

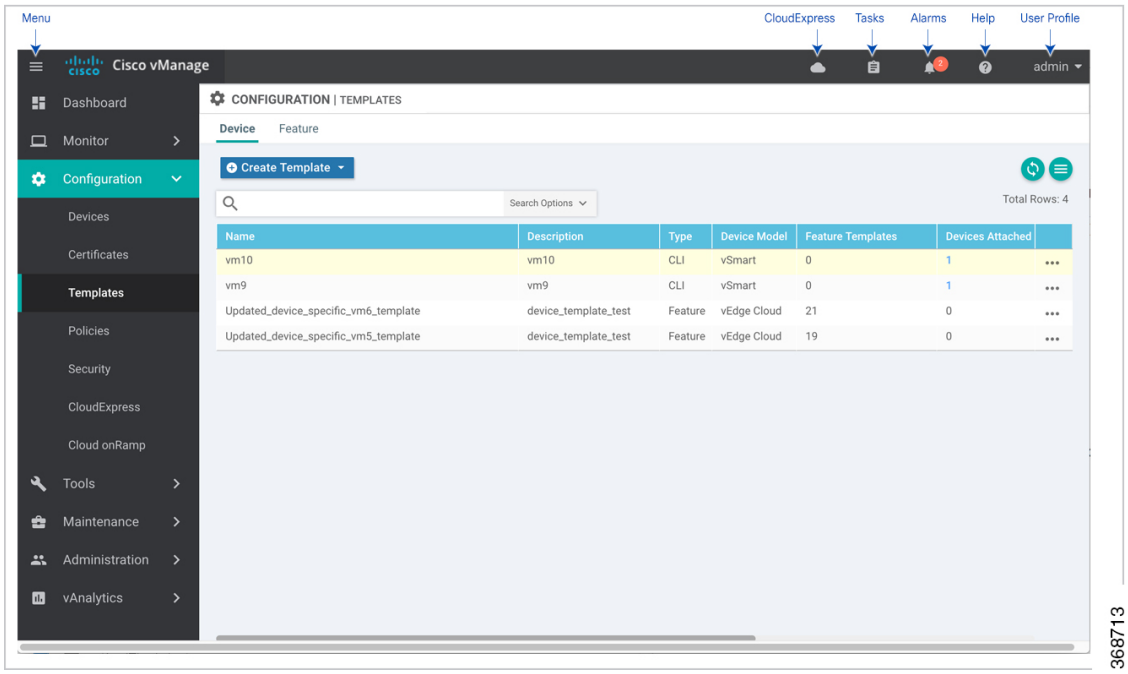
Create a Device Template from Feature Templates

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, 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:

Figure 1: Create a Device Template in Cisco vManage



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:

Table 1:

Parameter Scope	Scope Description
Device Specific (indicated by a host icon)	Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a device to a device template . When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a device to a device template. For more information, see Use Variable Values in Configuration Templates . To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.

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

1. 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 device to a device template.
2. Click Save.
3. 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.
4. 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.

• Configure Devices, on page 4

Configure Devices

Create a Device CLI Template

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.

Manage Device Templates

Edit a Device 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.

Delete a Template

Deleting a template does not remove the associated configuration from devices.

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.

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.

View Device Templates

•

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.

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.

Attach and Detach a Device Template

On Cisco Cisco vEdge 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.

1. Click Update
2. 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.
3. 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.
4. If you are attaching a Cisco vEdge device, 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.

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.

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 Cisco vEdge device 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 Device 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.

