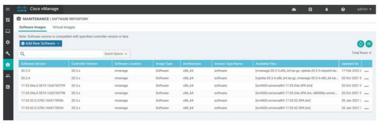
Manuals+ — User Manuals Simplified.



Note: Software version is compatible with specified controller version or less

Total Rows: 6

Software Version	Controller Version	Software Location	Image Type	Architecture	Version Type Name	Available Files	Updated On
20.3.5	20.3.x	vmanage	Software	x86_64	software	[vmanage-20.3.5-x86_64.tar.gz, viptela-20.3.5-mips64.tar...	17 Feb 2022
20.3.4	20.3.x	vmanage	Software	x86_64	software	[viptela-20.3.4-x86_64.tar.gz, vmanage-20.3.4-x86_64.tar...	20 Oct 2021
17.03.04a.0.5574.1626783799	20.3.x	vmanage	Software	x86_64	software	[isr4400-universalk9.17.03.04a.SPA.bin]	20 Oct 2021
17.03.04a.0.5574.1626783798	20.3.x	vmanage	Software	x86_64	software	[isr4300-universalk9.17.03.04a.SPA.bin, c8000be-univer...	20 Oct 2021
17.03.02.0.3785.1604178956	20.3.x	vmanage	Software	x86_64	software	[isr4400-universalk9.17.03.02.SPA.bin]	20 Jan 2021
17.03.02.0.3785.1604178934	20.3.x	vmanage	Software	x86_64	software	[isr4300-universalk9.17.03.02.SPA.bin]	20 Jan 2021

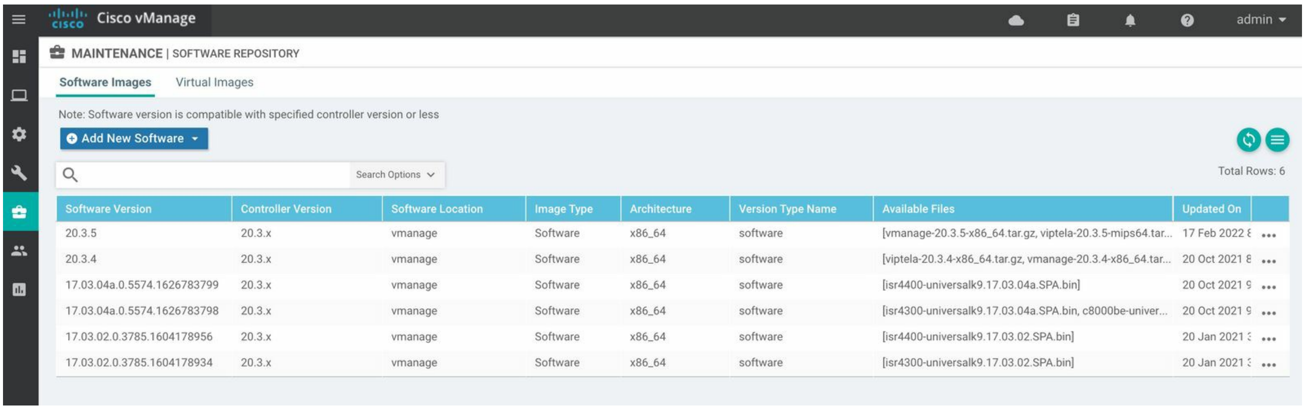
CISCO Catalyst SD-WAN Manage Software Upgrade and Repository User Guide

Home » Cisco » **CISCO Catalyst SD-WAN Manage Software Upgrade and Repository User Guide**

Contents

1 CISCO Catalyst SD-WAN Manage Software Upgrade and Repository
2 Manage Software Upgrades and Repository
3 Software Upgrade
4 Upgrade the Software Image on a Device
5 Activate a New Software Image
6 Delete a Software Image
7 Set the Default Software Version
8 Manage Software Repository
9 Manage Remote Server
10 Add Software Images to the Repository
11 View Software Images
12 Create Customized VNF Image
13 View VNF Images
14 Documents / Resources
14.1 References
15 Related Posts

