Maintenance

Software Repository

Use the Software Repository screen to download software images to 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
16.8.55	18.1.x	vmanage	software

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 Cisco SD-WAN 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 Cisco SD-WAN 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 Cisco SD-WAN 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. In vManage NMS, select the **Maintenance** > **Software Repository** screen
2. Click **Add New Software**.
3. Select the location to store the software image:
   a. To store the software image or on the local vManage server and have it be downloaded to Cisco SD-WAN devices over a control plane connection, select vManage. The Upload Software to vManage dialog box opens.
      1. 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.
      2. Click **Upload** to add the image to the software repository. The Software Repository tables display the added software image, and it is available for installing on the devices.

Note The local vManage server is available for storing NFVIS upgrade images and no other locations are available.

   b. To store the software image on a remote server, select **Remote Server**. The Location of Software on Remote Server dialog box opens.
      1. In the Version box, enter the version number of the software image.
      2. In the URL box, enter the FTP or HTTP URL of the software image.
      3. Click **Add** to add the image to the software repository. The Software Repository tables display 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 Cisco SD-WAN devices over an out-of-band management connection, select **Remote Server - vManage**. The Upload Software to Remote Server - vManage dialog box opens.

   1. 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).
   2. 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.
   3. Click **Upload** to add the image to the software repository. The Software Repository tables display the added software image, and it is available for installing on the devices.

Upload VNF Images in Software Repository

See Upload VNF Images , on page 3.

Create Customized VNF Image

See Create Customized VNF Image, on page 4.

View VNF Images

See View VNF Images .

Delete a Software Image from the Repository

To delete a software image from the vManage software repository:

1. In vManage NMS, select the **Maintenance** > **Software Repository** screen.
2. In the software repository table, select the software image.
3. 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.

Delete VNF Image

See Delete VNF Images .

Upload VNF Images

The VNF images are stored in software respository. These VNF images are referenced during service chain deployment, and then they are pushed to NFVIS during service chain attachment.

In vManage, click **Maintenance** > **Software Repository**. The Maintenance|Software Repository screen appears, and the **Add New Software** button is highlighted. To upload VNF images, use the **Virtual Images** tab. In the Maintenance|Software Repository screen, perform the following tasks:

a) To add a prepackaged VNF image, click the **Virtual Images** tab, and then click the **Upload Virtual Images** button.
b) Choose the location to store the virtual image.

- To store the virtual image on the local vManage server and then get it downloaded to CSP devices over a control plane connection, click **vManage**. The **Upload Software to vManage** dialog box appears.

  1. Drag and drop the virtual image file to the dialog box or click **Browse** to choose the virtual image from the local vManage server. For example, CSR.tar.gz, ASAv.tar.gz.
  2. Click **Upload** to add the image to the virtual image repository. The virtual image repository table displays the added virtual image, and it is available for installing on the CSP devices.

- To store the image on a remote vManage server and then get it downloaded to CSP devices over an out-of-band management connection, click **Remote Server - vManage**. The **Upload Virtual Image to Remote Server - vManage** dialog box appears.

  1. In **vManage Hostname/IP Address**, enter the IP address of an interface on the vManage server that is in a management VPN (typically, VPN 512).
  2. Drag and drop the virtual image file to the dialog box, or click **Browse** to choose the virtual image from the local vManage server.
  3. Click **Upload** to add the image to the virtual image repository. The virtual image repository table displays the added virtual image, and it is available for installing on the CSP devices.

c) Click **Submit**.

You can have multiple VNF entries such as a firewall from same or different vendors. Also, different versions of VNF that are based on the release of the same VNF can be added. However, ensure that the VNF name is unique.

Create Customized VNF Image

Before you begin

You can upload one or more qcow2 images in addition to a root disk image as an input file along with VM-specific properties, bootstrap configuration files (if any), and generate a compressed TAR file. Through custom packaging, you can:

- Create a custom VM package along with image properties and bootstrap files (if needed) into a TAR archive file.
- Tokenize custom variables and apply system variables that are passed with the bootstrap configuration files.