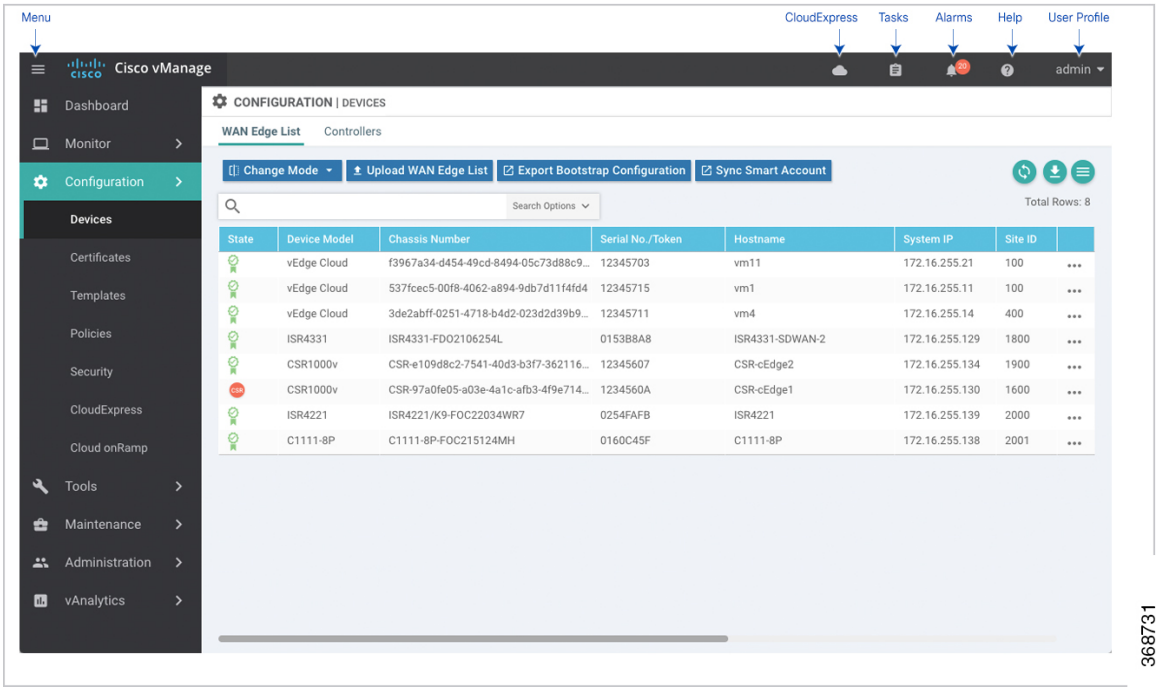
After you have pushed the configuration to a device, you can change the value assigned to any variable:

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.

Configuring Devices using vManage

Use the **Devices** screen to add and delete devices, toggle the mode of a device between CLI and vManage, upload the WAN Edge Serial number file, export bootstrap configuration and, and perform other device-related tasks.



Change Configuration Modes

A device can be in either of these configuration modes:

- vManage mode–A template is attached to the device and you cannot change the configuration on the device by using the CLI.
- CLI mode – No template is attached to the device and the device can be configured locally by using the CLI.

When you attach a template to a device from vManage, it puts the device in vManage mode. You can change the device back to CLI mode if needed to make local changes to its configuration.

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 Cisco vEdge devices in the overlay network. You retrieve a serial number file from the Cisco Plug-and-Play (PnP) portal and upload it to the vManage NMS. Then, from the vManage NMS, you send it to the controllers in the network. This file is required to allow the Cisco SD-WAN 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 Cisco SD-WAN.
   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

Chassis and serial numbers of all valid Cisco vEdge devices in the overlay network are required to allow the Cisco SD-WAN 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 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

In an overlay network, you might have multiple devices of the same type that have identical or effectively identical configurations. For example, in a network with redundant Cisco vSmart Controllers, each controller must be configured with identical policies. Another example is a network with Cisco vEdge devices at multiple sites, where each Cisco vEdge device is providing identical services at each site.

Because the configurations for these devices are essentially identical, you can create one set of feature templates, which you then consolidate into one device template that you use to configure all the devices. You can create an Excel file in CSV format that lists the variables and defines each device specific variable value for each device. Then you can load the file when you attach a device template to a device.

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.

View and Copy Device Configuration

View a Device's Running Configuration

Running configuration is configuration information that vManage obtains from the memory of a device. This information can be useful for troubleshooting.

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 Local Configuration

Local configuration is configuration that vManage has stored for a device. This information can be useful for troubleshooting or for determining how to access a device if, for example, a device is not reachable from vManage.

To view a device's local 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.

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 Cisco vEdge device 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.

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. Delete a router if you need to remove it from your deployment.

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.

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 Template Log and Device Bringup

View Log of Template Activities

A log of template activities contains information that relates to creating, editing, and deleting configuration templates, and the status of attaching configuration templates to devices. This information can be useful for troubleshooting.

To view a log of template activities:

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

You can view the status of the operations involved in bringing a router or controller up in the overlay network. This information can help you monitor these operations.