CISCO Catalyst SD-WAN Manage Software Upgrade and Repository



Note: Software version is compatible with specified controller version or less

Total Rows: 6

Software Version	Controller Version	Software Location	Image Type	Architecture	Version Type Name	Available Files	Updated On
20.3.5	20.3.x	vmanage	Software	x86_64	software	[vmanage-20.3.5-x86_64.tar.gz, viptela-20.3.5-mips64.tar...	17 Feb 2022 8
20.3.4	20.3.x	vmanage	Software	x86_64	software	[viptela-20.3.4-x86_64.tar.gz, vmanage-20.3.4-x86_64.tar...	20 Oct 2021 8
17.03.04a.0.5574.1626783799	20.3.x	vmanage	Software	x86_64	software	[isr4400-universalk9.17.03.04a.SPA.bin]	20 Oct 2021 9
17.03.04a.0.5574.1626783798	20.3.x	vmanage	Software	x86_64	software	[isr4300-universalk9.17.03.04a.SPA.bin, c8000be-univer...	20 Oct 2021 9
17.03.02.0.3785.1604178956	20.3.x	vmanage	Software	x86_64	software	[isr4400-universalk9.17.03.02.SPA.bin]	20 Jan 2021 3
17.03.02.0.3785.1604178934	20.3.x	vmanage	Software	x86_64	software	[isr4300-universalk9.17.03.02.SPA.bin]	20 Jan 2021 3

Manage Software Upgrades and Repository

Table 1: Feature History

Feature Name	Release Information	Description
Software Upgrade Using a Remote Server	Cisco IOS XE Release 17.7.1a Cisco SD-WAN Release 20.7.1 Cisco vManage Release 20.7.1	This feature enables you to upgrade device or controller software using software images stored on a remote server. The feature enables you to register a remote server with Cisco vManage and add locations of software images on the remote server to the Cisco vManage software repository. When you upgrade the device or controller software, the device or controller can download the new software image from the remote server. This feature also improves the listing of images available in the repository. When two or more images have the same version but different file names, each image is listed as a separate entry.

- Software Upgrade, on page 1
- Manage Software Repository,

Software Upgrade

- Use the Software Upgrade window to download new software images and to upgrade the software image running on a Cisco SD-WAN device.
- From a centralized Cisco vManage, 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 Cisco vBond Orchestrator, Cisco vSmart Controllers, and Cisco IOS XE SD-WAN devices or Cisco vEdge devices in either a standalone or Cisco vManage cluster deployment, the

software upgrade and reboot is performed first on the Cisco vBond Orchestrator, next on the Cisco vSmart Controller, and finally on the Cisco IOS XE SD-WAN devices or Cisco vEdge devices. Up to 40 Cisco IOS XE SD-WAN devices or Cisco vEdge devices can be upgraded and rebooted in parallel, depending on CPU resources.

- Introduced in the Cisco vManage Release 20.8.1, the software upgrade workflow feature simplifies the software upgrade process for the Cisco SD-WAN edge devices through a guided workflow and displays the various device and software upgrade statuses. For more information on creating a Software Upgrade Workflow, see Software Upgrade Workflow.

Note

- You cannot include Cisco vManage in a group software upgrade operation. You must upgrade and reboot the Cisco vManage server by itself.
- You can create a software upgrade workflow only for upgrading the Cisco SD-WAN edge devices.
- It is recommended that you perform all software upgrades from Cisco vManage rather than from the CLI.
- For software compatibility information, see the Cisco SD-WAN Controller Compatibility Matrix and Server Recommendations.

Upgrade Virtual Image on a Device

1. From the Cisco vManage menu, choose Maintenance > Software Upgrade.
2. To choose a device, check the check box for the desired device.
3. Click Upgrade Virtual Image.
    - The Virtual Image Upgrade dialog box opens.
4. Choose vManage or Remote Server – vManage, as applicable.
5. From the Upgrade to Version drop-down list, choose the virtual image version to upgrade the device to.
6. Click Upgrade.

Upgrade the Software Image on a Device

Note

- This procedure does not enable downgrading to an older software version. If you need to downgrade, see Downgrade a Cisco vEdge Device to an Older Software Image in the Cisco SD-WAN Getting Started Guide.
- If you want to perform a vManage cluster upgrade see, Upgrade Cisco vManage Cluster.
- Starting from Cisco vManage Release 20.1.1, before upgrading the configuration database, ensure that you verify the database size. We recommend that the database size is less than or equal to 5 GB. To verify the database size, use the following diagnostic command: request nms configuration-db diagnostics

To upgrade the software image on a device:

1. From the Cisco vManage menu, choose Maintenance > Software Upgrade.
2. Click WAN Edge, Controller, or vManage based on the type of device for which you wish to upgrade the software.

