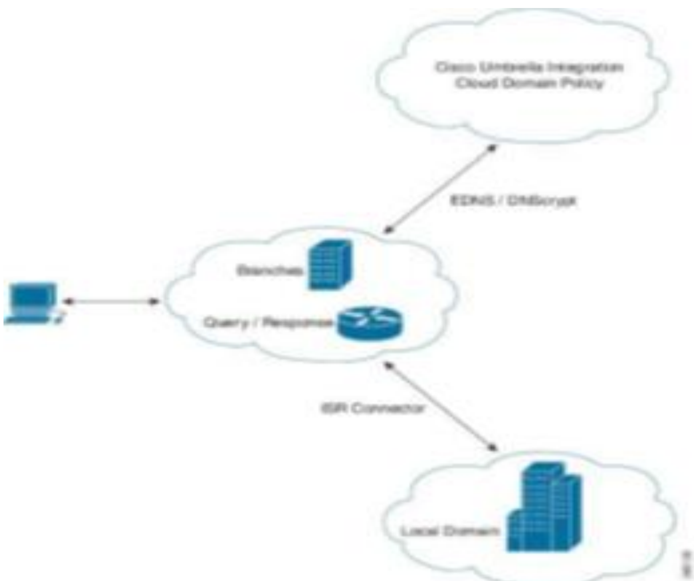
**Encrypting the DNS Packet**

The DNS packet sent from the device to Umbrella Integration server must be encrypted if the EDNS information in the packet contains information such as user IDs, internal network IP addresses, and so on. When the DNS response is sent back from the DNS server, device decrypts the packet and forwards it to the host. You can encrypt DNS packets only when the DNScrypt feature is enabled on the device.

The device uses the following Anycast recursive Umbrella Integration servers:

- 208.67.222.222
- 208.67.220.220
- 2620:119:53::53
- 2620:119:35::35

Figure 3: Umbrella Integration Topology




**Benefits of Umbrella Integration**

The Umbrella Integration provides security and policy enforcement at DNS level. It enables the administrator to split the DNS traffic and directly send some of the desired DNS traffic to a specific DNS server (DNS server located within the enterprise network). This helps the administrator to bypass the Umbrella Integration.

**Configure the Umbrella Connector**

Communication for device registration to the Cisco Umbrella server is via HTTPS. This requires a DigiCert root certificate which is auto installed on the router by default.

To configure Umbrella Connector:

- Get the API token from the Umbrella portal.
- Define VRFs and each VRF can has two options: DNS resolver and enabling local domain list.
  - Umbrella registration is done per VRF only if DNS resolver is configured as Umbrella.

  - Local domain bypass list is global and each VRF can enable or disable the local domain bypass list. If enabled, the DNS packet will be matched against the local domain list.

- Umbrella is a Direct Internet Access (DIA) feature, so NAT configuration is mandatory.

**Sample configuration:**

```
    Device# config-transaction
    Device(config)# parameter-map type umbrella global
    Device(config-profile)#?
    parameter-map commands:
        dnscrypt          Enable DNSCrypt
        exit              Exit from parameter-map
        local-domain      Local domain processing
        no                Negative or set default values of a command
        public-key        DNSCrypt provider public key
        registration-vrf  Cloud facing vrf
        resolver          Anycast address
        token             Config umbrella token
        udp-timeout       Config timeout value for UDP sessions
        vrf               Configure VRF
Per-VRF options are provided under VRF option:
Device(config)# parameter-map type umbrella global
Device(config-profile)#vrf 9
Device(config-profile-vrf)#?
vrf options:
  dns-resolver        DNS resolver address
  exit                Exit from vrf sub mode
  match-local-domain  Match local-domain list(if configured)
  no                  Negate a command or set its defaults

parameter-map type regex dns_bypass
pattern www.cisco.com
pattern www.amazon.com
pattern.*sales.abc.*
!
parameter-map type umbrella global
token 648BF6139C379DCCFFBA637FD1E22755001CE241
local-domain dns_bypass
dnscrypt
udp-timeout 5
vrf 9
    dns-resolver 8.8.8.8
    match-local-domain
vrf 19
    dns-resolver 8.8.8.8
    no match-local-domain
vrf 29
    dns-resolver umbrella
    match-local-domain
vrf 39
    dns-resolver umbrella
    no match-local-domain
!
```

The following table captures the per VRF DNS packet behavior:

| VRF | dns-resolver | Match-local-domain (dns_bypass) |
|---|---|---|
| 9 | 8.8.8.8 | Yes |
| 19 | 8.8.8.8 | No |
| 29 | umbrella | Yes |

| | | |
|---|---|---|
| 39 | umbrella | No |

Note: The VRFs must be preconfigured. For example, the VRFs 9,19, 29, 39 are preconfigured in the above example.

**Sample NAT config for DIA internet connectivity:**

```
ip access-list extended dia-nat-acl
10 permit ip any any
ip nat inside source list dia-nat-acl interface <WAN-facing-Interface> overload
"ip nat outside" MUST be configured under <WAN-facing-Interface>
```

**Configuring the Device as a Pass-through Server**

You can identify the traffic to be bypassed using domain names. In the SD-WAN device, you can define these domains in the form of regular expressions. If the DNS query that is intercepted by the device matches one of the configured regular expressions, then the query is bypassed to the specified DNS server without redirecting to the Umbrella cloud. This sample configuration shows how to define a regex parameter-map with a desired domain name and regular expressions:

```
Device# config-transaction
Device(config)# parameter-map type regex dns_bypass
Device(config)# pattern www.cisco.com
Device(config)# pattern www.amazon.com
Device(config)# pattern.*sales.abc.*
```

**DNSCrypt, Resolver, and Public-key**

When you configure the device using the **parameter-map type umbrella global** command, the following values are auto-populated:

- DNSCrypt
- Public-Key

**Public-key**

Public-key is used to download the DNSCrypt certificate from Umbrella Integration cloud. This value is preconfigured to

**B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79** which is the public-key of Umbrella Integration Anycast servers. If there is a change in the public-key and if you modify this command, then you have to remove the modified command to restore the default value. If you modify the value, the DNSCrypt certificate download may fail.

**DNSCrypt**

DNSCrypt is an encryption protocol to authenticate communications between the device and the Umbrella Integration. When the **parameter-map type umbrella** is configured and enabled by default on all WAN interfaces. DNSCrypt gets triggered and a certificate is downloaded, validated, and parsed. A shared secret key is then negotiated, which is used to encrypt the DNS queries. For every hour this certificate is automatically downloaded and verified for an upgrade, a new shared secret key is negotiated to encrypt the DNS queries.

To disable DNSCrypt, use the **no dnscrypt** command and to re-enable DNSCrypt, use the **dnscrypt** command.

When the DNSCrypt is used, the DNS request packets size is more than 512 bytes. Ensure that these packets are allowed through the intermediary devices; otherwise, the response may not reach the intended recipients.

Sample umbrella dnscrypt notifications:

```
Device# show sdwan umbrella dnscrypt
    DNSCrypt: Enabled
    Public-key: B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79
Certificate Update Status:
    Last Successfull Attempt: 08:46:32 IST May 21 2018
Certificate Details:
    Certificate Magic       : DNSC
    Major Version           : 0x0001
    Minor Version           : 0x0000
    Query Magic             : 0x714E7A696D657555
```

```
    Serial Number         : 1517943461
    Start  Time           : 1517943461 (00:27:41 IST Feb 7 2018)
    End Time              : 1549479461 (00:27:41 IST Feb 7 2019)
    Server Public Key     :
240B:11B7:AD02:FAC0:6285:1E88:6EAA:44E7:AE5B:AD2F:921F:9577:514D:E226:D552:6836
    Client Secret Key Hash:
8A97:BBD0:A8BE:0263:F07B:72CB:BB21:330B:D47C:7373:B8C8:5F96:9F07:FEC6:BBFE:95D0
    Client Public key     :
0622:C8B4:4C46:2F95:D917:85D4:CB91:5BCE:78C0:F623:AFE5:38BC:EF08:8B6C:BB40:E844
    NM key Hash           :
88FC:7825:5B58:B767:32B5:B36F:A454:775C:711E:B58D:EE6C:1E5A:3BCA:F371:4285:5E3A
When disabled:
Device# show umbrella dnscrypt
    DNSCrypt: Not enabled
    Public-key: NONE
Sample configuration steps for dns-resolver and match-local-domain-to-bypass per vrf:
Router(config)# vrf definition 1
Router(config-vrf)# address-family ipv4
Router(config-ipv4)# exit-address-family
Router(config-vrf)# commitCommit complete.
Router(config-vrf)# exit
Router(config)# parameter-map type umbrella global
Router(config-profile)# ?
Possible completions:
    dnscrypt
    local-domain
    public-key
    registration-vrf
    resolver
    token
    udp-timeout
    vrf
Router(config-profile)# vrf ?
This line doesn't have a valid range expression
Possible completions:
    <name:string, min: 1 chars, max: 32 chars>  1
Router(config-profile)# vrf 1
Router(config-profile-vrf)# ?
Possible completions:
    dns-resolver
    match-local-domain-to-bypass
Router(config-profile-vrf)# dns-resolver umbrella
Router(config-profile-vrf)# match-local-domain-to-bypass
Router(config-profile-vrf)# commit
Commit complete.
Router(config-profile-vrf)# end
Router(config)# vrf definition 2
Router(config-vrf)# address-family ipv4
Router(config-ipv4)# exit-address-family
Router(config-vrf)# commitCommit complete.
Router(config-vrf)# exit
Router(config)# parameter-map type umbrella global
Router(config-profile)# vrf 2
Router(config-profile-vrf)# dns-resolver 8.8.8.8
Router(config-profile-vrf)# no match-local-domain-to-bypass
Router(config-profile-vrf)# commit
Commit complete.
Router(config-profile-vrf)# end
Router#sh umbrella config

Umbrella Configuration
========================
Token: AAC1A2555C11B2B798FFF3AF27C2FB8F001CB7B2
OrganizationID: 1882034
```

```
Local Domain Regex parameter-map name: NONE
DNSCrypt: Enabled
Public-key: B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79
UDP Timeout: 5 seconds
Resolver address:
    1. 208.67.220.220
    2. 208.67.222.222
    3. 2620:119:53::53
    4. 2620:119:35::35
Registration VRF: default
VRF List:
1. VRF 1 (ID: 1)
    DNS-Resolver: umbrella
    Match local-domain-to-bypass: Yes
2. VRF 2 (ID: 3)
    DNS-Resolver: 8.8.8.8
    Match local-domain-to-bypass: No
```

**Verifying the Umbrella Connector Configuration**

Verify the Umbrella Connector configuration using the following commands:

```
Device# show umbrella config
Umbrella Configuration
========================
  Token: 648BF6139C379DCCFFBA637FD1E22755001CE241
  OrganizationID: 1892929
  Local Domain Regex parameter-map name: dns_bypass
  DNSCrypt: Enabled
  Public-key: B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79
  UDP Timeout: 5 seconds
  Resolver address:
      1. 208.67.220.220
      2. 208.67.222.222
      3. 2620:119:53::53
      4. 2620:119:35::35
  Registration VRF: default
  VRF List:
      1. VRF 9 (ID: 4)
          DNS-Resolver: 8.8.8.8
          Match local-domain: Yes
      2. VRF 19 (ID: 1)
          DNS-Resolver: 8.8.8.8
          Match local-domain: No
      3. VRF 29 (ID: 2)
          DNS-Resolver: umbrella
          Match local-domain: Yes
      4. VRF 39 (ID: 3)
          DNS-Resolver: umbrella
          Match local-domain: No
The output of VRF will have name and ID. The ID here is VRF ID:
Device# show vrf detail | inc VRF Id
VRF 19 (VRF Id = 1); default RD <not set>; default VPNID <not set>
VRF 29 (VRF Id = 2); default RD <not set>; default VPNID <not set>
VRF 39 (VRF Id = 3); default RD <not set>; default VPNID <not set>
VRF 9 (VRF Id = 4); default RD <not set>; default VPNID <not set>

When DNSCrypt is disabled:
Device# show umbrella config
Umbrella Configuration
========================
    Token: 648BF6139C379DCCFFBA637FD1E22755001CE241
    OrganizationID: 1892929
    Local Domain Regex parameter-map name: dns_bypass
    DNSCrypt: Not enabled
```

```
    Public-key: NONE
    UDP Timeout: 5 seconds
    Resolver address:
        1. 208.67.220.220
        2. 208.67.222.222
        3. 2620:119:53::53
        4. 2620:119:35::35
 Registration VRF: default
 VRF List:
     1. VRF 9 (ID: 4)
         DNS-Resolver: 8.8.8.8
         Match local-domain: Yes
     2. VRF 19 (ID: 1)
         DNS-Resolver: 8.8.8.8
         Match local-domain: No
     3. VRF 29 (ID: 2)
         DNS-Resolver: umbrella
         Match local-domain: Yes
    4. VRF 39 (ID: 3)
        DNS-Resolver: umbrella
        Match local-domain: No
```

**Displaying Umbrella Registration Details**

The following example displays the device registration information:

```
Device# show sdwan umbrella device-registration
Device registration details
VRF        Tag     Status        Device-id29
vpn29      200     SUCCESS     010a9b2b0d5cb21f39
vpn39      200     SUCCESS     010a1a2e1989da19

The following example displays the device registration information in detail:
Device# show umbrella deviceid detailed
Device registration details
1.29
    Tag                : vpn29
    Device-id          : 010a9b2b0d5cb21f
    Description        : Device Id recieved successfully
    WAN interface      : None

2.39
    Tag                : vpn39
    Device-id          : 010a1a2e1989da19
    Description        : De
    vice Id recieved successfully
    WAN interface      : None
```

**Show Commands**

**Umbrella show commands at FP Layer**

The **show platform software umbrella f0 config** command displays all the local domains configured for Open DNS in the FP Layer.

```
Device# show platform software umbrella f0 config
+++ Umbrella Config +++
Umbrella feature:
------------------
Init: Enabled
Dnscrypt: Enabled
Timeout:
------------------
udp timeout: 5
OrgId :
------------------
```

```
orgid : 1892929
Resolver config:
RESOLVER IP's
---------------------
208.67.220.220
208.67.222.222
2620:119:35::35
2620:119:53::53
Dnscrypt Info:
public_key:
A5:BA:18:C5:59:70:67:94:E5:37:38:33:06:F9:63:83:39:86:82:E4:00:F5:D8:BE:C1:AA:77:4A:4C:BA:64:00
magic_key: 71 4E 7A 69 6D 65 75 55
serial number: 1517943461
ProfileID    DeviceID          Mode      Resolver     Local-Domain    Tag
------------------------------------------------------------------------------
     0                         OUT                      False
     4                         IN        8.8.8.8        True            vpn9
     1                         IN        8.8.8.8        False           vpn19
     2     010a9b2b0d5cb21f    IN     208.67.220.220    True            vpn29
     3     010a1a2e1989da19    IN     208.67.220.220    False           vpn39

The show platform software umbrella f0 local-domain displays the local domain list.
Device# show platform software umbrella f0 local-domain
01.  www.cisco.com
02.  www.amazon.com
03..*sales.abc.*
```