Ensure that the following custom packaging requirements are met:

- Root disk image for a VNF–qcow2
- Day-0 configuration files–system and tokenized custom variables
- VM configuration–CPU, memory, disk, NICs
- HA mode–If a VNF supports HA, specify Day-0 primary and secondary files, NICs for a HA link

- Additional Storage–If additional storage is required, specify predefined disks (qcow2), storage volumes (NFVIS layer)

Step 1 In the **Maintenance** > **Software Repository** screen, click the **Add Custom VNF Package** button from the **Virtual Images** tab.

Step 2 Configure the VNF with the following VNF package properties and click **Save**.

Table 1: VNF Package Properties

Field	Mandatory or Optional	Description
Package Name	Mandatory	Specifies the filename of the target VNF package. It is the NFVIS image name with .tar or .gz extensions.
App Vendor	Mandatory	Specifies whether Cisco VNFs or third-party VNFs.
Name	Mandatory	Specifies name of the VNF image.
Version	Optional	Specifies version number of the program.
Type	Mandatory	Choose VNF type. Supported VNF types are: Router, Firewall, Load Balancer, and Other.

Step 3 To package a VM qcow2 image, click **File Upload** under **Image**, and browse to choose a qcow2 image file.

Step 4 To choose a bootstrap configuration file for VNF, if any, click the **Bootstrap Files** button under **Day 0 Configuration**, click **File Upload**, and then browse to choose a bootstrap file.

Include the following Day-0 configuration properties:

Table 2: Day-0 Configuration

Field	Mandatory or Optional	Description
Mount	Mandatory	Specifies the path where the bootstrap file gets mounted.
Parseable	Mandatory	Specifies whether a Day-0 configuration file can be parsed or not. Options are: true or false. By default, it is true.
High Availability	Mandatory	Choose high availability of a Day-0 configuration file. Supported values are: Standalone, HA Primary, HA Secondary.

Note If any bootstrap configuration is required for a VNF, you must create *bootstrap-config* or *day0-config*.

Step 5 To add a Day-0 configuration, click **Add**, and then click **Save**. The Day-0 configuration appears in the **Day 0 Config File** table. You can tokenize the bootstrap configuration variables with system and custom variables. To tokenize variables of a Day-0 configuration file, click **View Configuration File** against the configuration file. In the **Day 0 configuration file** dialog box, perform the following tasks:

Note The bootstrap configuration file is an XML or a text file, and contains properties specific to a VNF and the environment. For a shared VNF, see the topic, Additional References in Cisco SD-WAN Cloud OnRamp for Colocation Solution Guide for the list of system variables that must be added for different VNF types..

a) To add a system variable, in the **CLI configuration** dialog box, select and highlight a property from the text fields. Click **System Variable**. The **Create System Variable** dialog box appears.
b) Choose a system variable from the **Variable Name** drop-down, and click **Done**. The highlighted property is replaced by the system variable name.
c) To add a custom variable, in the **CLI configuration** dialog box, select and highlight a custom variable attribute from the text fields. Click **Custom Variable**. The **Create Custom Variable** dialog box appears.
d) Enter custom variable name and choose a type from **Type** drop-down.
e) To set the custom variable attribute, do the following:

- To ensure that the custom variable is mandatory when creating a service chain, check the **Type** check box against **Mandatory**.
- To ensure that a VNF includes both primary and secondary Day-0 files, check the **Type** check box against **Common**.

f) Click **Done**, and then click **Save**. The highlighted custom variable attribute is replaced by the custom variable name.

Step 6 To upload extra VM images, expand **Advance Options**, click **Upload Image**, and then browse to choose an additional qcow2 image file. Choose the root disk, Ephemeral disk 1, or Ephemeral disk 2, and click **Add**. The newly added VM image appears in the **Upload Image** table.

Note Ensure that you do not combine ephemeral disks and storage volumes when uploading extra VM images.

Step 7 To add the storage information, expand **Add Storage**, and click **Add volume**. Provide the following storage information and click **Add**. The added storage details appear in the **Add Storage** table.