3. In the table of devices, select the devices to upgrade by selecting the check box on the far left.
   - **Note** While upgrading Cisco vManage clusters, select all the nodes of the cluster in the table.
4. Click Upgrade.
5. In the Software Upgrade slide-in pane, do as follows:
   - **a**. Choose the server from which the device should download the image: vManage, Remote Server, or Remote Server – vManage.
   - **Note**
   - The Remote Server option is introduced in Cisco vManage Release 20.7.1. If you choose Remote Server, ensure that the device can reach the remote server.
   - Starting from Cisco vManage Release 20.9.1, when downloading an image from a remote server manually, ensure that only the following valid characters are used:
   - User ID: a-z, 0-9, ., _, –
   - Password: a-z, A-Z, 0-9, _, *, ., +, =, %, –
   - URL Name or Path: a-z, A-Z, 0-9, _, *, ., +, =, %, -,:, /, @,? ~
   - **b.** For vManage, choose the image version from the Version drop-down list.
   - **c.** For Remote Server – vManage, choose the vManage OOB VPN from the drop-down list and choose the image version from the Version drop-down list.
   - **d**. For Remote Server, configure the following:

Remote Server Name	Choose the remote server that has the image.
Image Filename	Choose the image filename from the drop-down list.

     e. Check the Activate and Reboot check box.

   - If you do not check this check box, the software image is downloaded and installed on the device, but, the image is not activated, and the device is not rebooted. You must activate the image after the upgrade task is completed.
   - **f**. Click Upgrade.
     The device restarts, using the new software version, preserving the current device configuration. The Task View page opens, showing the progress of the upgrade on the devices.
6. Wait for the upgrade process, which takes several minutes, to complete. When the Status column indicates Success, the upgrade is complete.
7. From the Cisco vManage menu, choose Maintenance > Software Upgrade and view the devices.
8. Click WAN Edge, Controller, or vManage based on the type of device for which you wish to upgrade the software.
9. In the table of devices, confirm that the Current Version column for the upgraded devices shows the new version. Confirm that the Reachability column says reachable.

Note

- f the control connection to Cisco vManage does not come up within the configured time limit, Cisco vManage 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 Cisco vEdge devices, which have a default time of 12 minutes.

- If you upgrade the Cisco vEdge device 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 Cisco vEdge device software.
- When upgrading a Cisco CSR1000V or Cisco ISRv device to Cisco IOS XE Release 17.4.1a or later, the software upgrade also upgrades the device to a Cisco Catalyst 8000V. After the upgrade, on the Devices page, the Chassis Number and Device Model columns show the device as a Cisco CSR1000V or Cisco ISRv, but the device has actually been upgraded to a Cisco Catalyst 8000V. The reason for preserving the old name is to avoid invalidating licenses, and so on. To confirm that the device has been upgraded to a Cisco Catalyst 8000V, note that the Current Version column for the device indicates 17.4.1 or later.

Activate a New Software Image

- Use this procedure to activate a software image that is currently loaded on a device. The software image may be a later release (upgrade) or earlier release (downgrade) than the current active release.
- When you use Cisco vManage to upgrade the software image on a device, if you did not check the Activate and Reboot check box during the procedure, the device continues to use the existing configuration. Use this procedure to activate the upgraded software version.

Note

- To activate the software for Cisco vManage while using a custom user group, you need read permission and read-write permissions to upgrade each software feature.

To activate a software image:

1. From the Cisco vManage menu, choose Maintenance > Software Upgrade.
2. Choose WAN Edge, Controller, or Cisco vManage.
3. For the desired device or devices, check the check box to choose the device or devices,
4. Click Activate. The Activate Software dialog box opens.
5. Choose the software version to activate on the device.
6. Click Activate. Cisco vManage reboots the device and activates the new software image.

- If the control connection to Cisco vManage does not come up within the configured time limit, Cisco vManage 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 Cisco vEdge device, which has a default time of 12 minutes.