To view the status of a device bringup:

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 Cisco vBond Orchestrator

A Cisco vBond Orchestrator automatically orchestrates connectivity between Cisco vEdge devices and vManage controllers. If any Cisco vEdge device or Cisco vSmart Controller is behind a NAT, the Cisco vBond Orchestrator also serves as an initial NAT-traversal orchestrator. To add a Cisco 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 Cisco vBond Orchestrators.

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

Configure Cisco vSmart Controllers

Add a vSmart Controller

After the Cisco vBond Orchestrator authenticates Cisco vEdge devices, the Cisco vBond Orchestrator provides Cisco vEdge devices information that they need to connect to the Cisco vSmart Controller. A Cisco vSmart Controller controls the flow of data traffic throughout the network via data and app-route policies. To configure Cisco vSmart Controllers:

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 Cisco vSmart Controller.
   b. Enter the username and password to access the Cisco vSmart Controller.
   c. Select the protocol to use for control-plane connections. The default is DTLS. The DTLS (Datagram Transport Layer Security) protocol is designed to provide security for UDP communications.
   d. If you select TLS, enter the port number to use for TLS connections. The default is 23456.

      The TLS (Transport Socket Layer) protocol that provides communications security over a network.
   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 Cisco vSmart Controllers. The vManage NMS can support up to 20 Cisco vSmart Controllers in the network.

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

Edit Controller Details

Editing controller details lets you update the IP address and login credentials of a controller device. To edit controller details:

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

Deleting a controller removes it from the overlay. Delete a controller it if you are replacing it or if you no longer need it in your network.

To 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 Cisco vSmart Controller:

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 Cisco 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.

Create a UCS-E Template

Table 2: Feature History

Feature Name	Release Information	Feature Description
Create a UCS-E Template		This feature allows you to connect a UCS-E interface with a UCS-E server through the interface feature template.

For more information about the Cisco Unified Computing System (UCS) E-Series Servers, see the Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine Hardware Installation Guide.

1. From the vManage menu, select Configuration ► Templates.
2. Click Feature.
3. Click Add Template.
4. Select a Cisco XE SD-WAN device from the list.

5. From the Other Templates section, click UCSE.

   The UCSE Feature template opens. The top of the form contains fields for naming the template, and the bottom contains fields for configuring the Integrated Management Controller (IMC).

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.

Configure Bay and Slot for Template

Click the Basic Configuration tab to configure the bay and the slot for the template.

Parameter Name	Description
Bay	Specify the number for the SAS drive bays.
Slot	Specify the slot numbers for the mezzanine adapters.

IMC Configuration

Click the IMC tab to configure the IMC parameters for the template.

Parameter Name	Description

Access Port	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.
	
	Not all hardware models have a dedicated access port. See the Release Notes for your Cisco SD-WAN release for the supported hardware.
	
	Available options:
	
	• Dedicated
	
	• Shared
	
	The type of port, GE or TE, depends on the hardware model.
	
	For example:
	
	`Router(config-ucse)#imc access-port shared-lom ?`
	`GE1 GE1`
	`TE2 TE2`
	`TE3 TE3`
	`console Console`
	`failover Failover`
	
	Some hardware models have GE ports whereas some have TE ports.
	
	Depending on the hardware module, the appropriate port (GE or TE) needs to be configured. Otherwise you will get an error.
	
	• You can obtain the UCS-E module hardware model type by using the following commands:
	
	show inventory
	
	show platform
	
	• Failover - sub-option under Shared.
	
	For example:
	
	`Router(config)#ucse subslot 1/0`
	
	`Router(config-ucse)#imc access-port ?`
	`MGMT MGMT Interface`
	`shared-lom Shared LOM`
	
	`Router(config-ucse)#imc access-port shared-lom ?`
	`GE1 GE1`
	`TE2 TE2`
	`TE3 TE3`
	`console Console`
	`failover Failover`

IPv4 Address	Provide the UCS-E management port address.

Parameter Name	Description
Default Gateway	Gateway tracking determine, for static routes, whether the next hop is reachable before adding that route to the device's route table. Default: Enabled.
VLAN ID	Provide the VLAN number, which can be a value from 1 through 4094.
Assign Priority	Assign the priority.

Parameter Scope	Scope Description
Global (indicated by a globe icon)	Enter a value for the parameter and apply that value to all devices.
Device Specific (indicated by a host icon)	Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Cisco SD-WAN device to a device template. When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Cisco SD-WAN device to a device template. To change the default key, type a new string and move the cursor out of the Enter Key box.
Default	When Default is selected, this field is not enabled.