Table 3: Storage Properties

Field	Mandatory or Optional	Description
Size	Mandatory	Specifies the disk size that is required for the VM operation. The maximum disk size can be 256 if the size unit is GiB.
Size Unit	Mandatory	Choose size unit. Supported units are: MIB, GiB, TiB.
Device Type	Optional	Choose a disk or CD-ROM. Default is a disk.
Location	Optional	Specifies location of the disk or CD-ROM. By default, it is local.

Field	Mandatory or Optional	Description
Format	Optional	Choose a disk image format. Supported formats are: qcow2, raw, and vmdk. Buy default, it is raw.
Bus	Optional	Choose a value from the drop-down. Supported values for a bus are: virtio, scsi, and ide. By default, it is virtio.

Step 8 To add VNF image properties, expand **Image Properties** and provide the following image information.

Table 4: VNF Image Properties

Field	Mandatory or Optional	Description
SR-IOV Mode	Mandatory	Specifies enabling or disabling SR-IOV support. By default, it is enabled.
Monitored	Mandatory	VM health monitoring for those VMs that can be bootstrapped. Options are: enable or disable. By default, it is enabled.
Bootup Time	Mandatory	Specifies monitoring timeout period for a monitored VM. By default, it is 600 seconds.
Serial Console	Optional	Specifies serial console that is supported or not. Options are: enable or disable. By default, it is disabled.
Privileged Mode	Optional	Allows special features like promiscuous mode and snooping. Options are: enable or disable. By default, it is disabled.
Dedicate Cores	Mandatory	Facilitates allocation of a dedicated resource (CPU) to supplement a VM's low latency (for example, router and firewall). Otherwise, shared resources are used. Options are: enable or disable. By default, it is enabled.

Step 9 To add VM resource requirements, expand **Resource Requirements** and provide the following information.

Table 5: VM Resource Requirements

Field	Mandatory or Optional	Description
Default CPU	Mandatory	Specifies CPUs supported by a VM. The maximum numbers of CPUs supported are 8.
Default RAM	Mandatory	Specifies RAM supported by a VM. The RAM can range from 2–32.
Disk Size	Mandatory	Specifies disk size in GB supported by a VM. The disk size can range from 4–256.
Max number of VNICs	Optional	Specifies maximum number of VNICs allowed for the VM. The number of VNICs can range from 8–32 and the default value is 8.
Management VNIC ID	Mandatory	Specifies the management VNIC ID corresponding to the management interface. Valid range is from 0 to maximum number of VNICs.
Number of Management VNICs ID	Mandatory	Specifies number of VNICs.
High Availability VNIC ID	Mandatory	Specifies VNIC IDs where high availability is enabled. Valid range is from 0–maximum number of VNICs. It should not conflict with management VNIC Id. The default value is 1.
Number of High Availability VNICs ID	Mandatory	Specifies maximum number of VNIC IDs where high availability is enabled. Valid range is 0–(maximum number of VNICs-number of management VNICs-2) and default value is 1.

Step 10 To add Day-0 configuration drive options, expand **Day0 Configuration Drive options** and provide the following information.

Table 6: Day-0 Configuration Drive Options

Field	Mandatory or Optional	Description
Volume Label	Mandatory	Displays the volume label of the Day-0 configuration drive. Options are: V1 or V2. By default, it is V2. V2 is the config-drive label config-2. V1 is config-drive label cidata.

Field	Mandatory or Optional	Description
Init Drive	Optional	Mounts the Day-0 configuration file as a disk. The default drive is CD-ROM.
Init Bus	Optional	Choose an init bus. Supported values for a bus are: virtio, scsi, and ide. By default, it is ide.

The Software Repository table displays the customized VNF image, and it is available for choosing while creating a custom service chain.

View VNF Images

In vManage, click **Maintenance** > **Software Repository**. The Maintenance|Software Repository screen appears, and the **Add New Software** button is highlighted. To view VNF images, use the **Virtual Images** tab. In the Maintenance|Software Repository screen, perform the following tasks:

a) To view VNF images, click the **Virtual Images** tab. The images in the repository are displayed in the table.

b) To filter the list, search or type a string in the Search box.

The Software Version column provides the version of the software image.

The Software Location column indicates where the software images are stored. It can be stored either in the repository on the vManage server or in a repository in a remote location.