Upgrade a CSP Device with a Cisco NFVIS Upgrade Image

Before you begin

- Ensure that the Cisco NFVIS software versions are the files that have .nfvispkgextension.
- **Step** 1 From the Cisco vManage menu, choose Maintenance > Software Upgrade >WAN Edge.
- **Step** 2 Check one or more CSP device check boxes for the devices you want to choose.

- **Step** 3 Click Upgrade. The Software Upgrade dialog box appears.
- **Step** 4 Choose the Cisco NFVIS software version to install on the CSP device. If the software is located on a remote server, choose the appropriate remote version.
- **Step** 5 To automatically upgrade and activate with the new Cisco NFVIS software version and reboot the CSP device, check the Activate and Reboot check box.
- If you don't check the Activate and Reboot check box, 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 Cisco NFVIS software version by choosing the device again and clicking the Activate button in the Software Upgrade window.
- **Step** 6 Click Upgrade.
- The Task View window displays a list of all running tasks along with the total number of successes and failures. The window periodically refreshes and displays messages to indicate the progress or status of the upgrade. You can easily access the software upgrade status window by clicking the Task View icon located in the Cisco vManage toolbar.

Note

- If two or more CSP devices belonging to the same cluster are upgraded, the software upgrade for the CSP devices happens in a sequence.
- **Note** The Set the Default Software Version option isn't available for the Cisco NFVIS images.
- The CSP device reboots and the new NFVIS version is activated on the device. This reboot happens during the Activate phase. The activation can either happen immediately after the upgrade if you check the Activate and Reboot check box or by manually clicking Activate after choosing the CSP device again.
- To verify if the CSP device has rebooted and is running, use the task view window. Cisco vManage polls your entire network every 90 seconds up to 30 times and shows the status on the task view window.

Note

- You can delete a Cisco NFVIS software image from a CSP device if the image version isn't the active version that is running on the device.

Delete a Software Image

To delete a software image from a Cisco SD-WAN device:

1. From the Cisco vManage menu, choose Maintenance > Software Upgrade.
2. ClickWAN Edge, Controller, or vManage.
3. Choose one or more devices from which to delete a software image.
4. Click the Delete Available Software The Delete Available Software dialog box opens.
5. Choose the software version to delete.
6. 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. From the Cisco vManage menu, choose Maintenance > Software Upgrade.
2. Click WAN Edge, Controller, or vManage.
3. Choose one or more devices by checking the check box for the desired device or devices.
4. Click Set Default Version.
   - The Set Default Version dialog box opens.
5. From the Version drop-down list, choose the software image to use as the default for the chosen device or devices.
6. Click Set Default.

Export Device Data in CSV Format

1. From the Cisco vManage menu, choose Maintenance > Software Upgrade.
2. Click WAN Edge, Controller, or vManage.
3. Choose one or more devices by checking the checkbox for the desired device or devices.
4. Click the download icon.

Cisco vManage 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 Software_Upgrade.csv

View Log of Software Upgrade Activities

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

Manage Software Repository

Register Remote Server

- Register a remote server with Cisco vManage so that you can add locations of software images on the remote server to the Cisco vManage software repository and upgrade device or controller software using these software images. In multitenant Cisco SD-WAN deployment, only the provider can register a remote server and perform software upgrades using images on the remote server.

1. From the Cisco vManage menu, choose Maintenance > Software Repository.
2. Click Add Remote Server.
3. In the Add Remote Server slide-in page, configure the following:

Server Info	• **Server Name**: Enter a name for the server. • **Server IP or DNS Name**: Enter the IP address or the DNS name of the server. • **Protocol**: Choose HTTP or FTP. • **Port**: Enter the access port number.

Credentials	• **User ID**: Enter the user ID required to access the server. The username can contain only the following characters: a, 0-9, ., _, and -. • **Password**: Enter the password required to access the server. The password can contain only the following characters: a-z, A-Z, 0-9, _, *, ., +, =, %, and -. **Note** Special characters such as /, ?,:, @, and SPACE, which are used in URLs and are needed for proper parsing of fields so files can be fetched properly with the relevant protocol, are not supported in the username and the password. The use of valid characters is supported starting from Cisco vManage Release 20.9.1.
Image Info	• **Image Location Prefix**: Enter the folder path where the uploaded images must be stored • **VPN**: Enter the VPN ID, either the transport VPN, management VPN, or service VPN

1. Click Add to add the remote server.

Manage Remote Server

1. From the Cisco vManage menu, choose Maintenance > Software Repository.
2. For the desired remote server, click …
3. To view the remote server settings, click View Details.
4. To edit the remote server settings, click Edit. Edit any of the following settings as necessary and click Save.