**Umbrella show commands at CPP Layer**

The show platform hardware qfp active feature umbrella client config command displays the configuration in CPP layer.

```
 +++ Umbrella Config +++
Umbrella feature:
----------------
Init: Enabled
Dnscrypt: Enabled
Timeout:
--------
udp timeout: 5
Orgid:
--------
orgid: 1892929
Resolver config:
------------------
RESOLVER IP's
    208.67.220.220
    208.67.222.222
    2620:119:53::53
    2620:119:35::35
Dnscrypt Info:
--------------
public_key:
D9:2D:20:93:E8:8C:B4:BD:32:E6:A3:D1:E0:5B:7E:1A:49:C5:7F:96:BD:28:79:06:A2:DD:2E:A7:A1:F9:3D:7E
magic_key: 71 4E 7A 69 6D 65 75 55
serial number: 1517943461

Umbrella Interface Config:
--------------------------
11      GigabitEthernet4 :
        Mode     : IN
        DeviceID : 010a9b2b0d5cb21f
        Tag      : vpn29
10      GigabitEthernet3 :
        Mode     : IN
        DeviceID : 0000000000000000
```

```
        Tag      : vpn9
05      Null0 :
        Mode     : OUT
06     VirtualPortGroup0 :
        Mode     : OUT
07     VirtualPortGroup1 :
        Mode     : OUT
08      GigabitEthernet1 :
        Mode     : OUT
09      GigabitEthernet2 :
        Mode     : OUT
12      GigabitEthernet5 :
        Mode     : OUT

Umbrella Profile Deviceid Config:
----------------------------------
ProfileID: 0
    Mode     : OUT
ProfileID: 1
    Mode     : IN
    Resolver : 8.8.8.8
    Local-Domain: False
    DeviceID : 0000000000000000
    Tag      : vpn19
ProfileID: 3
    Mode     : IN
    Resolver : 208.67.220.220
    Local-Domain: False
    DeviceID : 010a1a2e1989da19
    Tag      : vpn39
ProfileID: 4
    Mode     : IN
    Resolver : 8.8.8.8
    Local-Domain: True
    DeviceID : 0000000000000000
    Tag      : vpn9
ProfileID: 2
    Mode     : IN
    Resolver : 208.67.220.220
    Local-Domain: True
    DeviceID : 010a9b2b0d5cb21f
    Tag      : vpn29

Umbrella Profile ID CPP Hash:
------------------------------
VRF ID :: 1
    VRF NAME : 19
    Resolver : 8.8.8.8
    Local-Domain: False
VRF ID :: 4
    VRF NAME : 9
    Resolver : 8.8.8.8
    Local-Domain: True
VRF ID :: 2
    VRF NAME : 29
    Resolver : 208.67.220.220
    Local-Domain: True
VRF ID :: 3
    VRF NAME : 39
    Resolver : 208.67.220.220
    Local-Domain: False
```

**Umbrella Data-Plane show commands**

The **show platform hardware qfp active feature umbrella datapath stats** command displays the umbrella statistics in data plane.

```
Device# show platform hardware qfp active feature umbrella datapath stats
Umbrella Connector Stats:
    Parser statistics:
        parser unknown pkt: 0
        parser fmt error: 0
        parser count nonzero: 0
        parser pa error: 0
        parser non query: 0
        parser multiple name: 0
        parser dns name err: 0
        parser matched ip: 0
        parser opendns redirect: 0
        local domain bypass: 0
        parser dns others: 0
        no device id on interface: 0
        drop erc dnscrypt: 0
        regex locked: 0
        regex not matched: 0
        parser malformed pkt: 0
    Flow statistics:
        feature object allocs : 0
        feature object frees  : 0
        flow create requests  : 0
        flow create successful: 0
        flow create failed, CFT handle: 0
        flow create failed, getting FO: 0
        flow create failed, malloc FO : 0
        flow create failed, attach FO : 0
        flow create failed, match flow: 0
        flow create failed, set aging : 0
        flow lookup requests  : 0
        flow lookup successful: 0
        flow lookup failed, CFT handle: 0
        flow lookup failed, getting FO: 0
        flow lookup failed, no match  : 0
        flow detach requests  : 0
        flow detach successful: 0
        flow detach failed, CFT handle: 0
        flow detach failed, getting FO: 0
        flow detach failed freeing FO : 0
        flow detach failed, no match  : 0
        flow ageout requests          : 0
        flow ageout failed, freeing FO: 0
        flow ipv4 ageout requests     : 0
        flow ipv6 ageout requests     : 0
        flow update requests  : 0
        flow update successful: 0
        flow update failed, CFT handle: 0
        flow update failed, getting FO: 0
        flow update failed, no match  : 0
     DNSCrypt statistics:
         bypass pkt: 0
         clear sent: 0
         enc sent: 0
         clear rcvd: 0
         dec rcvd: 0
         pa err: 0
         enc lib err: 0
         padding err: 0
         nonce err: 0
         flow bypass: 0
         disabled: 0
         flow not enc: 0
```

```
    DCA statistics:
        dca match success: 0
        dca match failure: 0
```

The **show platform hardware qfp active feature umbrella datapath memory** command displays CFT information.

```
Device# show platform hardware qfp active feature umbrella datapath memory
==Umbrella Connector CFT Information==
CFT inst_id 0 feat id 0 fo id 0 chunk id 4
==Umbrella Connector Runtime Information==
umbrella init state 0x4
umbrella dsa client handler 0x2
```

The **show platform hardware qfp active feature umbrella datapath runtime** command displays internal information. For example, key index used for DNSCrypt.

```
Device# show platform hardware qfp active feature umbrella datapath runtime
udpflow_ageout: 5
ipv4_count: 2
ipv6_count: 2
ipv4_index: 0
ipv6_index: 0
Umbrella IPv4 Anycast Address
IP Anycast Address0: 208.67.220.220
IP Anycast Address1: 208.67.222.222
Umbrella IPv6 Anycast Address
IP Anycast Address0: 2620:119:53:0:0:0:0:53
IP Anycast Address1: 2620:119:35:0:0:0:0:35
=DNSCrypt=
key index: 0
-key[0]-
sn: 1517943461
ref cnt: 0
magic: 714e7a696d657555
Client Public Key: A5BA:18C5:5970:6794:E537:3833:06F9:6383:3986:82E4:00F5:D8BE:C1AA:774A:4CBA:6400
NM Key Hash      : 16E6:DDC7:53BE:2929:1CDA:06AE:0BE2:C270:6E39:EAE7:F925:78FD:3599:2AB6:74C9:A59D
-key[1]-
sn: 0
ref cnt: 0
magic: 0000000000000000
Client Public Key: 0000:0000:0000:0000:0000:0000:0000:0000:0000:0000:0000:0000:0000:0000:0000:0000
NM Key Hash      : 0000:0000:0000:0000:0000:0000:0000:0000:0000:0000:0000:0000:0000:0000:0000:0000
Local domain 1
VPN-DEVICEID TABLE d7f37410
```

**Clear Command**

The **clear platform hardware qfp active feature umbrella datapath stats** command clears the Umbrella connector statistics in datapath.

```
Device# clear platform hardware qfp active feature umbrella datapath stats
Umbrella Connector Stats Cleared
```

**Troubleshooting Umbrella Integration**

Troubleshoot issues that are related to enabling Umbrella Integration feature using these commands:

- **debug umbrella device-registration**
- **debug umbrella config**
- **debug umbrella dnscrypt**

Depending on the OS, run either of these two commands from the client device:

- The nslookup -type=txt debug.umbrella.com command from the command prompt of the Windows machine

· The nslookup -type=txt debug.umbrella.com command from the terminal window or shell of the Linux machine

```
nslookup -type=txt debug.opendns.com 8.8.8.8
Server: 8.8.8.8
Address: 8.8.8.8#53
Non-authoritative answer:
debug.opendns.com text = "server r6.mum1"
debug.opendns.com text = "device 010A826AAABB6C3D"
debug.opendns.com text = "organization id 1892929"
debug.opendns.com text = "remoteip 171.168.1.7"
debug.opendns.com text = "flags 436 0 6040 39FF000000000000000"
debug.opendns.com text = "originid 119211936"
debug.opendns.com text = "orgid 1892929"
debug.opendns.com text = "orgflags 3"
debug.opendns.com text = "actype 0"
debug.opendns.com text = "bundle 365396"
debug.opendns.com text = "source 72.163.220.18:36914"
debug.opendns.com text = "dnscrypt enabled (713156774457306E)"
```

Close message

Learn more

Welcome to your new guide!

Click on "New" to build out your guide.

*Tags recommended by the template:* article:topic

# Using Umbrella DNS Security

# Umbrella Configuration on SD-WAN

How to configure Umbrella policy with a configuration wizard.

## Umbrella Configuration on SD-WAN

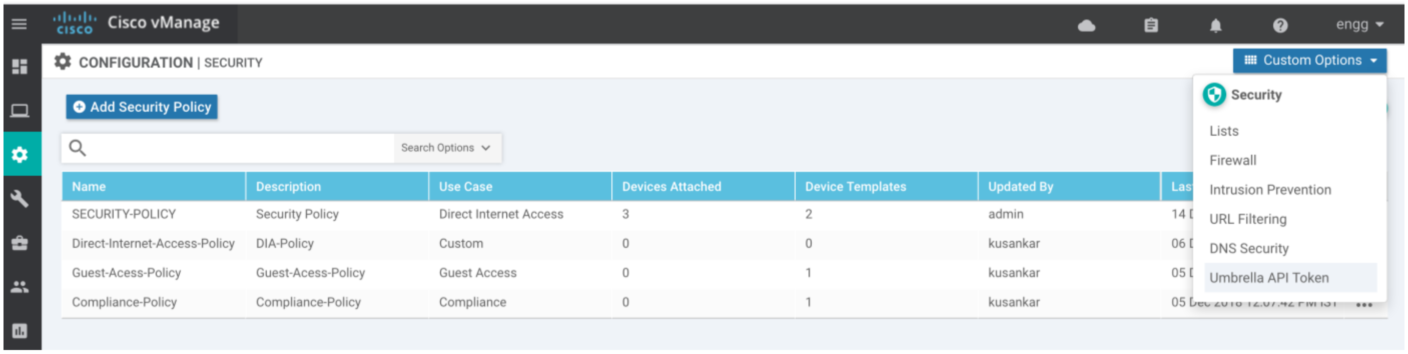
The Umbrella Integration feature enables cloud-based security service by inspecting the Domain Name System (DNS) query that is sent to the DNS server through the device.

You can configure Umbrella policy with a configuration wizard. The wizard is a UI policy builder that consists of the following components:

- Configure Umbrella API Token
- Define Domain list
- Configure Umbrella DNS
- Apply Umbrella DNS Security Policy to a Template
- Monitor Umbrella Feature

### Configure Umbrella API Token

1. In Cisco vManage NMS, select the Configuration ► Security tab ► Custom Options on the right side to configure the Umbrella API Token as shown in the following screenshot.



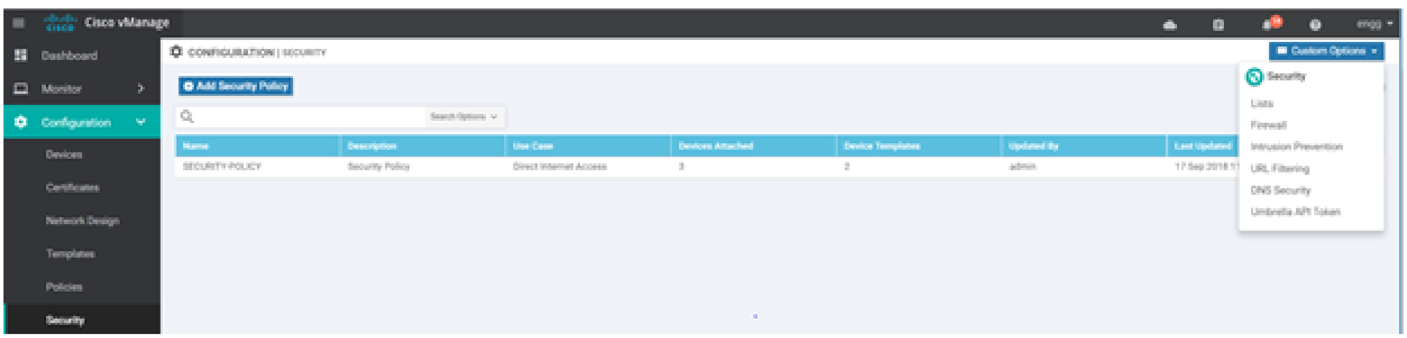

2. Enter token number in the **Umbrella Token** field.

3. Click **Save** to configure the Umbrella API Token.

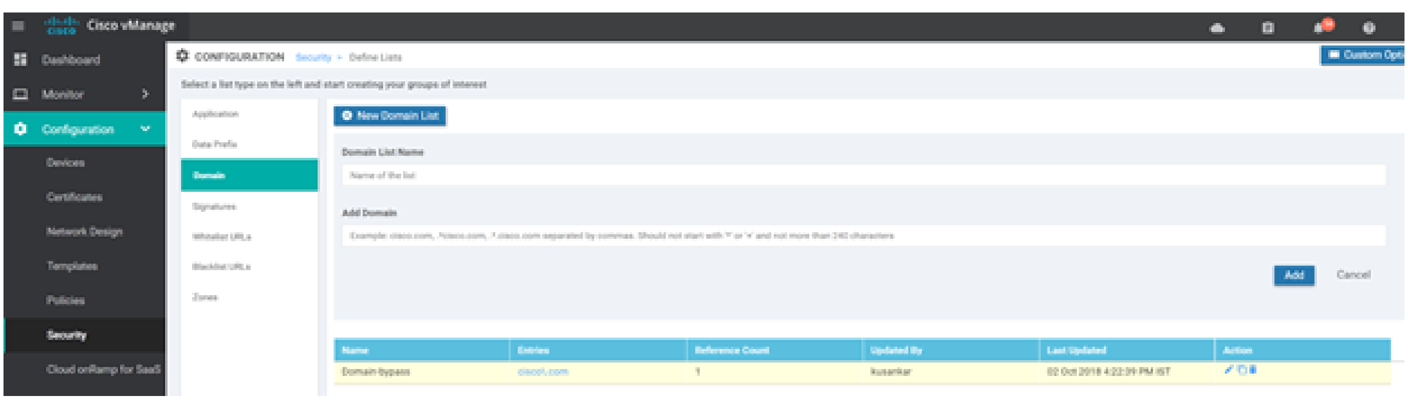
## Defining Domain Lists

To define Domain-List, use the vManage security configuration wizard:

