
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.
- 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.
- Statistics Setting bar—Click View to view the current settings for collecting device statistics or Edit to edit the settings.
- CloudExpress bar—Click View to view the current settings for CloudExpress 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.
- 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.
- Maintenance Window bar—Click Edit to configure a maintenance time window notification.
- Statistics Configuration bar—Click View to view the current time interval for collecting device statistics or Edit to edit the setting.



Menu

CloudExpress Tasks Alarms Help User Profile

Cisco vManage

ADMINISTRATION | SETTINGS

Organization Name	viPtela System TB	View
vBond	52.7.126.119 : 12346	View Edit
Certificate Authorization	Manual	View Edit
vEdge Cloud Certificate Authorization	Automated	View Edit
Web Server Certificate	04 Nov 2019 9:07:40 AM	CSR Certificate
Enforce Software Version (ZTP)	Disabled	View Edit
Banner	Disabled	View Edit
Statistics Setting		View Edit
CloudExpress	Enabled	View Edit
vAnalytics	Enabled	View Edit
Client Session Timeout	Disabled	View Edit
Data Stream	Disabled	View Edit
Tenancy Mode	Single Tenant	View Edit

G00419

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.

Configure 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—vManage NMSs, vBond orchestrators, and vSmart controllers.

To configure certification authorization settings:

1. Click the Edit button to the right of the Certificate Authorization bar.
2. In Certificate Signing by Symantec, select Automated to have the Symantec signing server automatically generate, sign, and install certificates on each controller device. If not, select Manual.
3. Enter the first and last name of the requestor of the certificate.
4. Enter the email address of the requestor of the certificate. If you selected Manual in Step 1, the signed certificate and a confirmation email are sent to the requestor via email and are also made available through the customer portal.
5. Specify the validity period for the certificate.
6. Click the Edit Challenge Phrase checkbox to enter a challenge phrase. The challenge phrase is your certificate password and is required when you renew or revoke a certificate.
7. Confirm your challenge phrase.
8. In the Certificate Retrieve Interval field, specify how often the vManage server checks if the Symantec signing server has sent the certificate.
9. Click Save.

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.

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:
 1. In vManage NMS, select the Maintenance ► Software Upgrade screen.
 2. 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.
 3. If you need to add a software image, click Add New Software.



4. Select the location from which to download the software images, either vManage or Remote Server.
 5. Select an x86-based or a MIPS-based software image.
 6. 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.

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 CloudExpress Service

1. Click the Edit button to the right of the CloudExpress bar.
2. In the Enable CloudExpress 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 Data Stream Collection

By default, collecting streams of data from a network device is not enabled. 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 collect the data. 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. 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.

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.