Note

- You cannot edit the remote server settings if you have added locations of any software images on the remote server to the Cisco vManage software repository.
- If you wish to edit the remote server settings, remove the software image entries from the software repository and then edit the settings.

Server Info	• **Server Name**: Enter a name for the server. • **Server IP or DNS Name**: Enter the IP address or the DNS name of the server. • **Protocol**: Choose HTTP or FTP. • **Port**: Enter the access port number.

Credentials	• **User ID**: Enter the user ID required to access the server. The username can contain only the following characters: a, 0-9, ., _, and -. • **Password**: Enter the password required to access the server. The password can contain only the following characters: a-z, A-Z, 0-9, _, *, ., +, =, %, and -. **Note** Special characters such as /, ?,:, @, and SPACE, which are used in URLs and are needed for proper parsing of fields so files can be fetched properly with the relevant protocol, are not supported in the username and the password. The use of valid characters is supported starting from Cisco vManage Release 20.9.1.
Image Info	• **Image Location Prefix**: Enter the folder path where the uploaded images must be stored. • **VPN**: Enter the VPN ID, either the transport VPN, management VPN, or service VPN.

1. To delete the remote server, click Remove. Confirm that you wish to remove the remote server in the dialog box.

Note

Before deleting a remote server, remove any entries for software images on the remote server that you have added to the Cisco vManage software repository.

Add Software Images to the Repository

- Before you can upgrade the software on an edge device, Cisco vSmart Controller, or Cisco vManage to a new software version, you need to add the software image to the Cisco vManage software repository. The repository allows you to store software images on the local Cisco vManage server or add locations of software images stored on a remote file server.

The Cisco vManage software repository allows you to store images in three ways:

- **On the local Cisco** vManage server, to be downloaded over a control plane connection: Here, the software images are stored on the local Cisco 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 Cisco vManage server might not be able to monitor the software installation on the device even though it is proceeding correctly.
- **On the local Cisco v**Manage server, to be downloaded over an out-of-band connection: Here, the software images are stored on the local Cisco 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 Cisco vManage server can monitor the software installation.
- **On a remote server:** From Cisco vManage Release 20.7.1, you can store software images on a remote file server that is reachable through an FTP or HTTP URL. As part of the software upgrade process, the Cisco

vManage server sends this URL to the Cisco SD-WAN device, which establishes a connection to the file server to download the software images. In a multitenant Cisco SD-WAN deployment, only the provider can register a remote server with Cisco vManage and add locations of software images on the remote server to the Cisco vManage repository.

Note

- Starting from Cisco vManage Release 20.9.1, when downloading an image from a remote server manually, ensure that only the following valid characters are used:
- User ID: a-z, 0-9, ., _, –
- Password: a-z, A-Z, 0-9, _, *, ., +, =, %, –
- URL Name or Path: a-z, A-Z, 0-9, _, *, ., +, =, %, -,:, /, @, ? ~

1. From the Cisco vManage menu, choose Maintenance > Software Repository.
2. Click Software Images.
3. Click Add New Software.
4. Choose the location for the software image:

Note Store NFVIS upgrade images on the local Cisco vManage server.

a. To store the software image on the local Cisco vManage server and have it be downloaded to Cisco SD-WAN devices over a control plane connection, choose 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 Cisco vManage server.
2. Click Upload to add the image to the software repository.

b. To store the image on a remote Cisco vManage server and have it be downloaded to Cisco SD-WAN devices over an out-of-band management connection, choose Remote Server – vManage. The Upload Software to Remote Server – vManage dialog box opens.

1. In the vManage Hostname/IP Address field, enter the IP address of an interface on the Cisco vManage server that is in a management VPN (typically, VPN 512).
   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 Cisco vManage server.
2. Click Upload.

c. If the software image is stored on a remote server, choose Remote Server (preferred). The Add New Software via Remote Server slide-in pane appears. Before choosing this option, ensure that you have registered a remote server with Cisco vManage.