1. In Cisco vManage NMS, select the Configuration ▶ Security tab ▶ Custom Options in the right side.




2. Click on **Lists** in the Custom Options drop-down. A Define Lists wizard appears.



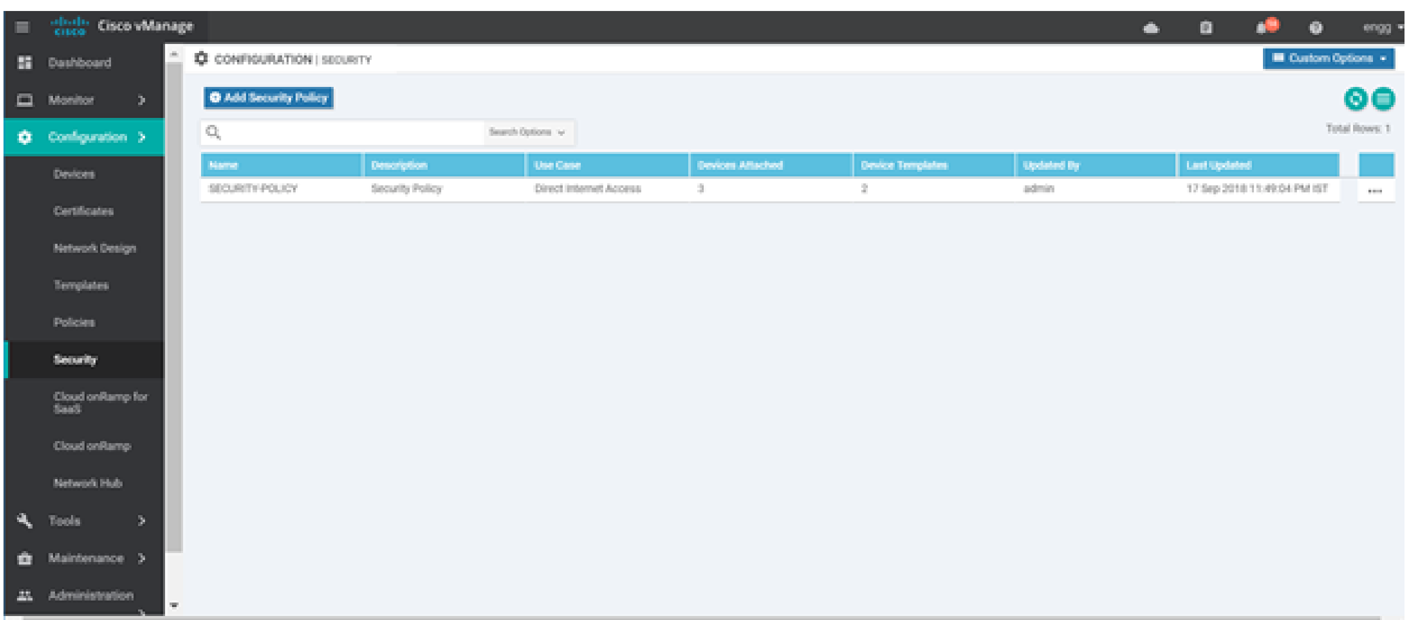

3. Click on **New Domain List** to create a new domain list or select the domain name and click on pencil icon on the right side for the existing list.


4. Enter the **Domain List Name, Domain** and click **Save** to create the list.

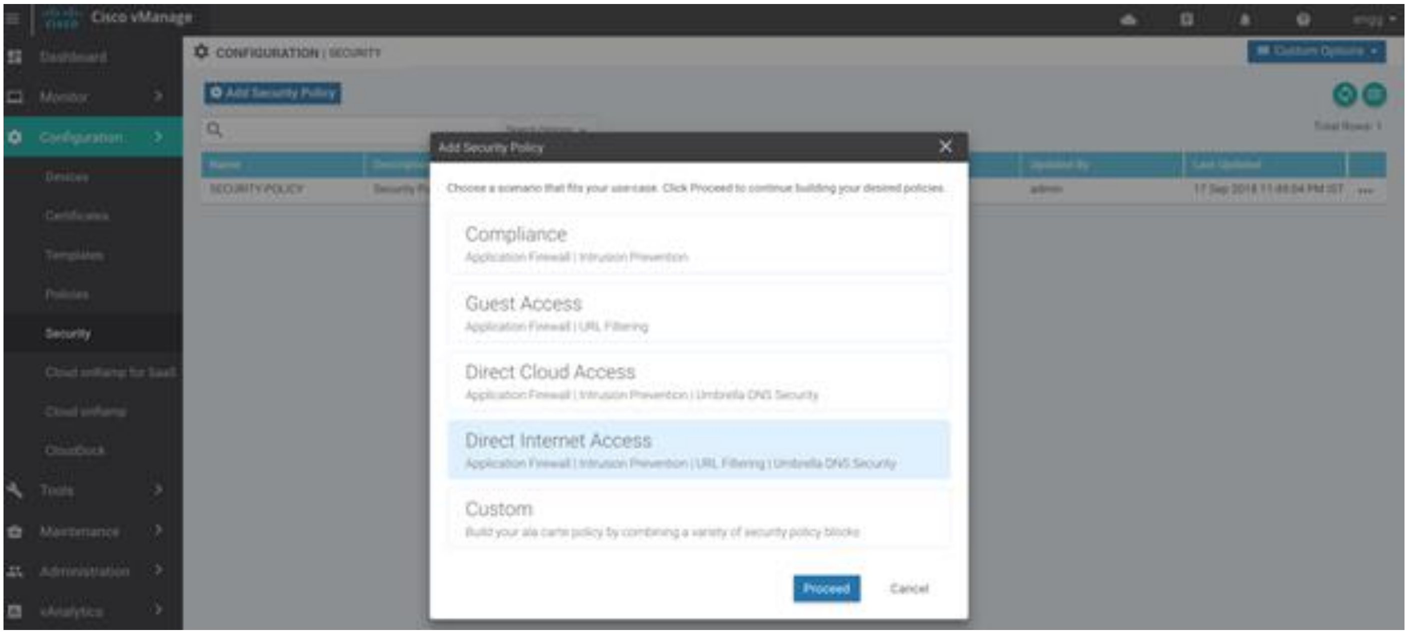
## Configure Umbrella DNS Policy

To configure umbrella through DNS Security, use the vManage security configuration wizard:

1. In Cisco vManage NMS, select the Configuration ▶ Security tab in the left side panel.




2. Click **Add Security Policy** . The Add Security Policy wizard appears.

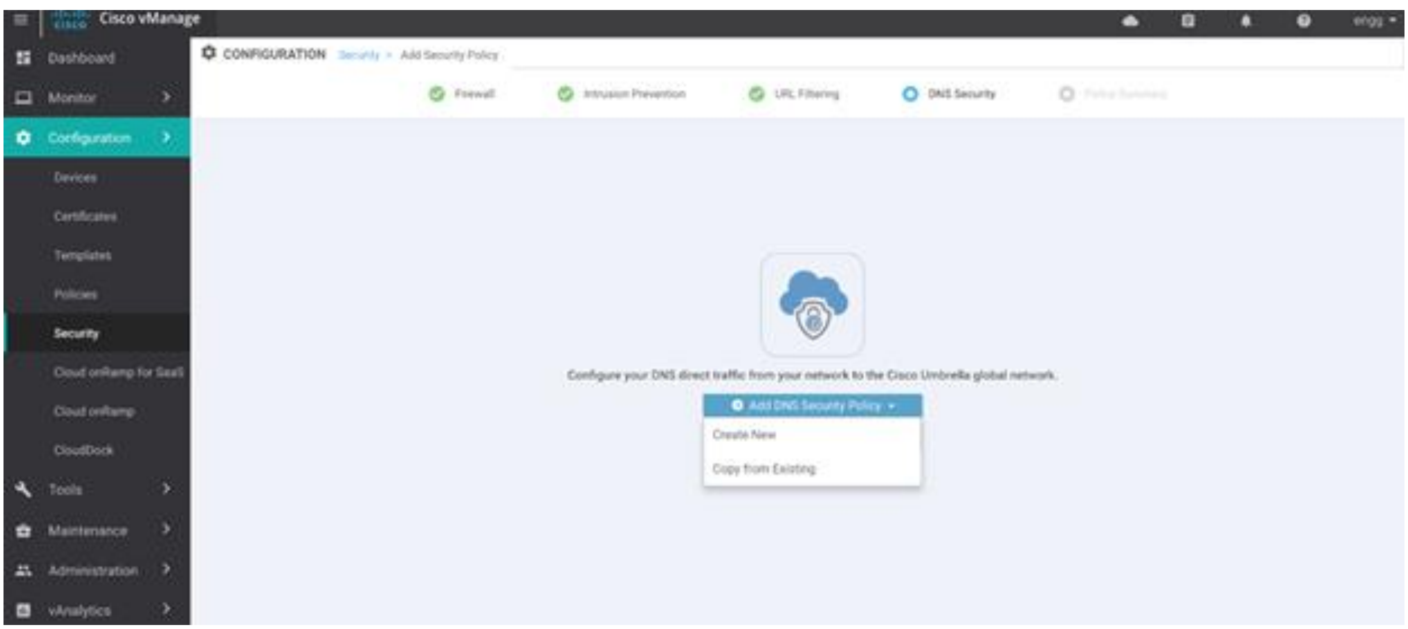



3. The Add Security Policy configuration wizard opens, and various use-case scenarios display.

4. In Add Security Policy, select **Direct Internet Access** .

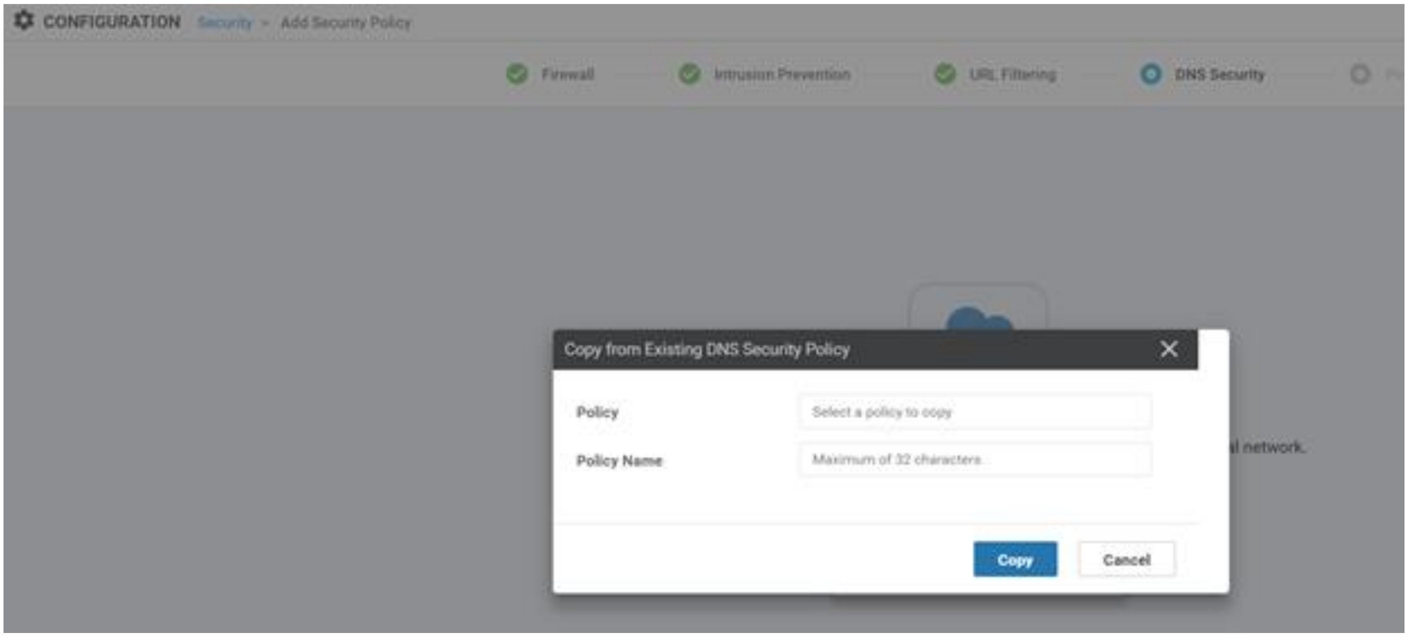
5. Click **Proceed** to add a Umbrella DNS Security policy in the wizard.

6. In the Add Security Policy wizard, select DNS Security tab to create a new DNS Security policy.

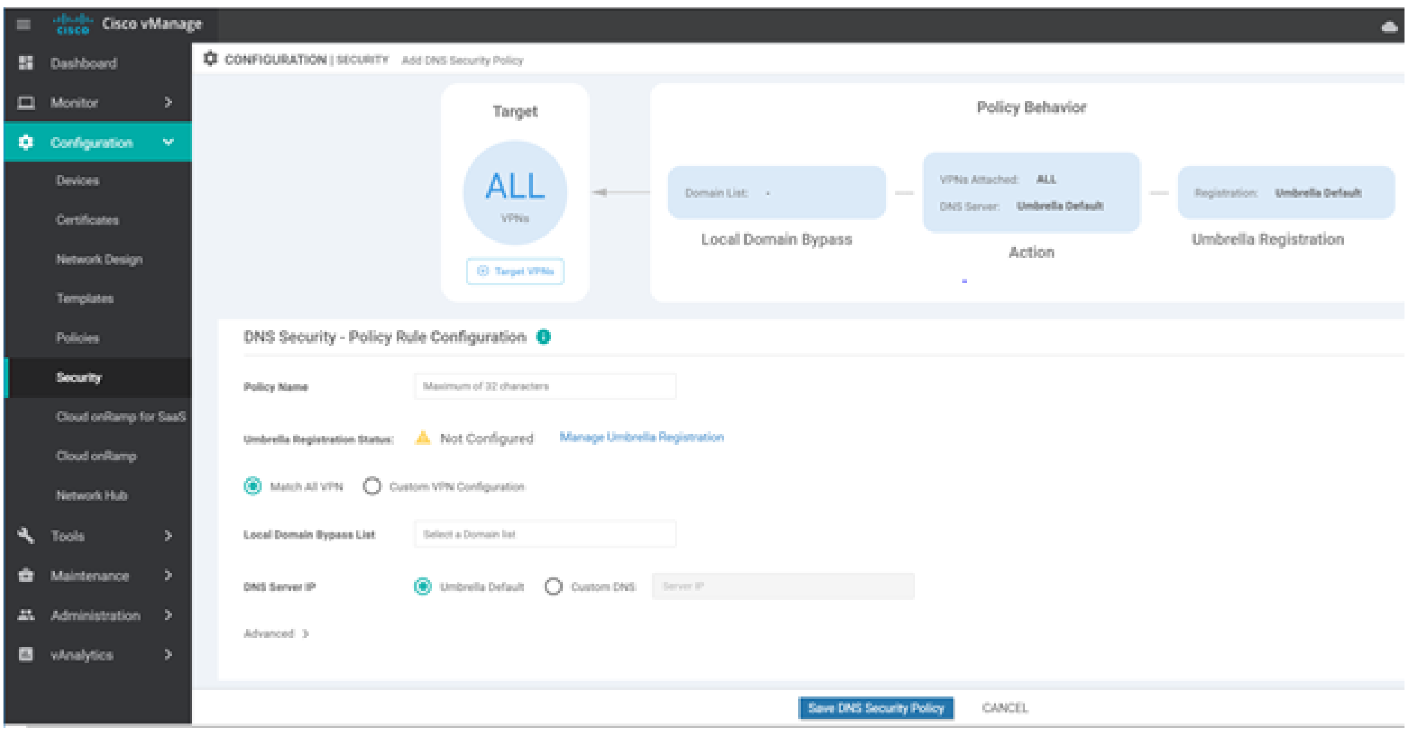



7. Click the **Add DNS Security Policy** drop-down and select from the following options:

- Create New - A DNS Security - Policy Rule Configuration wizard appears and continue with Step 8.
- Copy from Existing - A Copy from Existing DNS Security Policy wizard appears. Select a **Policy** from the drop-down and enter **Policy Name** and copy the policy to a device.