The Version Type Name column provides the type of firewall.

The Available Files column lists the names of the VNF image files.

The Update On column displays when the software image was added to the repository.

c) To view details of a VNF image, click a VNF image, click the **More Actions** icon, and click **Show Info** against the VNF image.

Delete VNF Images

In vManage, click **Maintenance** > **Software Repository**. The Maintenance|Software Repository screen appears, and the **Add New Software** button is highlighted. To upload VM images, use the **Virtual Images** tab. In the Maintenance|Software Repository screen, perform the following tasks:

a) To delete a VM image, click the **Virtual Images** tab. The images in the repository are displayed in the table.

b) In the repository table, click a VM image.

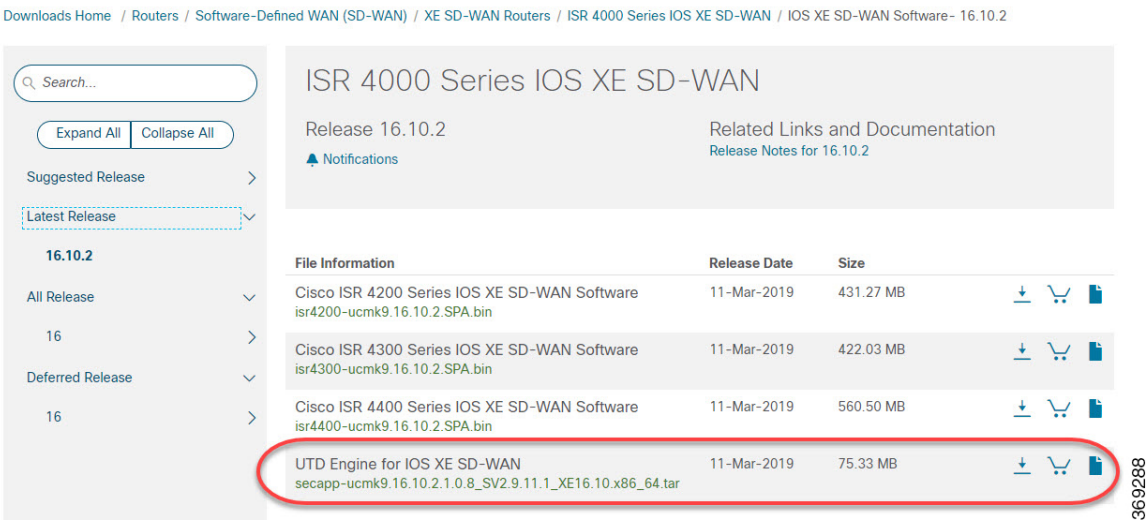
c) Click the **More Actions** icon to the right of its row, and click **Delete** against the VM image.

Note If a VNF image is being download to a router, you cannot delete the VNF image until the download process completes.

Note If the VNF image is referenced by a service chain, it cannot be deleted.

Upload the Cisco Security Virtual Image to vManage

Each router image supports a specific range of versions for a hosted application. For IPS/IDS and URL-Filtering, you can find the range of supported versions (and the recommended version) for a device on its Device Options page.

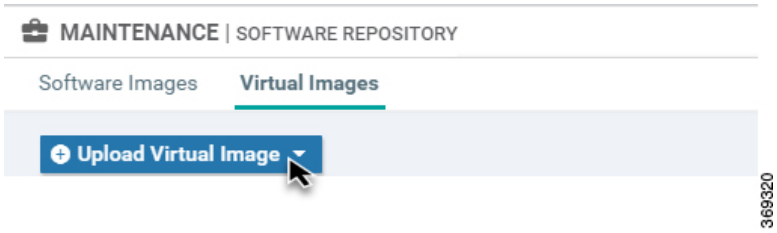


Step 1 From the Software Download page for your router, locate the image "**UTD Engine for IOS XE SD-WAN**."

Step 2 Click the **download** icon on the right-hand side of the window to download the image file.

Step 3 From the vManage dashboard, select **Maintenance** > **Software Repository**.

Step 4 Select **Virtual Images** from the top options.