1. Click Image to upload a new software image, or SMU Image to upload an SMU image. The default selection is Image.
2. From the Remote Server Name drop-down list, choose the desired remote server.
3. Image Filename: Enter the image filename, including the file extension. For an SMU image, the file extension

must be .smu.bin.

4. For an SMU image, enter the correct SMU Defect ID and choose the correct SMU Type. An incorrect defect ID or SMU type selection can cause the software upgrade to fail.
5. Click Save.

View Software Images

- From the Cisco vManage menu, choose Maintenance > Software Repository.
- The Software Repository window displays the images available in the repository.
- 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 Cisco controller version.
- The software image can operate with the listed controller version or with a higher controller version.
- The Software Location column indicates where the software images are stored, either in the repository on the Cisco vManage server or in a repository in a remote location.
- The Available Files column lists the names of the software image files.
- The Updated On column shows when the software image was added to the repository.
- The … option for a desired software version provides the option to delete the software image from the repository.
- In Cisco vManage Release 20.6.x and earlier releases, when two or more software images have the same software version but are uploaded with different filenames, the images are listed in a single row. The Available Files column lists the different filenames.
- This listing scheme is disadvantageous when deleting software images as the delete operation removes all the software images corresponding to a software version.
- From Cisco vManage Release 20.7.1, when two or more software images have the same software version but are uploaded with different filenames, each software image is listed in a separate row. This enables you to choose and delete specific software images.

Upload VNF Images

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

- **Step** 1 From the Cisco vManage menu, choose Maintenance > Software Repository.
- **Step** 2 To add a prepackaged VNF image, click Virtual Images, and then click Upload Virtual Image.
- **Step** 3 Choose the location to store the virtual image.
- To store the virtual image on the local Cisco vManage server and download it to CSP devices over a control plane connection, click vManage. The Upload VNF's Package to vManage dialog box appears.
- **a**. Drag and drop the virtual image file or the qcow2 image file to the dialog box or click Browse to choose the virtual image from the local Cisco vManage server. For example, CSR.tar.gz, ASAv.tar.gz, or ABC.qcow2
- **b.** If you upload a file, specify the type of the uploaded file: Image Package or Scaffold. Optionally, specify a description of the file and add custom tags to the file. The tags can be used to filter images and scaffold files when creating a service chain.
- **c**. If you upload a qcow2 image file, specify the service or VNF type: FIREWALL or ROUTER. Optionally,

specify the following:

- Description of the image
- Version number of the image
- Checksum
- Hash algorithm
- You can also add custom tags to the file that can be used to filter images and scaffold files when creating a service chain.
- It is mandatory to upload a scaffold file if you choose a qcow2 image file.
- The option to select a qcow2 image file is available from Cisco vManage Release 20.7.1. In Cisco vManage Release 20.6.1 and earlier releases, you can select only a tar.gz file.
- **d**. 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 installation on the CSP devices.
- To store the image on a remote Cisco vManage server and then download it to CSP devices, click Remote Server
- vManage. The Upload VNF’s Package to Remote Server-vManage dialog box appears.
- **a.** In the vManage Hostname/IP Address field, enter the IP address of an interface on the Cisco vManage server that is in the management VPN (typically, VPN 512).
- **b.** Drag and drop the virtual image file or the qcow2 image file to the dialog box, or click Browse to choose the virtual image from the local Cisco vManage server.
- **c**. If you upload a file, specify the type of the uploaded file: Image Package or Scaffold. Optionally, specify a description of the file and add custom tags to the file. The tags can be used to filter images and scaffold files when creating a service chain.
- **d**. If you upload a qcow2 image file, specify the service or VNF type: FIREWALL or ROUTER. Optionally, specify the following:
- Description of the image
- The version number of the image
- Checksum
- Hash algorithm
- You can also add custom tags to the file that can be used to filter images and scaffold files when creating a service chain.
- It is mandatory to upload a scaffold file if you choose a qcow2 image file.
- The option to select a qcow2 image file is available from Cisco vManage Release 20.7.1. In Cisco vManage Release 20.6.1 and earlier releases, you can select only a tar.gz file.
- **e**. 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.
- You can have multiple VNF entries such as a firewall from the same or from different vendors. Also, you can add different versions of VNF that are based on the release of the same VNF. 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, and NICs for an HA link.
- Additional Storage–If more storage is required, specify predefined disks (qcow2), storage volumes (NFVIS layer)
- **Step** 1 From the Cisco vManage menu, choose Maintenance > Software Repository.
- Step 2 Click Virtual Images > Add Custom VNF Package.
- **Step** 3 Configure the VNF with the following VNF package properties and click Save.