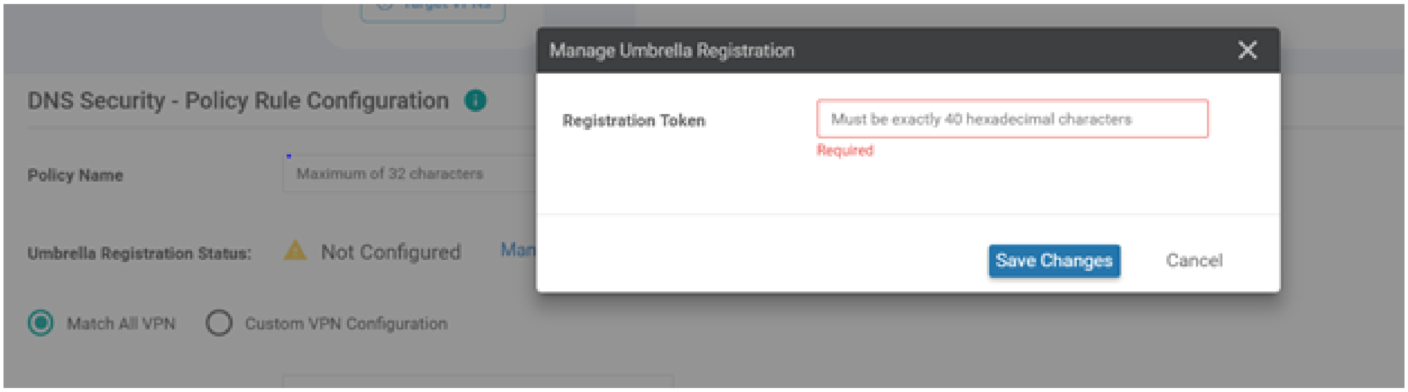

8. If you are creating a new policy using **Create New** , a DNS Security - Policy Rule Configuration wizard appears.




9. Enter a policy name in the **Policy Name** field.

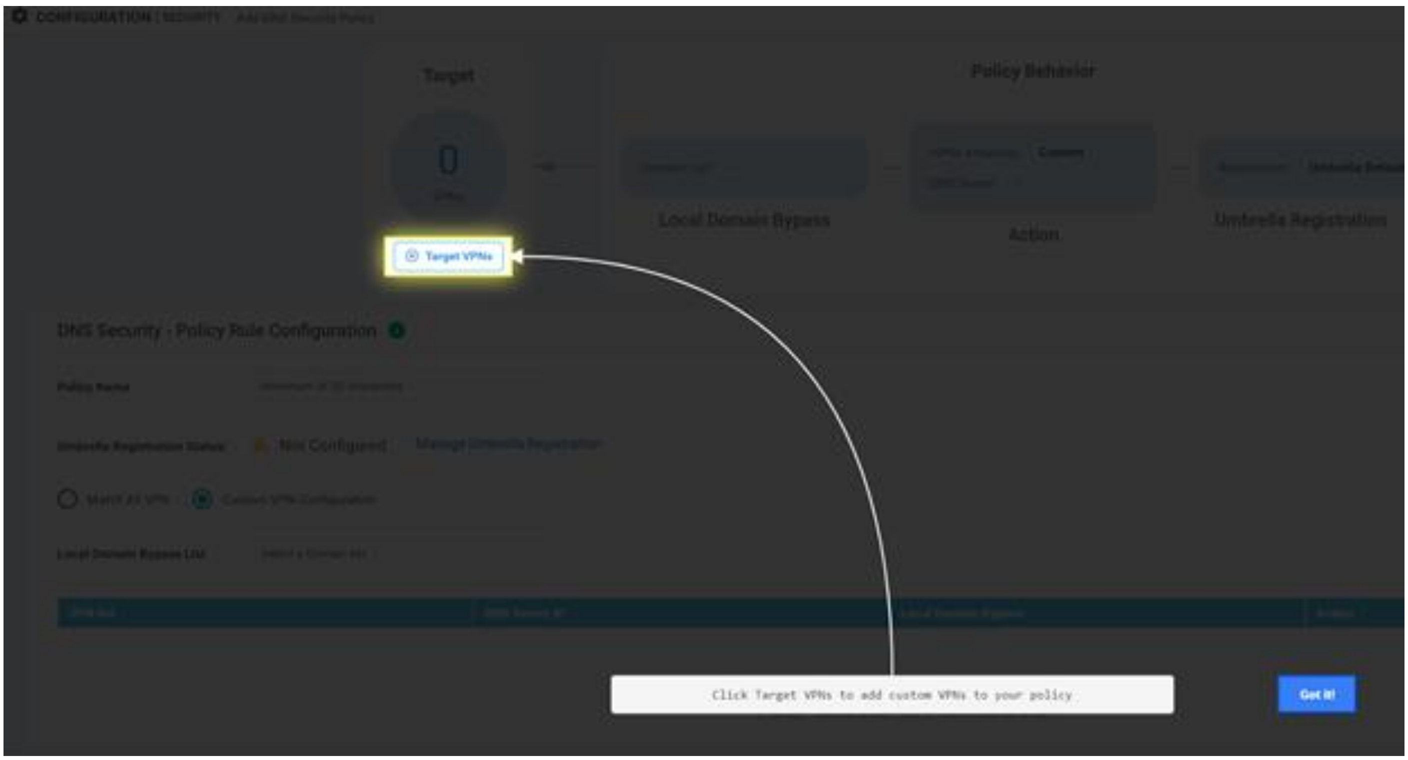
10. The Umbrella Registration Status displays the status about the API Token configuration.

11. Click on **Manage Umbrella Registration** to add a token.

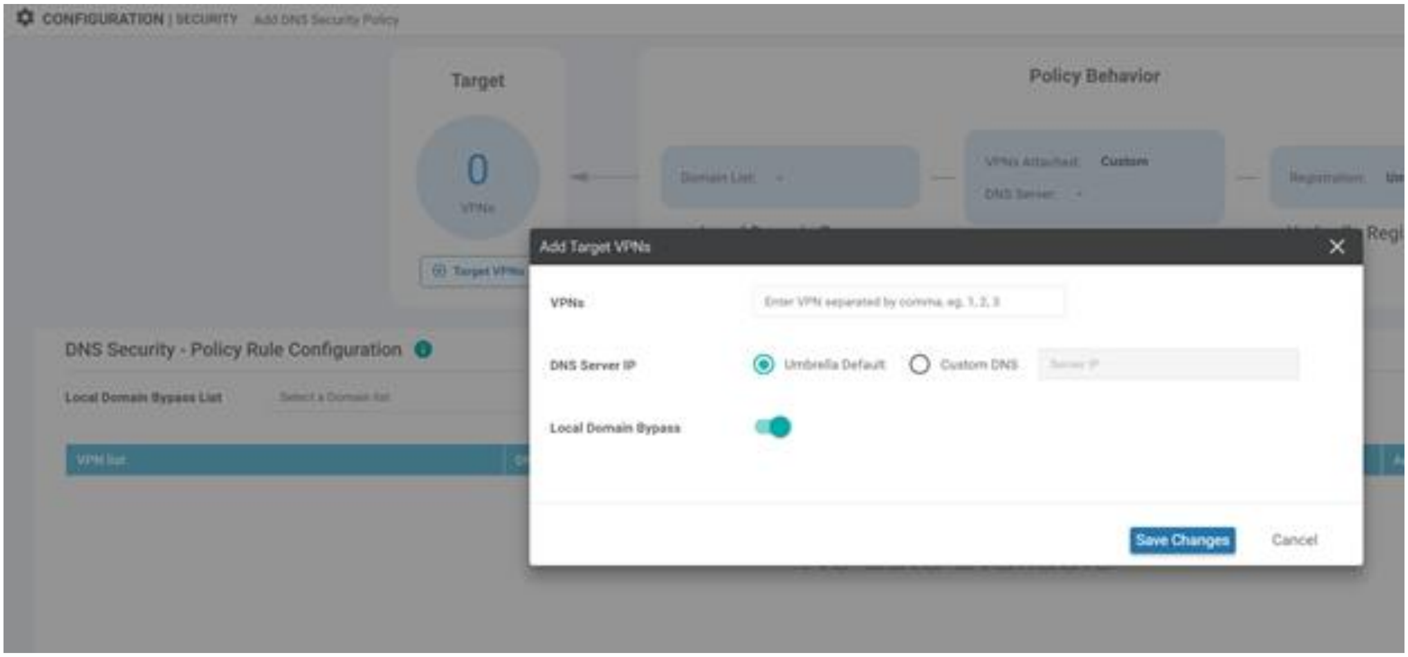



12. Select **Match All VPN** option if you need to keep the same configuration for all the available VPNs and continue with step 13.

Or select **Custom VPN Configuration** if you need to add target VPNs to your policy. A Target VPNs wizard appears.

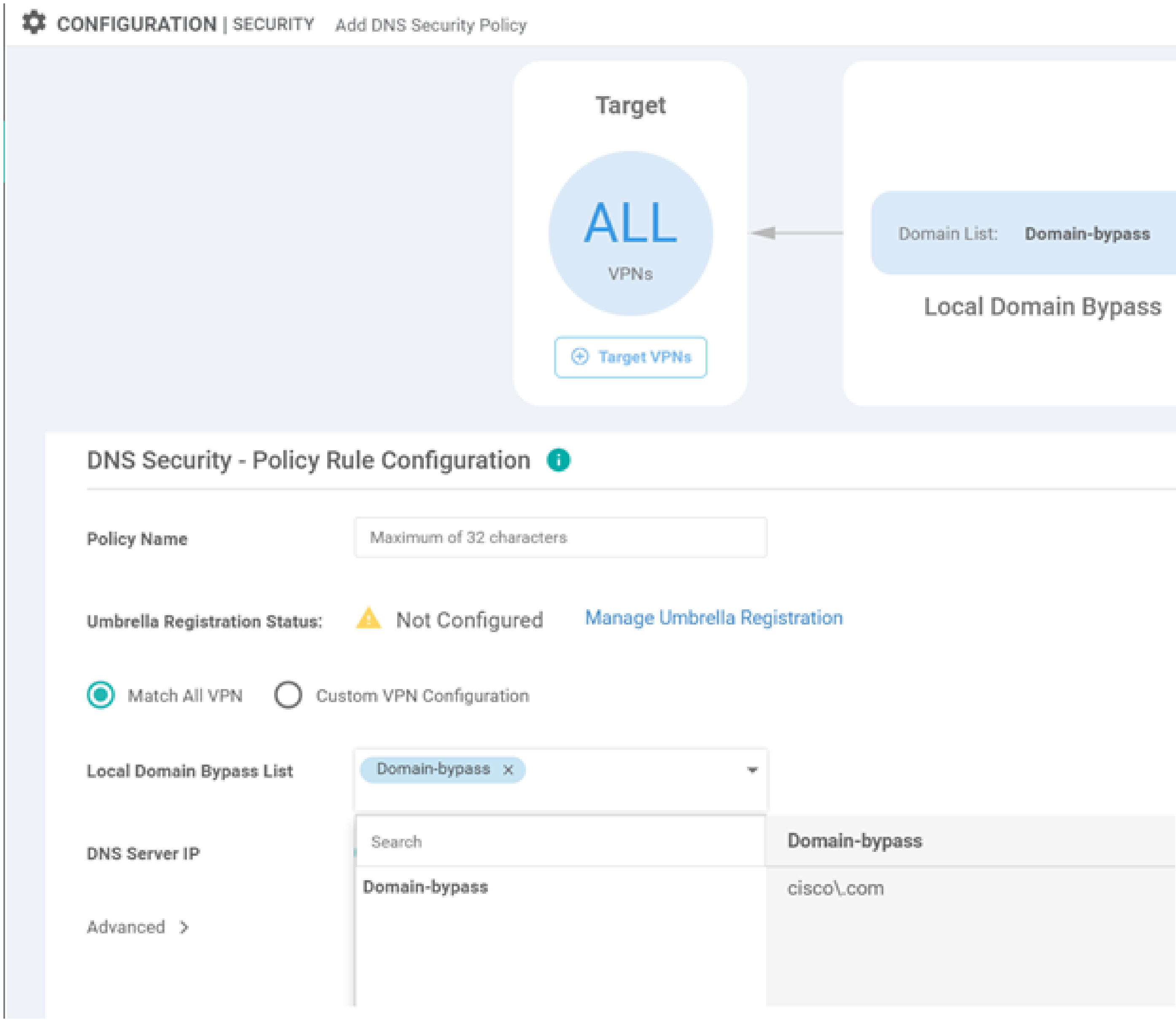



To add target VPNs, click **Target VPNs** in the Add DNS Security Policy wizard.




Click **Save Changes** to add the VPN.