Step 5 Click **Upload Virtual Image**, and select either **vManage** or **Remote Server – vManage**. The Upload Virtual Image to vManage window opens.

Step 6 Drag and drop, or browse to the image file and select it.

Step 7 Click **Upload**. When the upload completes, a confirmation message displays. The new virtual image displays in the Virtual Images Software Repository.

Software Upgrade

Use the Software Upgrade screen to download new software images and to upgrade the software image running on a Cisco SD-WAN device.

From a centralized vManage NMS, you can upgrade the software on Cisco SD-WAN 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.

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 Cisco SD-WAN 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 Cisco SD-WAN 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.

Upgrade CSP device with NFVIS Upgrade Image

See Upgrade CSP Device with NFVIS Upgrade Image, on page 13.

Delete a Software Image

To delete a software image from a Cisco SD-WAN 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 Cisco SD-WAN 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 on the arrow 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.

Upgrade CSP Device with NFVIS Upgrade Image

Before you begin

Ensure that the NFVIS software versions are the files that have `.nfvispkg` extension.

Step 1 In the **Maintenance** > **Software Upgrade** > **WAN Edge** screen, view the list of all CSP devices along with their current and available versions.

Step 2 Select one or more devices, and click **Upgrade**.

Step 3 Choose a CSP device on which to upgrade the NFVIS software image.

Step 4 Click the **Upgrade** button. The **Software Upgrade** dialog box appears.

Step 5 Choose the NFVIS software version to install on the CSP device. If software is located on a remote server, choose the appropriate remote version.

Step 6 To automatically upgrade and activate with the new NFVIS software version and reboot the CSP device, check the **Activate and Reboot** checkbox.

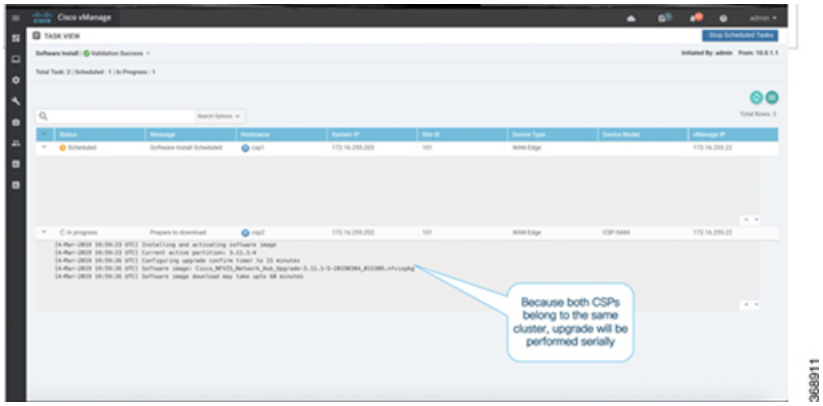
If you do not check the **Activate and Reboot** checkbox, the CSP device downloads and verifies the software image. However, the CSP device continues to run the old or current version of the software image. To enable the CSP device to run the new software image, you must manually activate the new NFVIS software version by selecting the device again and clicking the **Activate** button on the **Software Upgrade** page. For more information about activation, see the "Activate a New Software Image" topic in the Cisco SD-WAN Configuration Guides.

Step 7 Click **Upgrade**.

To view the status of software upgrades, the task view page displays a list of all running tasks along with total number of successes and failures. The page periodically refreshes and displays messages to indicate the progress or status of the

upgrade. You can easily access the software upgrade status page by clicking the Tasks icon located in the vManage toolbar.

Note If two or more CSP devices belonging to the same cluster are upgraded, the software upgrade for the CSP devices happen in a sequence.



Note The **Set the Default Software Version** option is not available for NFVIS images.

The CSP device reboots and the new NFVIS version is activated on it. This reboot happens during the **Activate** phase. The activation can either happen immediately after upgrade if you check the **Activate and Reboot** check box, or by manually selecting the activate button after selecting the device again.

To verify if CSP device has rebooted and is running, vManage polls your entire network every 90 seconds up to 30 times.

Note You can delete an NFVIS software image from a CSP device if the image version is not the active version that is running on the device.