Table 2: VNF Package Properties

Field	**Mandatory or Optional**	**Description**
Package Name	Mandatory	The filename of the target VNF packa ge. It’s the Cisco NFVIS image name with .tar or .gz extensions.
App Vendor	Mandatory	Cisco VNFs or third-party VNFs.
Name	Mandatory	Name of the VNF image.

Field	**Mandatory or Optional**	**Description**
Package Name	Mandatory	The filename of the target VNF packa ge. It’s the Cisco NFVIS image name with .tar or .gz extensions.
App Vendor	Mandatory	Cisco VNFs or third-party VNFs.
Name	Mandatory	Name of the VNF image.

- **Step** 4 To package a VM qcow2 image, click File Upload and browse to choose a qcow2 image file.
  Step 5 To choose a bootstrap configuration file for VNF, if any, click Day 0 Configuration and click File Upload to browse and choose the file.

- Include the following Day-0 configuration properties

Table 3: Day-0 Configuration

Field	**Mandatory or Optional**	**Description**
Mount	Mandatory	The path where the bootstrap file g ets mounted.
Parseable	Mandatory	A Day-0 configuration file can be parsed or not. Options are: **Enable** or **Disable**. By default, **Enable** is chosen.
High Availability	Mandatory	High availability for a Day-0 configu ration file to choose from. Supported values are Standalone, HA Primary, and HA Secondary.

- **Note** If any bootstrap configuration is required for a VNF, create a bootstrap-config or a day0-config file.
- **Step** 6 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 next to the desired Day-0 configuration file. In the Day 0 configuration file dialog box, perform the following tasks:
- 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.

Note

- **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 list, 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, choose and highlight a custom variable attribute from the text fields. Click Custom Variable. The Create Custom Variable dialog box appears.
- **d**) Enter the custom variable name and choose a type from the Type drop-down list.
- **e**) To set the custom variable attribute, do the following:
- To ensure that the custom variable is mandatory when creating a service chain, click Type next to Mandatory.
- To ensure that a VNF includes both primary and secondary day-0 files, click Type next to Common.
- **f**) Click Done, and then click Save. The highlighted custom variable attribute is replaced by the custom variable name.
- **Step** 7 To upload extra VM images, expand Advance Options, click Upload Image, and then browse to choose an extra 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 don't combine ephemeral disks and storage volumes when uploading extra VM images.
- **Step** 8 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 4: Storage Properties

Field	Mandatory or Optional	Description
Size	Mandatory	The disk size that is required for th e VM operation. If the size unit is Gi B, the maximum disk size can be 2 56 GiB.
Size Unit	Mandatory	Choose size unit. The supported units are: MIB, GiB, TiB.
Device Type	Optional	Choose a disk or CD-ROM. By default, disk is chosen.
Location	Optional	The location of the disk or CD-RO M. By default, it's local.
Format	Optional	Choose a disk image format. The supported formats are qcow2, r aw, and vmdk. By default, it's raw.
Bus	Optional	Choose a value from the drop-down list. The supported values for a bus are virtio, scsi, and ide. By default, it's v irtio.

- **Step** 9 To add VNF image properties, expand Image Properties and enter the following image information.

Table 5: VNF Image Properties

Field	Mandatory or Optional	Description
SR-IOV Mode	Mandatory	Enable or disable SR-IOV support. By default, it's enabled.

Field	Mandatory or Optional	Description
Monitored	Mandatory	VM health monitoring for those VM s that you can bootstrap. The options are: enable or disable. By default, it’s enabled.
Bootup Time	Mandatory	The monitoring timeout period for a monitored VM. By default, it’s 600 s econds.
Serial Console	Optional	The serial console is supported or not? The options are: enable or disable. By default, it’s disabled.
Privileged Mode	Optional	Allows special features like promisc uous mode and snooping. The options are: enable or disable. By default, it’s disabled.
Dedicate Cores	Mandatory	Facilitates allocation of a dedicated resource (CPU) to supplement a V M’s low latency (for example, router and firewall). Otherwise, shared res ources are used. The options are: enable or disable. By default, it’s enabled.