13. Select the domain bypass from the **Local Domain Bypass List** drop-down as shown.

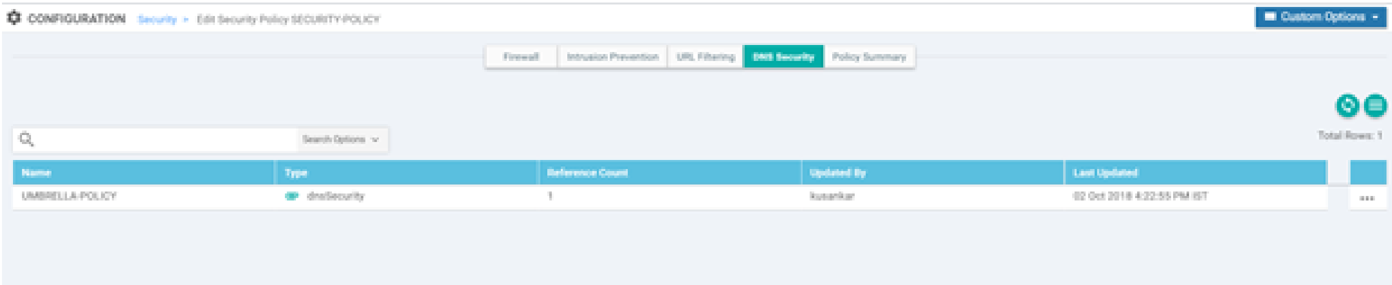



14. Configure the **DNS Server IP** from the following options:

- Umbrella Default
- Custom DNS

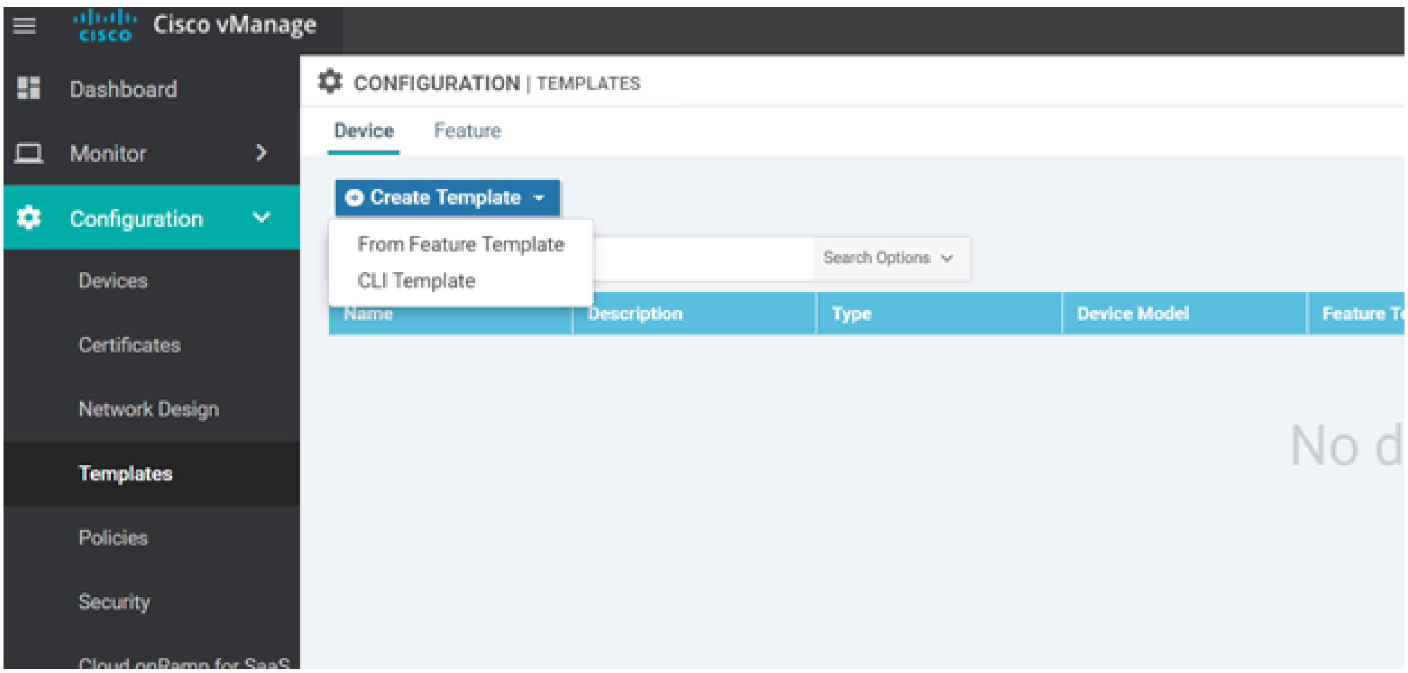
15. Click on the **Advanced** tab to enable or disable the DNSCrypt. By default, the DNSCrypt is enabled.

16. Click **Save DNS Security Policy** to configure DNS Security policy. The Configuration ► Security screen is then displayed, and the DNS Policy list table includes the newly created dns security policy.




## Applying DNS Umbrella Policy to a IOS XE Router

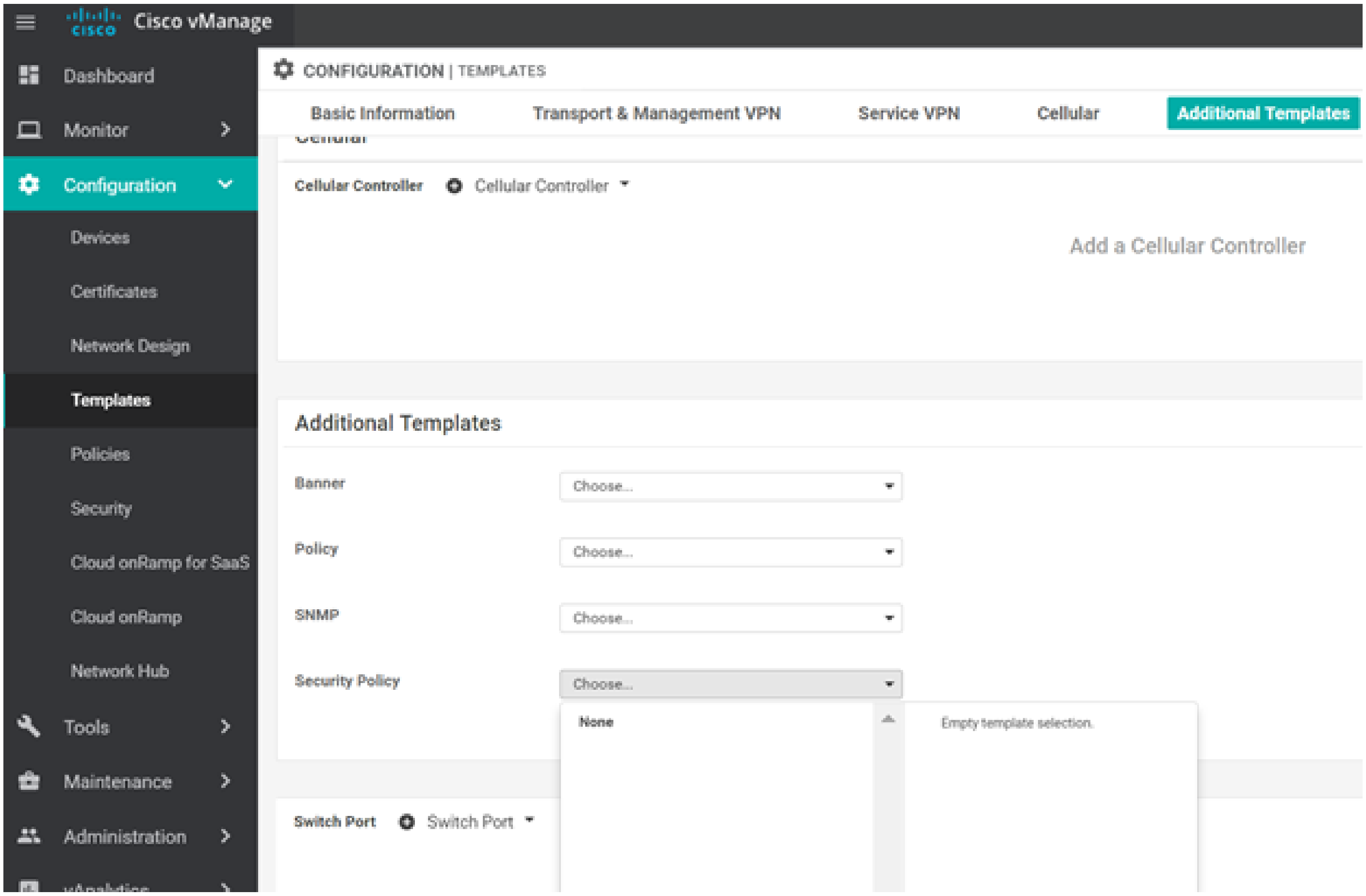
1. In vManage NMS, select the Configuration ▶ Templates screen.




2. In the **Device** tab, from the Create Template drop-down, select **From Feature Template** .

3. From the Device Model drop-down, select one of the IOS XE devices.

4. Click the **Additional Templates** tab located directly beneath the **Description** field. The screen scrolls to the **Additional Templates** section.




5. From the Security Policy drop-down, select the name of the Umbrella DNS Security Policy you configured in the above procedure.

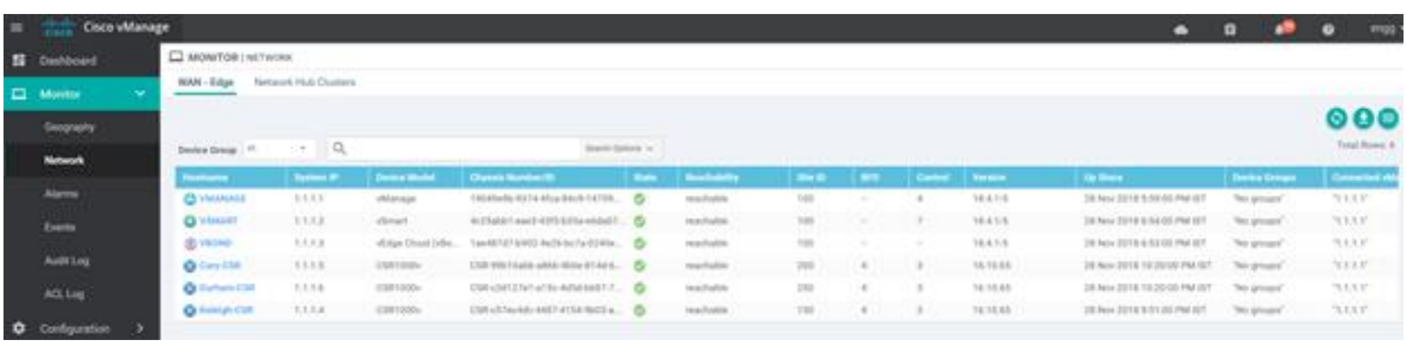
6. Click **Create** to apply Umbrella policy to a device.

## Monitoring Umbrella Feature

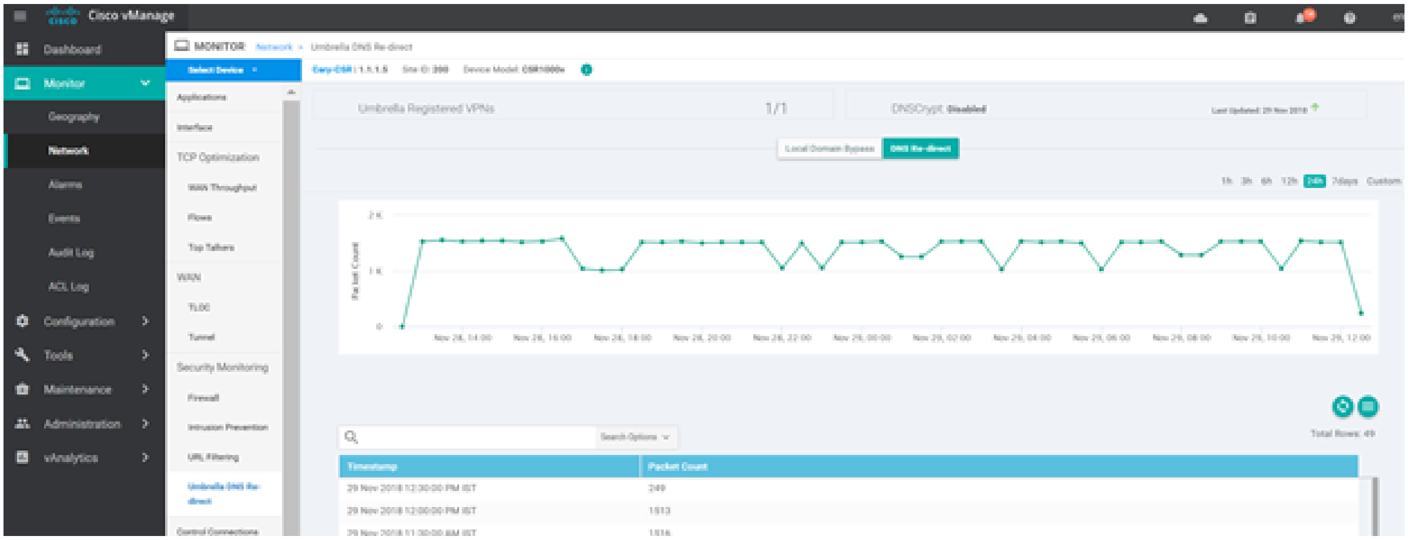
You can monitor the registered VPNs, DNSCrypt status, packet counts for required timestamps on a umbrella configured router using the following steps.

To monitor the status of Umbrella DNS Configuration on IOS XE device:

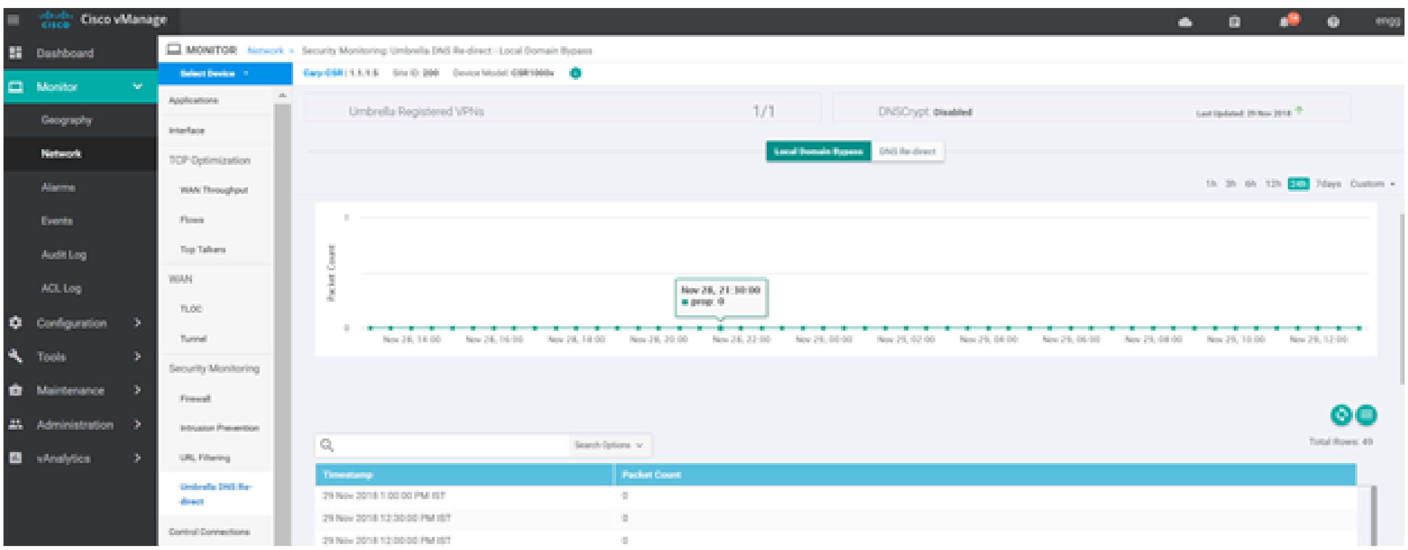
1. From the Monitor ► Network screen, select an IOS XE device.



