
Certificates

Use the Certificates screen to manage certificates and authenticate Viptela 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.
- vEdge authorized serial number file contains the serial numbers of all valid vEdge routers in your network. You receive this file from Viptela, mark each vEdge 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 vEdge 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.
- vEdge List tab—Install the vEdge 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 vEdge List tab is selected.
 - Send to Controllers—Send the vEdge router chassis and serial numbers to the controllers in the network.
 - Table of vEdge 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.
 - 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.

Menu

Cisco vManage

CONFIGURATION | CERTIFICATES

vEdge List Controllers

Send to Controllers

Search Options

Total Rows: 5

| Stat... | Device Model | Chassis Number | Serial No./Token | Hostname | IP Address | Validate |
|---------|--------------|--------------------------------------|------------------|----------|---------------|---------------------------|
| ✓ | vEdge Cloud | 56b09249-058d-4a12-9641-48ad18cef50c | 12345703 | vm11 | 172.16.255.21 | Invalid Staging Valid |
| ✓ | vEdge Cloud | 1f14e297-7649-4f24-a788-89847569c2f0 | 12345711 | vm4 | 172.16.255.14 | Invalid Staging Valid |
| ✓ | vEdge Cloud | d0af68a4-50f1-4a6a-bffb-3a667d29855a | 12345715 | vm1 | 172.16.255.11 | Invalid Staging Valid |
| ✓ | vEdge Cloud | 42a65ffc-0b74-4539-9c41-eb0c08c63830 | 12345712 | vm5 | 172.16.255.15 | Invalid Staging Valid |
| ✓ | vEdge Cloud | 5826ec38-ea10-430a-b1b1-b6dcf4b7350c | 12345709 | vm6 | 172.16.255.16 | Invalid Staging Valid |

CloudExpress Tasks Alarms Help User Profile

admin

Install Certificate

G00421



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 both in the vEdge 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 browser's default download location and is named `viptela_download.csv`.

Check the vEdge Router Certificate Status

In the vEdge 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 vEdge Router

When you add vEdge 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 vEdge 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 vEdge List tab, select the vEdge 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 vEdge routers to the controller devices in the network. vManage NMS displays the Push vEdge List screen showing the status of the push operation.

Stage a vEdge Router

When you initially bring up and configure a vEdge 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 vEdge 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 vEdge router:



1. In the vEdge List tab, select the vEdge 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 vEdge authorized serial number file with the controllers. vManage NMS displays the Push vEdge List screen showing the status of the push operation.

Invalidate a vEdge Router

1. In the vEdge List tab, select the vEdge 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 vEdge routers to the controller devices in the network. vManage NMS displays the Push vEdge 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.

View the CSR

1. In the 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.