Step 10 To add VM resource requirements, expand Resource Requirements and enter the following information.

Table 6: VM Resource Requirements

Field	Mandatory or Optional	Description
Default CPU	Mandatory	The CPUs are supported by a VM. The maximum number of CPUs supported is 8.
Default RAM	Mandatory	The RAM is supported by a VM. Th e RAM can range from 2–32.
Disk Size	Mandatory	The disk size in GB is supported by a VM. The disk size can range from 4–256.
Max number of VNICs	Optional	The maximum number of VNICs all owed for a VM. The number of VNI Cs can from range 8–32 and by def ault, the value is 8.

Field	Mandatory or Optional	Description
Management VNIC ID	Mandatory	The management VNIC ID corresponds to the management interface. The valid range is from 0 to the maximum number of VNICs.
Number of Management VNICs ID	Mandatory	The number of VNICs.
High Availability VNIC ID	Mandatory	The VNIC IDs where high availability is enabled. The valid range is from 0–the maximum number of VNICs. It shouldn’t conflict with the management VNIC Id. By default, the value is 1.
Number of High Availability VNICs ID	Mandatory	The maximum number of VNIC IDs where high availability is enabled. The valid range is 0–(maximum number of VNICs-number of management VNICs-2) and by default, the value is 1.

Step 11 To add day-0 configuration drive options, expand Day 0 Configuration Drive options and enter the following information.

Table 7: Day-0 Configuration Drive Options

Field	Mandatory or Optional	Description
Volume Label	Mandatory	The volume label of the Day-0 configuration drive. The options are V1 or V2. By default, the option is V2. V2 is the config-drive label config-2. V1 is config-drive label data.
Init Drive	Optional	The Day-0 configuration file as a disk when mounted. The default drive is CD-ROM.
Init Bus	Optional	Choose an init bus. The supported values for a bus are virtio, scsi, and ide. By default, it’s ide.

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

View VNF Images

- **Step 1** From the Cisco vManage menu, choose Maintenance > Software Repository.

- **Step 2** Click Virtual Images.
- **Step 3** To filter the search results, use the filter option in the search bar.
- The Software Version column provides the version of the software image.
- The Software Location column indicates where the software images are stored. Software images can be stored either in
- the repository on the Cisco 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.
- Step 4 For the desired VNF image, click … and choose Show Info.
- Delete a Software Image from the Repository

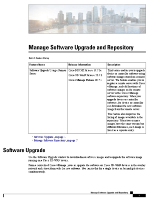
To delete a software image from the Cisco vManage software repository:

- **Step 1** From the Cisco vManage menu, choose Maintenance > Software Repository.
- **Step 2** For the desired software image, click … and choose Delete.
- If a software image is being downloaded to a router, you cannot delete the image until the download process completes.

Delete VNF Images

- **Step 1** From the Cisco vManage menu, choose Maintenance > Software Repository.
- **Step** 2 Click Virtual Images. The images in the repository are displayed in a table.
- **Step 3** For the desired image, click … and choose Delete.
- If you're downloading a VNF image to a device, you can't delete the VNF image until the download process completes.
  Note If the VNF image is referenced by a service chain, it can't be deleted.
- Manage Software Upgrades and Repository

Documents / Resources

	**CISCO Catalyst SD-WAN Manage Software Upgrade and Repository** [pdf] User Guide Catalyst SD-WAN Manage Software Upgrade and Repository, Catalyst SD-WAN, Manage Software Upgrade and Repository, Software Upgrade and Repository, Upgrade and Repository, Repository

References

- **Cisco SD-WAN Cloud OnRamp for Co-Location - End-User Guides - Cisco**

- Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide - Software Upgrade Workflow [Cisco SD-WAN] - Cisco
- Cisco Catalyst SD-WAN Getting Started Guide - Hardware and Software Installation [Cisco SD-WAN] - Cisco
- Cisco Catalyst SD-WAN Getting Started Guide - Cluster Management [Cisco SD-WAN] - Cisco
- Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Recommended Computing Resources - Cisco
- User Manual