2. In the left panel, under Security Monitoring, select **Umbrella DNS Re-direct** tab. The Umbrella DNS Re-direct wizard displays showing how many packets are redirected to configured DNS server.




3. Click on **Local Domain Bypass** to monitor the packet counts showing how many packets are bypassed to DNS server.




How to configure Umbrella policy with a configuration wizard.

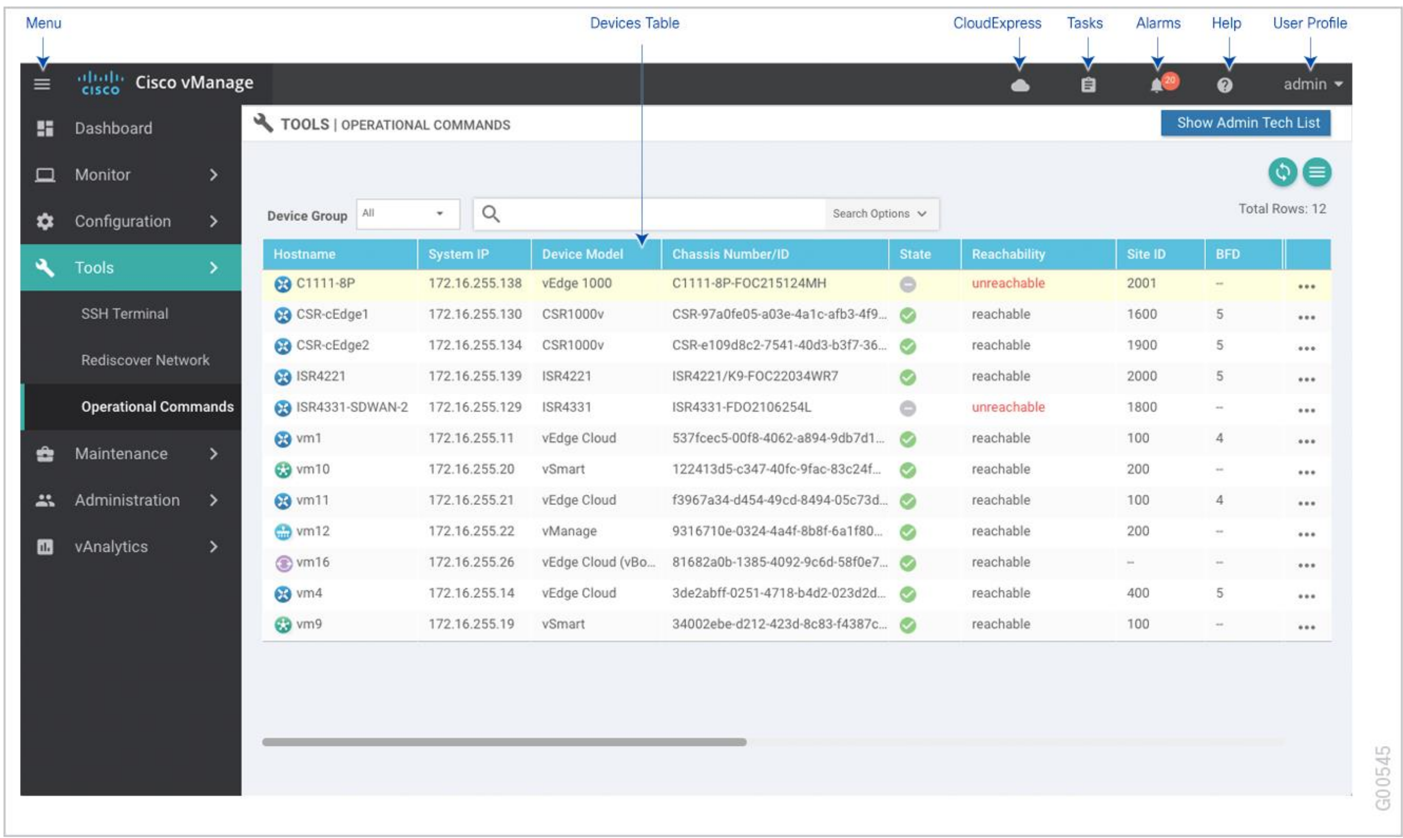
# Tools

## Operational Commands

Use the Operational Commands screen to run, on Viptela devices, a group of two or more operational commands as a single command.

## Screen Elements

- Top bar—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.
- Title bar—Includes the title of the screen, Operational Commands.
  - Show Admin Tech List button—Click to display a list of all requests to generate admin-tech file.
- Device Groups drop-down—Lists all configured device groups in the network.
- Search box—Includes the Search Options drop-down, for a Contains or Match string.
- Refresh icon—Click to refresh data in the device table with the most current data.
- Show Table Fields icon—Click to display or hide columns from the device table. By default, all columns are displayed.
- Table of devices in the overlay network—To re-arrange the columns, drag the column title to the desired position.



## Admin Tech Command

Use the Admin Tech command to collect system status information for a device in a tar file, to aid in troubleshooting and diagnostics.

1. From the device table, select the device.
2. Click the More Actions icon to the right of the row and click Admin Tech.
3. In the Generate admin-tech File window, limit the contents of the Admin Tech tar file if desired:
    a. The Include Logs checkbox is selected by default. Deselect this checkbox to omit any log files from the compressed tar file. Log files are stored in the /var/log/directory on the local device.
    b. Select the Include Cores checkbox to include any core files. Core files are stored in the /var/crash directory on the local device.
    c. Select the Include Tech checkbox to include any files related to device processes (daemons) and operations. These files are stored in the /var/tech directory on the local device.
4. Click Generate. A tar file is created which contains the contents of various files on the local device. This file has a name similar to 20150709-032523-admin-tech.tar.gz, where the numeric fields are the date and time.
5. Send the admin-tech.tar.gz file to your Viptela customer support contact.

## Interface Reset Command

Use the Interface Reset command to shutdown and then restart an interface on a device in a single operation, without having to modify the device's configuration.

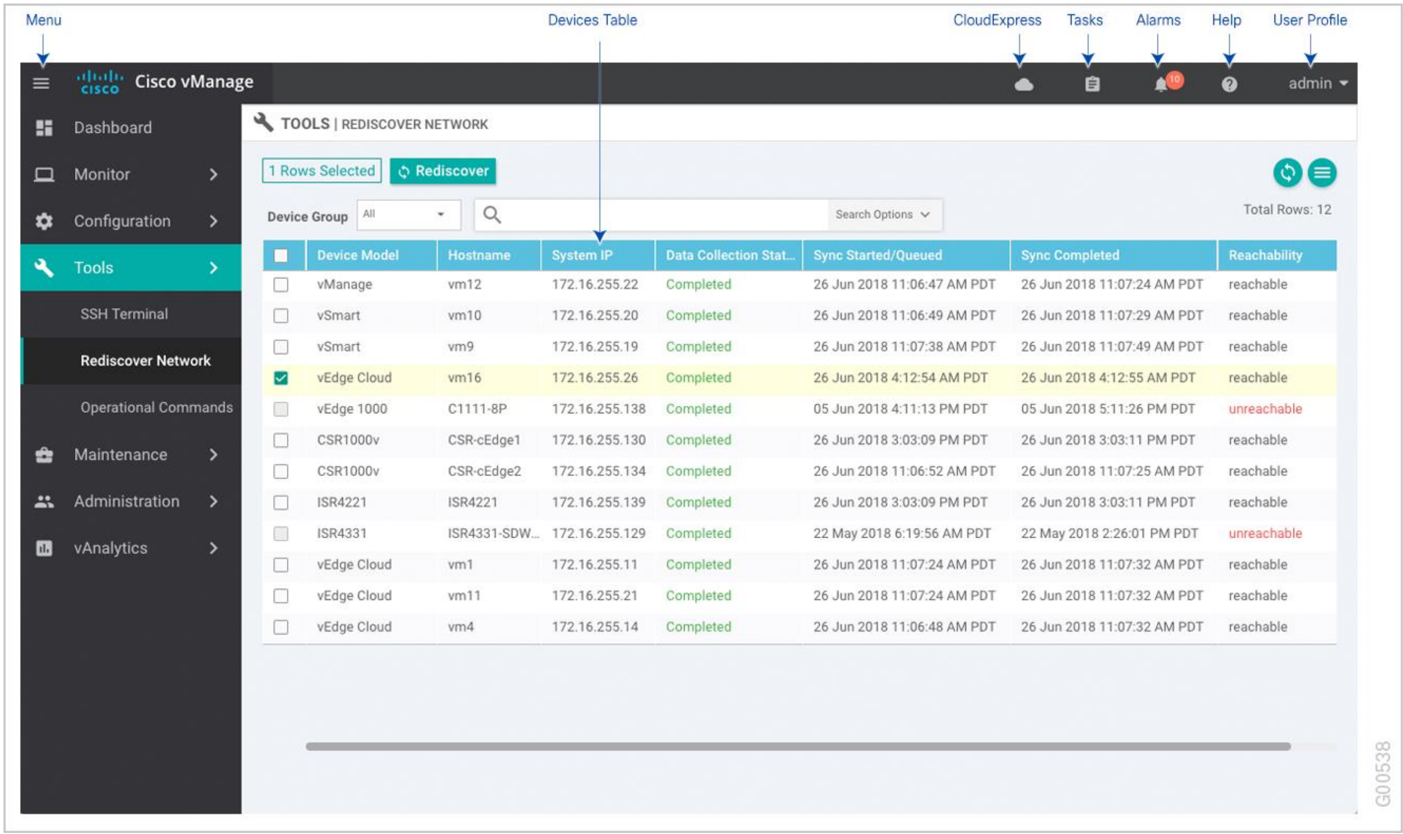
1. From the device table, select the device.
2. Click the More Actions icon to the right of the row and click Interface Reset.
3. In the Interface Reset window, select the desired interface.
4. Click Reset.

## Rediscover Network

Use the Rediscover Network screen to locate new devices in the overlay network and synchronize them with the vManage NMS.

## Screen Elements

- Top bar—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.
- Title bar—Includes the title of the screen, Rediscover Network.
- Rows Selected—Displays the number of rows selected from the table.
    - Rediscover button—Click to rediscover the devices in the network.
- Device Groups drop-down—Lists all configured device groups in the network.
- Search box—Includes the Search Options drop-down, for a Contains or Match string.
- Refresh icon—Click to refresh data in the device table with the most current data.
- Show Table Fields icon—Click to display or hide columns from the device table. By default, all columns are displayed.
- Table of devices in the overlay network—To re-arrange the columns, drag the column title to the desired position.




## Rediscover the Network

To locate new devices in the overlay network, click the Rediscover button located directly beneath the title bar. vManage NMS rediscovers every device and link and displays updated information about the network.

## Synchronize Device Data

To synchronize the data on a specific device with the vManage NMS:

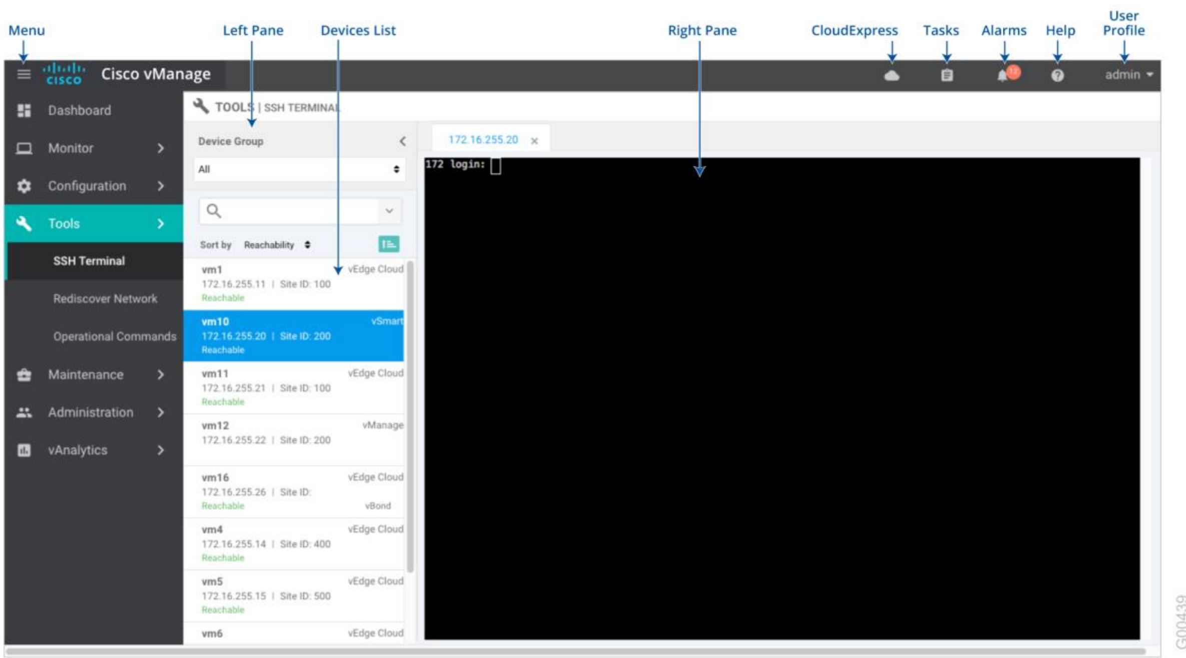
1. From the Device Groups drop-down list, select the device group to which the device belongs. The device table lists all the devices in the selected group.
2. Select the device.
3. Click the Rediscover button.
4. In the Rediscover Network window, click Rediscover to confirm re-synchronization of the device data.

## SSH Terminal

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

## Screen Elements

- Top bar—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.
- Title bar—Includes the title of the screen, SSH Terminal.
- Left pane—Includes:
    - Device Groups drop-down—Lists all configured device groups in the network.
    - Search box—Includes the Search Options drop-down, for a Contains or Match string.
    - Sort by drop-down options. You can sort the device list by reachability, hostname, system IP, site ID, or device model.
    - List of all Viptela devices in the selected device group.
- Right pane—Includes:
    - An open SSH window. The size of the window is based on the current browser size, and it does not readjust if you change the window size. A vertical scroll bar allows you to scroll up and down in the SSH window.