Upgrade a Security Virtual Image

When a Cisco IOS-XE SD-WAN router is upgraded to a new software image, the security virtual image must also be upgraded to match.

Note If the IPS Signature Update option is enabled, the matching IPS signature package is automatically updated as a part of the upgrade. You can enable the setting from **Administration** > **Settings** > **IPS Signature Update**.

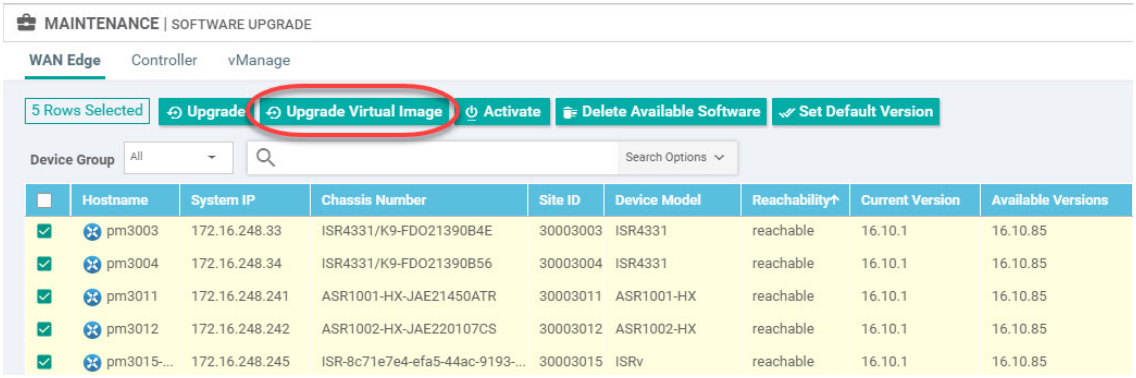
To upgrade the application hosting virtual image for a device, follow these steps:

Step 1 Follow the steps in "Upload the Correct Cisco Security Virtual Image to vManage" to download the recommended version of the SVI for your router. Note the version name.

Step 2 From the vManage menu, select **Maintenance** > **Software Repository** > **Virtual Images** to verify that the image version listed under the Recommended Version column matches a virtual image listed in the Virtual Images table.

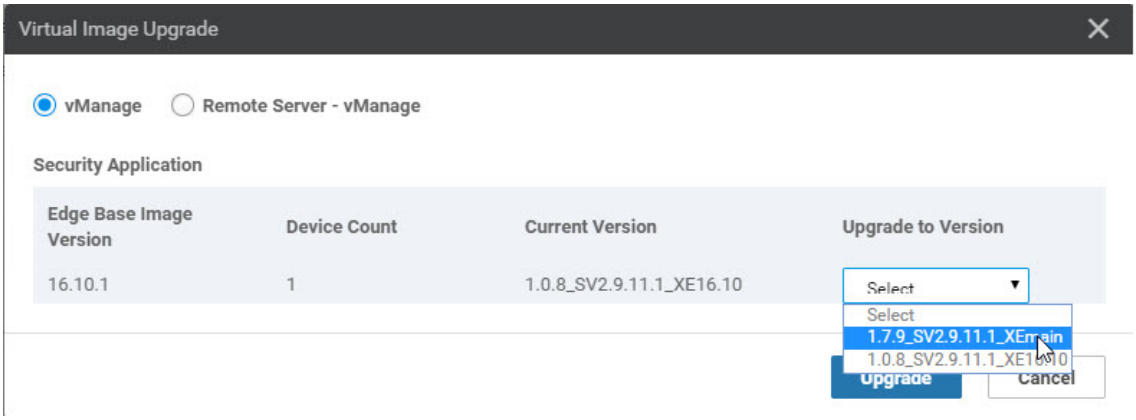
Step 3 Select **Maintenance** > **Software Upgrade**. The WAN Edge Software upgrade page displays.

Step 4 Select the devices you want to upgrade by clicking the boxes in the leftmost column. When you have selected one or more devices, a row of options display, as well as the number of rows you selected.



Step 5 When you are satisfied with your choices, select **Upgrade Virtual Image** from the options menu. The Virtual Image Upgrade dialog box opens.