## 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.

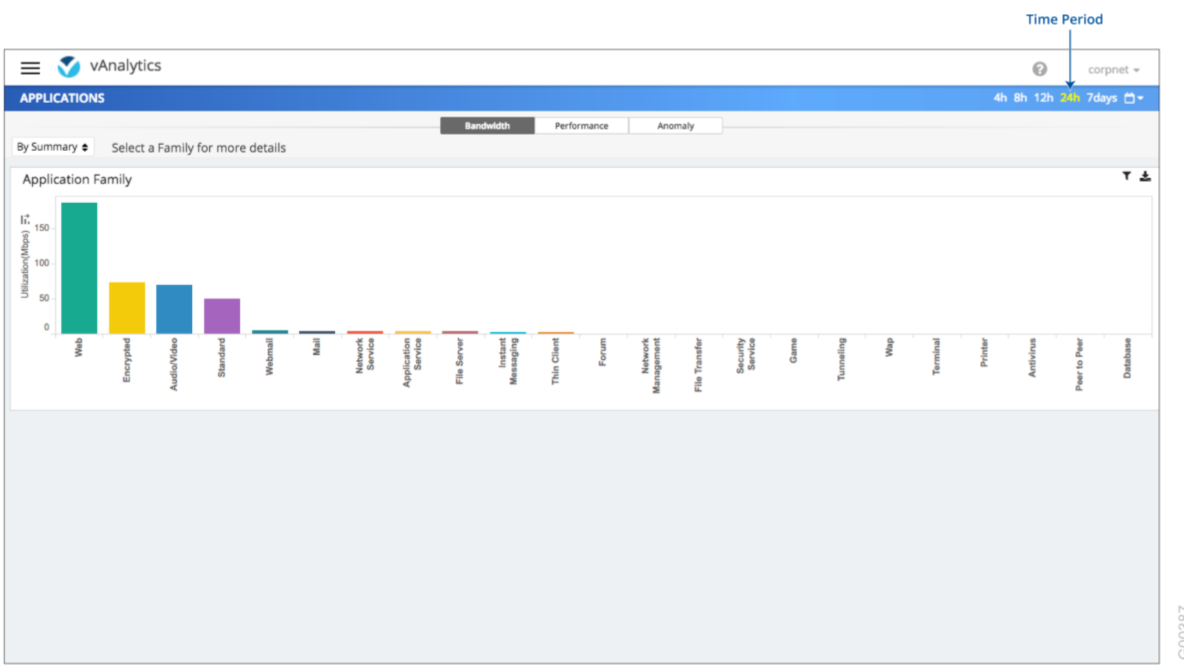
# vAnalytics

## Applications

Use the Applications screen to monitor application families and individual applications in your overlay network over time.

## Screen Elements

- Top bar—On the left are the menu icon, for expanding and collapsing the vAnalytics menu, and the vAnalytics product name. On the right are a number of icons and the user profile drop-down.
- Title bar—Includes the title of the screen, Applications.
  - Time Period—Click a predefined or custom time period for which to display data.
- Bandwidth—Displays bandwidth utilization for application families.
- Performance—Displays Viptela Quality of Experience (vQoE) values for application families. The vQoE value ranges from zero to ten, with zero being the worst performance and ten being the best. vQoE calculates this value based on latency, loss, and jitter, customizing the calculation for each application.
- Anomaly—Displays application families using more bandwidth than their baseline.




## Display Bandwidth Utilization

To display bandwidth utilization for application families:

1. Click Bandwidth.
2. Click the Filter icon to select a specific application family to view.
3. Click the PDF icon to open a PDF version of the chart in a new tab.

4. Hover over an item in any chart to open a hover box with details about that item.

5. Select a view: By Summary, By Time, or By Sites:

   – By Summary displays a summary by application family. Click an application family to display applications in that family. Click an application to see that application's bandwidth utilization over time. Click a point on the timeline to see that application's bandwidth utilization by site. Click a site to see flows for that application at that site.

   – By Time displays a timeline of application family bandwidth utilization. Click an application family to display utilization for the applications in that family. Click an application to display utilization at each site running the application. Click a site to display flows for that application at that site.

   – By Sites displays bandwidth utilization on each vEdge router. Click a site to display a timeline of application family bandwidth utilization at that site. Click an application family to display utilization for applications in that family at that time. Click an application to display flows for that application at that site.

## Display vQoE Values

To display vQoE values for each application family:

1. Click Performance.

2. Click the Filter icon to select a specific application family to view.

3. Click the PDF icon to open a PDF version of the chart in a new tab.

4. Hover over an application family in the chart to open a hover box with details for that application family.

5. Click an application family to display average latency, loss, jitter, and vQoE for each application in that family:

   a. Click an application to display that application's performance on each device in the tunnel.

   b. Click a device to display an hourly summary of that application on that device.

## Display Deviations from Baseline Utilization

vAnalytics platform computes daily averages and standard deviations for application families at every site in a rolling window of seven days. An anomaly occurs if an application family's bandwidth utilization exceeds the average plus two times the standard deviation.

To display deviations from baseline values of bandwidth utilization for application families:

1. Click Anomaly.

2. Click the Filter icon to select a specific application family to view.

3. Click the PDF icon to open a PDF version of the chart in a new tab.

4. Hover over an application family in the chart to open a hover box with details for that application family.

5. Click a site to see a timeline of anomalies for that site.

6. Click an hour on the timeline to see anomalous behavior of individual applications in that hour.

## Network Availability

Use the Network Availability screen to monitor downtime of nodes and circuits in your overlay network over time.

## Screen Elements

- Top bar—On the left are the menu icon, for expanding and collapsing the vAnalytics menu, and the vAnalytics product name. On the right are a number of icons and the user profile drop-down.
- Title bar—Includes the title of the screen, Network Availability.
  - Time Period—Click a predefined or custom time period for which to display data.
- Selected View—Displays downtime by sites or by time.
- Summary—Displays node and circuit downtime summaries.


## Display Downtime by Site

To display vEdge router and circuit downtime for each site:

1. Select Aggregated Downtime by Sites.
2. Click the Filter icon to select specific application family to view.
3. Click the PDF icon to open a PDF version of the chart in a new tab.
4. Click a vEdge router or circuit to display details about that downtime event.

## Display Downtime by Time

To display vEdge router and circuit downtime for a specified time period:

1. Select Aggregated Downtime by Time.
2. Select a length of time: Day, Week, Quarter, or Year.
3. Click the Filter icon to select specific device or circuit to view.

4. Click the PDF icon to open a PDF version of the chart in a new tab.

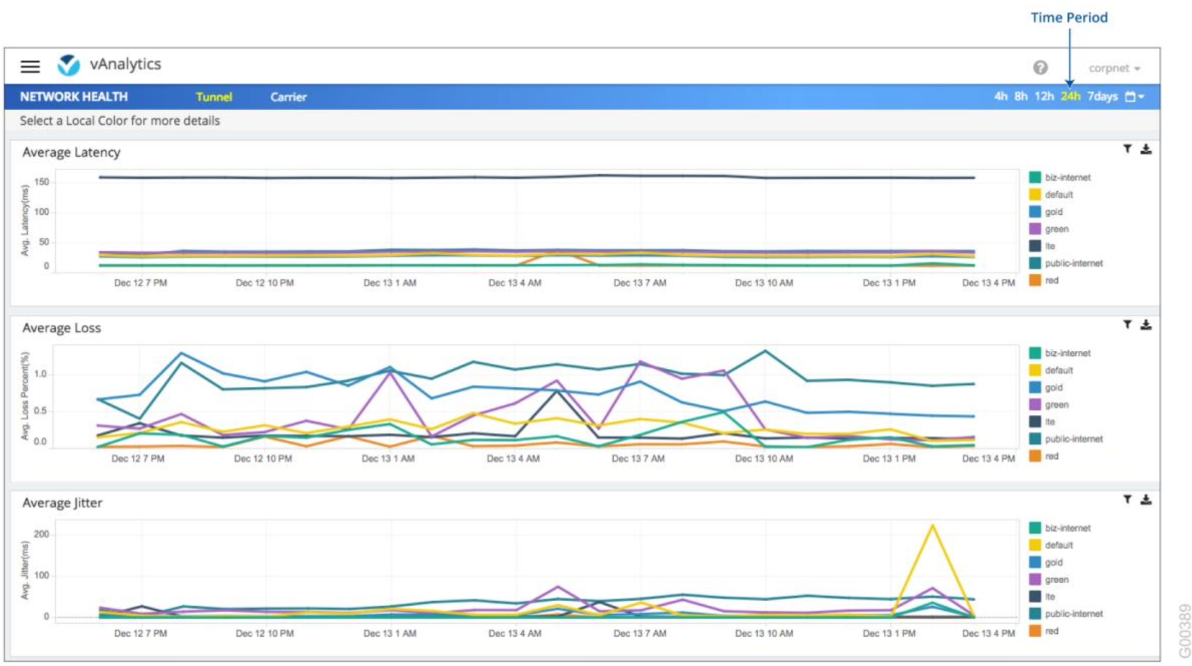
5. Click a vEdge router or circuit to display details about that downtime event.

# Network Health

Use the Network Health screen to monitor the performance of circuits, tunnels, and carriers in your overlay network over time.

# Screen Elements

- Top bar—On the left are the menu icon, for expanding and collapsing the vAnalytics menu, and the vAnalytics product name. On the right are a number of icons and the user profile drop-down.
- Title bar—Includes the title of the screen, Network Health.
  - Tunnel—Displays latency, loss, and jitter by circuit.
  - Carrier—Displays application performance by carrier on a geographical map of your overlay network.
  - Time Period—Click a predefined or custom time period for which to display data.




# Display Latency, Loss, and Jitter on Circuits

To display graphs for latency, loss, and jitter on each circuit in your overlay network:

1. Click Tunnel. Each line in the graphs indicates one circuit. The legend to the right indicates the color of each circuit.

2. Click the Filter icon to select specific circuits to view.

3. Click the PDF icon to open a PDF version of the graph in a new tab.

4. Hover over a point on a line to open a hover box with details for that point in time.

5. Click a point on a line to display average latency, loss, or jitter in that circuit at that point in time:
    a. Click a site to see latency, loss, or jitter for all tunnels at that site.
    b. Click a tunnel to see hourly latency, loss, or jitter for that tunnel.
    c. Click Overview to return to Network Health ► Tunnel.
6. To highlight specific circuits:
    a. Click a circuit in the legend to select it. To select more than one circuit, hold down the Shift key.
    b. Click the Highlight icon that appears. The selected circuits are highlighted on the map.
    c. To display all circuits again, click the Highlight icon.

## Display Application Performance by Carrier

To display application performance by carrier on a geographical map of the overlay network:

1. Click Carrier. Circles on the map represent each carrier. The legend to the right indicates the color of each carrier.
2. Select Latency, Loss, or Jitter to change the data displayed.
3. Click the Filter icon to select specific carriers to view.
4. Click the PDF icon to open a PDF version of the map in a new tab.
5. Hover over a carrier's circle to display a hover box with details for that location.
6. Click a circle on the map to display that location's performance by loss, latency, or jitter:
    a. Click a point on the graph to see a graph of performance for each carrier at that location.
    b. Click a carrier to see performance for each vEdge router at that site.
    c. Click a vEdge router to see that device's performance over time.
    d. Click Overview to return to Network Health ► Carrier.
7. Hover over the map to display map functions:
    a. Click Search to search for a geographical location by name.
    b. Click the + (plus) or - (minus) zoom icons to zoom in or out.
    c. Click Home to return to the world-wide view.
    d. Hover over the right arrow for other map functions, such as selecting a zoom area and panning.
8. To highlight specific carriers:
    a. Click a carrier in the legend to select it. To select more than one carrier, hold down the Shift key.
    b. Click the Highlight icon that appears. The selected carriers are highlighted on the map.
    c. To display all carriers again, click the Highlight icon.

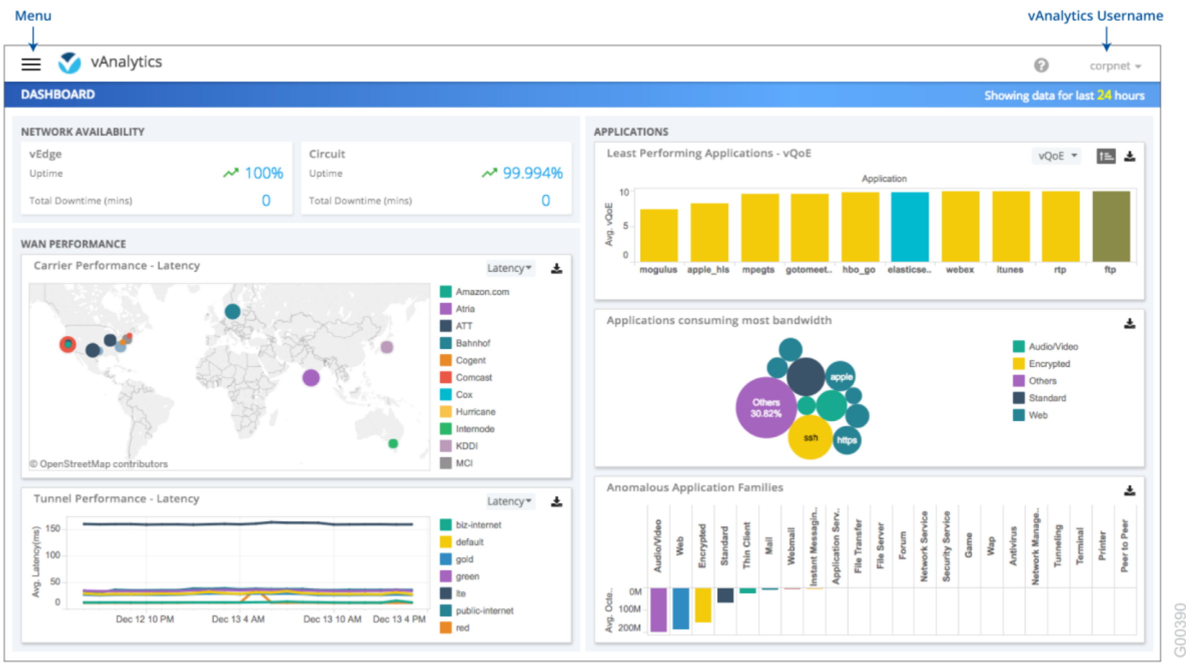
## vAnalytics Dashboard

Use the vAnalytics dashboard screen to monitor the performance of the entire Viptela overlay network over time.

## Top Bar

The top bar is located at the top of every vAnalytics screen and includes the following screen elements:

- Menu icon—Click the icon to expand or collapse the vAnalytics menu. The vAnalytics menu is closed by default.
- vAnalytics product name.
- Help—Links to product help and software version information about the vAnalytics platform.
- vAnalytics username—Username for the vAnalytics platform that you are logged into. Includes the sign-out button.




## Network Availability Pane

The Network Availability pane displays network-wide availability for the last 24 hours by device and circuit. Each box displays uptime as a percentage and total downtime in minutes.

Click in the Device box to display downtime for each vEdge router in the overlay network. Click in the Circuit box to display downtime for each circuit in the overlay network.