Step 6 For each device you selected, select the correct upgrade version from the **Upgrade to Version** drop-down list.



Step 7 When you have selected an upgrade version for each device, click **Upgrade**. When the update completes, a confirmation message displays.

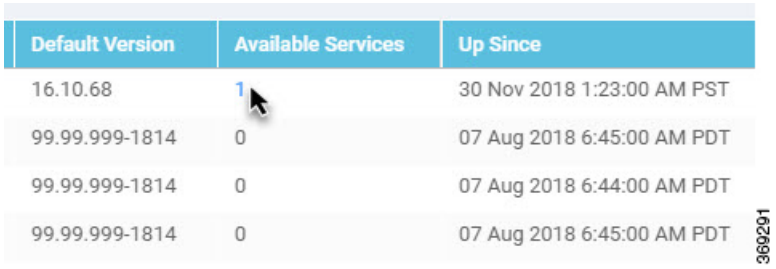
Verifying Your SVI Upgrade

To verify your Security Virtual Image (SVI) upgrade:

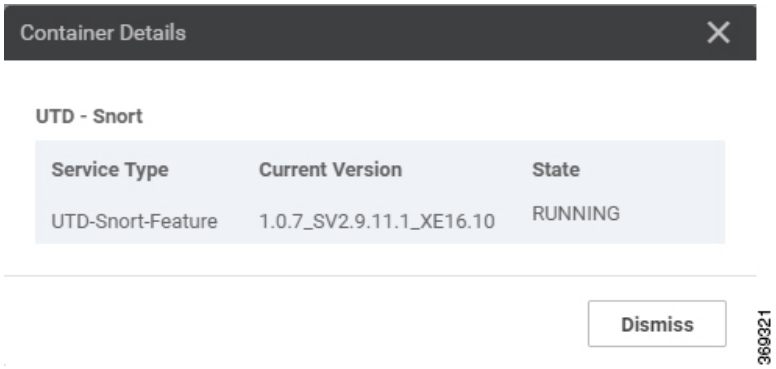
Step 1 From the vManage menu, select **Maintenance ▸ Software Upgrade.**

Step 2 Locate an upgraded device in the device table.

Step 3 Scroll to the Available Services column on the far right of the device table.



Step 4 Click the linked number in the Available Services column. The Container Details popup displays.



Step 5 Verify that the device is running the updated image.

Reboot Your Device

Use the Device Reboot screen to reboot one or more Cisco SD-WAN devices.

Reboot Devices

To reboot Cisco SD-WAN devices in the overlay network:

1. In the title bar, click **vEdge** > **Controller** > **vManage**.
2. Choose 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 that is 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.

Reload Security Application

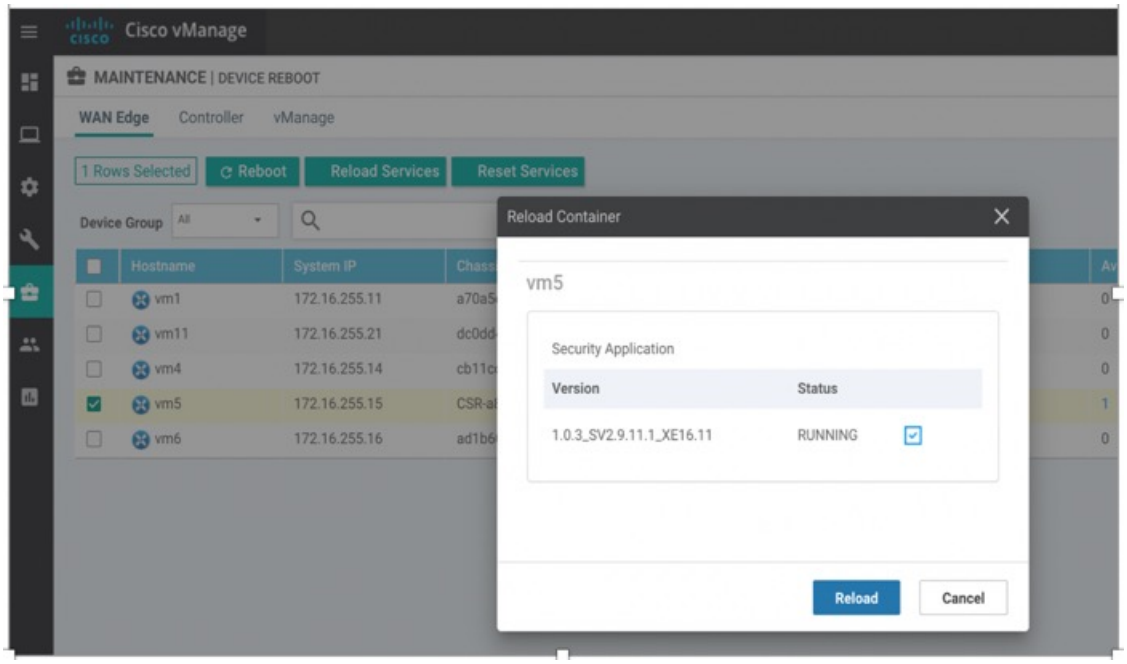
The reload service button enables you to recover a security application from an inoperative state. See Determine Security Applications in Inoperative State, on page 18. For more information about a security application, see Configuring Security Application.

Note The reload service can recover some security applications from an inoperative state. Make sure to use this service as an initial recovery option. See Determine Security Applications in Inoperative State, on page 18.

Ensure that a security application has already been installed on the device which is chosen from the device table. To reload one or more security applications:

1. In the **WAN Edge** tab, check against a Cisco SD-WAN device to reload the security application
2. Click **Reload Services**.

   The Reload Container dialog box appears.
3. If the security application version is correct, check the box against the version of the security app. See the topic *Upgrade a Security Virtual Image* in Configuring Security Application for more information about an application version.



4. Click **Reload**.

   The security application is stopped, uninstalled, reinstalled, and started again.

Reset Security Application

The reset service button enables you to recover a security application from an inoperative state. See Determine Security Applications in Inoperative State, on page 18. For more information about a security application, see Configuring Security Application.

When the virtual network configuration of a security application changes such as the virtual port group configuration on a device, use the reset service button.

Note The reset service can recover some security applications from an inoperative state, and therefore ensure to use this service as an initial recovery option. See Determine Security Applications in Inoperative State, on page 18.

- Ensure that a security application has already been installed on the device which is chosen from the device table.
- Ensure that the chosen security application is in a running state.

To reset one or more security applications:

1. Go to the **WAN Edge** tab, check against a Cisco SD-WAN device to reload the security application.
2. Click **Reset Services**.

   The Reset Container dialog box appears.
3. If the security application version is correct, check the box against the version of the device. See the topic *Upgrade the Security Virtual Image* in Configuring Security Application for more information about an application version
4. Click **Reset**.

   The security application is stopped, and then restarted.

Determine Security Applications in Inoperative State

To determine if a security application is in inoperative state:

1. In vManage NMS, click **Monitor** > **Network**.
2. In the MONITOR|NETWORK screen, click a Cisco SD-WAN device from **Hostname**.
3. In the left pane, click **Real Time**.

   The real time device information appears in the right pane.
4. Choose **App Hosting Details** from the **Device Options** drop-down.

   A table appears with the device-specific application hosting information. In the table, if the state of the device is "ACTIVATED," "DEPLOYED," or "STOPPED," perform a reload or reset operation on the security application.

If the state of the device is "RUNNING," the security application is in an operative state.

5. Choose **Security App Dataplane Global** from the **Device Options** drop-down.

   A table appears with the device-specific application data plane information. In the table, if the SN Health of the device is "yellow," or "red," perform a reload or reset operation on the security application.

   If the SN Health of the device is "green," the security application is in an operative state.

Security

Rekey the Device Threat Grid API Key

To rekey the device Threat Grid API key from the Maintenance screen:

Step 1 In Cisco vManage, select the **Maintenance** > **Security** tab in the left side panel.

Step 2 Select the **Advanced Malware Protection** tab.

Step 3 Select the device or devices that you want to rekey.

Step 4 Select **Action** > **API Rekey**.