- Click the Filter icon to select a specific vEdge router or circuit to view.
- Click the PDF icon to open a PDF version of the chart in a new tab.
- Click any bar to display the time period when that device or circuit was down.

## Applications Pane

The Applications Pane displays application performance for the last 24 hours in three views: Least Performing Applications, Applications Consuming Most Bandwidth, and Anomalous Application Families.

## Least Performing Applications

The Least Performing Applications box displays the applications in the network with the lowest performance.

vAnalytics platform calculates application performance with the Viptela Quality of Experience (vQoE) value. This value ranges from zero to 10, with zero being the worst performance and 10 being the best. vQoE combines scores for latency, loss, and jitter, customizing the calculation for the needs of each application.

- Select vQoE, Latency, Loss, or Jitter to change the data displayed.
- Click the Sort icon to toggle between Least Performing Applications and Top Performing Applications.
- Click the PDF icon to open a PDF version of the chart in a new tab.
- Hover over a bar in the graph to open a hover box with details about that application.
- Click a bar in the graph to display that application's performance on each tunnel. Click a tunnel to display the application's hourly performance on that tunnel.

## Applications Consuming Most Bandwidth

The Applications Consuming Most Bandwidth box displays applications consuming the most bandwidth in the network.

Each circle represents an application; the larger the circle, the greater is the bandwidth that it consumes. The legend to the right indicates the color of each application family. The graph displays the top ten applications using the most bandwidth, and an additional circle called Others. Click Others for details about any remaining applications.

- Click the PDF icon to open a PDF version of the graph in a new tab.
- Hover over a circle in the graph to open a hover box with details about that application.
- Click a circle in the graph to display that application's bandwidth consumption over time. Click a point on the graph to display sites using that application. Click a site to display flows for that site.
- To highlight specific application families:
    a. Click a family in the legend to select it. To select more than one family, hold down the Shift key.
    b. Click the Highlight icon that appears. The selected carriers are highlighted on the map.
    c. To display all families again, click the Highlight icon.

## Anomalous Application Families

The Anomalous Application Families box displays application families using more bandwidth than their baseline.

- Click the PDF icon to open a PDF version of the chart in a new tab.
- Hover over a bar in the graph to display a hover box with details about that application family.
- Click a bar in the graph to display that family's average octets by site. Click a bar in the graph to display that site's octets over time for that family. Click a bar in the timeline to display octets at that point in time for each application in the family.

# WAN Performance Pane

The WAN Performance pane displays performance of carriers and tunnels for the last 24 hours by latency, loss, or jitter.

## Carrier Performance

The Carrier Performance box displays application performance by carrier on a geographical map of the overlay network.

Circles on the map represent each carrier. The legend to the right indicates the color of each carrier.

- Select Latency, Loss, or Jitter to change the data displayed.
- Click the PDF icon to open a PDF version of the map in a new tab.
- Hover over a carrier's circle to display a hover box with details for that location.
- Click a circle on the map to display that location's performance for the last 24 hours in graphical format. Hover over a point on the graph for details about that point in time.
- Hover over the map to display map functions:
  - Click Search to search for a geographical location by name.
  - Click the + (plus) or – (minus) zoom icons to zoom in or out.
  - Click Home to return to the world-wide view.
  - Hover over the right arrow for other map functions, such as selecting a zoom area and panning.
- To highlight specific carriers:
  a. Click a carrier in the legend to select it. To select more than one carrier, hold down the Shift key.
  b. Click the Highlight icon that appears. The selected carriers are highlighted on the map.
  c. To display all carriers again, click the Highlight icon.

## Tunnel Performance

The Tunnel Performance box displays the performance of tunnels for the last 24 hours by latency, loss, or jitter. The legend to the right indicates the color of each tunnel.

- Select Latency, Loss, or Jitter to change the data displayed.
- Click the PDF icon to open a PDF version of the chart in a new tab.
- Hover over a point on the graph to display a hover box with details about that point in time.
- To highlight specific tunnels:
  a. Click a tunnel in the legend to select it. To select more than one tunnel, hold down the Shift key.
  b. Click the Highlight icon that appears. The selected tunnels are highlighted on the graph.
  c. To display all tunnels again, click the Highlight icon.

# vManage NMS Product Help

The vManage NMS is a centralized network management system that provides a GUI interface to easily monitor, configure, and maintain all Viptela devices and links in the overlay network. The vManage NMS software runs on a server in the network.

## Browser Support

You can access the vManage NMS using the Chrome, Firefox, or Internet Explorer 11 browsers.

You can access the vManage NMS from VPN 0 (the WAN transport VPN) and from VPN 512 (the management VPN).

## vManage Dashboard

When you log into the vManage NMS, the dashboard provides a quick summary of the network.

Here, at a glance, you can view the health of the entire network including the operational state of any device, total number of reboots and crashes, and the state of all controller certificates. This visibility into the network eases the task of managing the Viptela devices.

## vManage Menu

As shown in the above figure, the menu is located to the left of the Dashboard screen. The following table lists each menu and sub-menu item and provides a brief description.

Menu Item

Description

**Dashboard**

Dashboard

Monitor, at a glance, the health of the Viptela overlay network.

**Monitor**

Geography

A map view of the entire network and displays the geographic location of the devices in the network.

Network

An inventory of all Viptela devices in the network along with detailed information on each device.

Alarms

Details on alarms generated by all Viptela devices in the network.

Events

Details on events generated by all Viptela devices in the network.

Audit Log

An audit log of all activities on Viptela devices.

**Configuration**

Devices

Add or delete devices from the overlay network.

Certificates

Manage certificates and authenticate Viptela devices in the overlay network.

Templates

Create configuration templates for a set of Viptela devices.

**Policy**

Create common policies for a set of vSmart controllers.

**Tools**

SSH Terminal

Establish an SSH session to a Viptela device.

Rediscover Network

Locate new devices in the overlay network and synchronize them with the vManage NMS.

Operational Commands

Run two or more operational commands as a single command.

**Maintenance**

Software Upgrade

Download new software images and upgrade the software image running on Viptela devices.

Device Reboot

Reboot one or more Viptela devices.

**Administration**

Settings

Configure organization name and certificate authorization settings.

Manage Users

Add, edit, or delete users and user groups from the vManage NMS.

## Bringing Up the Viptela Overlay Network

The following table lists the tasks for bringing up the Viptela overlay network using the vManage NMS.

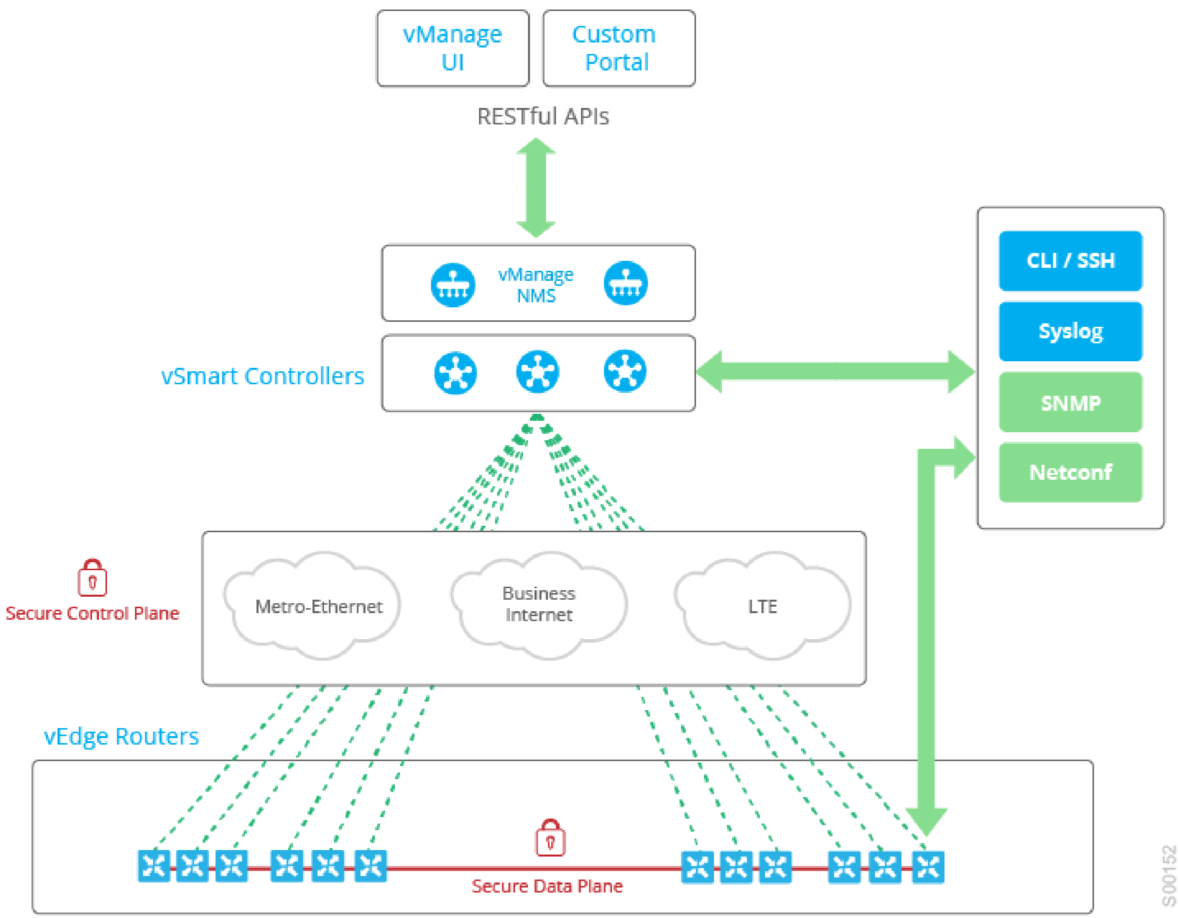
| Bringup Task | Step-by-Step Procedure |
|---|---|

| | |
|---|---|
| Step 1: Start the vManage NMS | 1. On the hypervisor, create a VM instance.<br>2. Boot the vManage NMS server, start the VM, and enter login information.<br>3. In vManage ▶ Administration ▶ Settings, configure certificate authorization settings. Select Automated to allow the certificate-generation process to occur automatically when a CSR is generated for a controller device.<br>4. In vManage ▶ Certificates, generate the CSR.<br>5. Check for a confirmation email from Symantec that your request has been received.<br>6. Check for an email from Symantec that Viptela has approved your request and the certificate is signed.<br>7. In vManage ▶ Configuration ▶ Devices, check that the certificate has been installed. |
| Step 2: Start the vBond orchestrator | 8. On the hypervisor, create a VM instance.<br>9. B oot the vBond server and start the VM.<br>10. In vManage ▶ Configuration ▶ Devices ▶ Controller, add the vBond orchestrator and generate the CSR.<br>11. Check for a confirmation email from Symantec that your request has been received.<br>12. Check for an email from Symantec that Viptela has approved your request and the certificate is signed.<br>13. In vManage ▶ Configuration ▶ Devices, check that the certificate has been installed.<br>14. In vManage ▶ Configuration ▶ Templates:<br>a. Create a configuration template for the vBond orchestrator.<br>b. Attach the template to the vBond orchestrator.<br>15. In vManage ▶ Dashboard, verify that the vBond orchestrator is operational. |
| Step 3: Start the vSmart controller | 16. On the hypervisor, create a VM instance.<br>17. Boot the vSmart server and start the VM.<br>18. In vManage ▶ Configuration ▶ Devices ▶ Controller, add the vSmart controller and generate the CSR.<br>19. Check for a confirmation email from Symantec that your request has been received.<br>20. Check for an email from Symantec that Viptela has approved your request and the certificate is signed.<br>21. In vManage ▶ Configuration ▶ Devices, check that the certificate has been installed.<br>22. In vManage ▶ Configuration ▶ Templates:<br>a. Create a configuration template for the vSmart controller.<br>b. Attach the template to the vSmart controller.<br>23. In vManage ▶ Dashboard, verify that the vSmart controller is operational. |

| | |
|---|---|
| Step 4: Configure the vEdge router | 24. In vManage ▶ Configuration ▶ Devices ▶ vEdge List, upload the vEdge authorized serial number file.<br>25. In vManage ▶ Configuration ▶ Certificates ▶ vEdge List, check that the router's chassis and serial number are in the vEdge list.<br>26. In vManage ▶ Configuration ▶ Certificates ▶ vEdge List, authorize each router by marking it Valid in the Validity column.<br>27. In vManage ▶ Configuration ▶ Certificates ▶ vEdge List, send the vEdge list to the controller devices.<br>28. In vManage ▶ Configuration ▶ Templates:<br>a. Create a configuration template for the vEdge router.<br>b. Attach the template to the vEdge router. |
| Step 5: Connect AC power and boot the vEdge router | 29. Connect AC power to the vEdge router.<br>30. If needed, flip the On/Off switch on the rear of the router to the ON position.<br>31. In vManage ▶ Dashboard or in vManage ▶ Monitor ▶ Network ▶ Device Dashboard, verify that the vEdge router is operational. |

## RESTful API for vManage NMS

The vManage NMS supports a RESTful (Representational State Transfer) API, which provides calls for retrieving real-time and static information about the Viptela overlay network and the devices in the network and for uploading device configuration templates and other configuration-related information. Using the RESTful API, you can design a custom portal for interacting with the vManage NMS.




The vManage API documentation is provided as part of the vManage software, at the URL https:// *vmanage-ip-address* /apidocs. (More accurately, the full URL includes the vManage port number, https:// *vmanage-ip-address* :8443/apidocs.) *vmanage-ip-address* is the IP address of the vManage server.

API calls are provided for the following categories of operations:

- Certificate Management
- Configuration
- Device and Device Inventory
- Monitoring
- Real-Time Monitoring
- Troubleshooting Tools

For each group of API calls, click Show/Hide to list the individual calls and the URL for each call. Each call shows its response class, required parameters, and response messages (status codes).

To display the request URL for each API call and the format of the response body, click the Try It Out button. The request URL consists of the vManage NMS's URL, followed by /dataservice. For example, https://10.0.1.32:8443/dataservice/device/interface/statistics/ge0/0?deviceId=172.16.255.11

Below are a few examples of the URLs to use for API calls:

| Requested Information | API Call |
|---|---|
| List all network devices | dataservice/device |
| Health status of hardware device components, such as CPU, memory, fan, and power | dataservice/device/hardware/environment?deviceId= *system-ip-address* |
| Status of a device's transport interfaces | dataservice/device/interface?deviceId= *system-ip-address* &port-type=transport |
| Interface statistics, errors, and packet drops | dataservice/device/interface?deviceId= *system-ip-address* |
| DTLS/TLS control connection status | dataservice/device/control/connections?deviceId= *system-ip-address* |
| OMP peering | dataservice/device/omp/peers?deviceId= *system-ip-address* |
| BGP peering on the service side | dataservice/device/bgp/neighbors?deviceId= *system-ip-address* |