

Manage Software Upgrade and Repository

- Manage Software Upgrade and Repository, on page 2
- Information about software upgrade, on page 5
- Restrictions for software upgrade, on page 8
- Upgrade Virtual Image on a Device, on page 9
- Upgrade the Software Image on a Device, on page 10
- Activate a New Software Image, on page 12
- Upgrade a CSP Device with a Cisco NFVIS Upgrade Image, on page 13
- Delete a Software Image, on page 14
- Set the Default Software Version, on page 14
- Export Device Data in CSV Format, on page 14
- View Log of Software Upgrade Activities, on page 15
- Manage Software Repository, on page 15

Manage Software Upgrade and Repository

Table 1: Feature History

Feature Name	Release Information	Description
Software Upgrade Using a Remote Server	Cisco IOS XE Catalyst SD-WAN 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 SD-WAN Manager, and add locations of software images on the remote server to the Cisco SD-WAN Manager software repository. When you upgrade 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 filenames, each image is listed as a separate entry.

Feature Name	Release Information	Description
Device version compliance in Cisco SD-WAN Manager	Cisco IOS XE Catalyst SD-WAN Release 17.18.x Cisco Catalyst SD-WAN Manager Release 20.18.1	

Manage Software Upgrade and Repository

Feature Name	Release Information	Description
		The Device Version Compliance feature in Cisco SD-WAN Manager ensures device compatibility when upgrading to Cisco Catalyst SD-WAN Manager Release 20.18.1. The Cisco Catalyst SD-WAN Manager Release 20.18.1 supports devices up to N-2 long-lived releases and does not support older versions in the Cisco Catalyst SD-WAN overlay. This feature implements the following key aspects: • Upgrade Blocking: Prevents Cisco SD-WAN Manager upgrades through the user interface if the overlay contains devices with software versions older than N-2. • Post-Upgrade Notification: After a Cisco SD-WAN Manager software upgrade to Cisco Catalyst SD-WAN Manager Release 20.18.1, Cisco SD-WAN Manager flags incompatible devices in the overlay through compliance banners and alarms. • Removal of End-of-Life (EOL) Platforms from ZTP Settings: Removes unsupported device families from the Zero Touch Provisioning settings page in Cisco SD-WAN Manager. • Cisco ISR 1100 and ISR 1100X Series Integrated Services Routers default operating system recognition: Changes the default recognition of Cisco ISR 1100 and ISR 1100X Series Integrated Services Routers from Viptela operating system to Cisco IOS XE operating system when they are added

Feature Name	Release Information	Description
		to and recognized by Cisco SD-WAN Manager. This change removes the Cisco ISR 1100 and ISR 1100X Series Integrated Services Routers migration menu in Cisco SD-WAN Manager when Cisco IOS XE operating system is detected.

Information about software upgrade

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

From a centralized Cisco SD-WAN Manager, you can upgrade the software on Cisco Catalyst 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 Catalyst SD-WAN Validator, Cisco Catalyst SD-WAN Controllers, and Cisco IOS XE Catalyst SD-WAN devices or Cisco vEdge devices in either a standalone or Cisco SD-WAN Manager cluster deployment, the software upgrade and reboot is performed first on the Cisco Catalyst SD-WAN Validator, next on the Cisco Catalyst SD-WAN Controller, and finally on the Cisco IOS XE Catalyst SD-WAN devices or Cisco vEdge devices. Up to 40 Cisco IOS XE Catalyst 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 Catalyst 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 SD-WAN Manager in a group software upgrade operation. You must upgrade and reboot the Cisco SD-WAN Manager server by itself.
- You can create a software upgrade workflow only for upgrading the Cisco Catalyst SD-WAN edge devices.
- It is recommended that you perform all software upgrades from Cisco SD-WAN Manager rather than from the CLI.
- For software compatibility information, see Cisco SD-WAN Controller Compatibility Matrix and Server Recommendations.

Note From Cisco Catalyst SD-WAN Manager Release 20.18.1, devices within the same site are upgraded sequentially. If a device fails, subsequent upgrades are skipped.

Prior to Cisco Catalyst SD-WAN Manager Release 20.18.1, devices within the same site are also upgraded sequentially. Even if a device fails, the remaining devices continue to upgrade.

The upgrade will proceed sequentially only if the certificate status of all devices with the same site ID is valid. If any device has an invalid certificate status, upgrades will occur in parallel.

Device version compliance

Device version compliance is a policy that

- ensures compatibility of network devices with Cisco SD-WAN Manager upgrades,
- supports devices in the overlay up to N-2 long-lived releases, and
- does not support devices older than this version in the overlay after an upgrade.

The release versions referenced in this policy are defined as follows:

- N: Represents the current Cisco SD-WAN Manager release (for example, Cisco Catalyst SD-WAN Manager Release 20.18.x).
- N-1: Refers to the prior long-lived release (for example, Cisco Catalyst SD-WAN Manager Release 20.15.x).
- N-2: Refers to the long-lived release two versions prior (for example, Cisco Catalyst SD-WAN Manager Release 20.12.x).

If you onboard a new device of any version, the device is still supported. However, after onboarding, this device will be flagged with a red banner in Cisco SD-WAN Manager, indicating that an upgrade is required.

Upgrade behavior

This feature changes the upgrade process depending on how the upgrade is initiated:

When a user initiates an upgrade to a newer Cisco SD-WAN Manager version (e.g., Cisco Catalyst SD-WAN Manager Release 20.18.x) through the UI, the upgrade is blocked if the overlay contains devices with software versions older than N-2 (e.g., Cisco Catalyst SD-WAN Manager Release 20.12.x).

For instance, if Cisco SD-WAN Manager is on version Cisco Catalyst SD-WAN Manager Release 20.15.1 and devices are on Cisco IOS XE Catalyst SD-WAN Release 17.9.x, an upgrade to Cisco Catalyst SD-WAN Manager Release 20.18.x will be blocked because the minimum supported device version for Cisco Catalyst SD-WAN Manager Release 20.18.x is Cisco Catalyst SD-WAN Manager Release 20.12.x. All devices in the network must be on version Cisco IOS XE Catalyst SD-WAN Release 17.12.x or above for the upgrade to proceed.

If a user performs the upgrade via the CLI, the upgrade proceeds even if devices are older than N-2. However, Cisco SD-WAN Manager displays a banner indicating the presence of less than N-2 devices and recommends upgrading them.

Device compliance notifications

Cisco SD-WAN Manager uses two primary methods to flag incompatible devices. If a user performs any operations on devices running versions older than N-2, it may lead to unexpected errors or device operational failures.

Compliance messages

A message appears in Cisco SD-WAN Manager when incompatible devices are detected. This message recommends upgrading those devices. Clicking the message redirects the user to the **Compliance & Conflicts** page, which displays the device status and software version.

- Error: If devices are less than N-2 versions, an error message appears:

```
Incompatible software version detected. Click here for details.
```

- Error: If devices are on N-3 version, or if Cisco Catalyst SD-WAN Controller or Cisco Catalyst SD-WAN Validator are on N-1 or N-2 versions, an error message appears:
  - N-3 devices with N version of SD-WAN Controller or SD-WAN Validator:

```
Incompatible software versions between the Manager and WAN Edge have been
 detected. Upgrade the software immediately to avoid any disruptions.
```

  - N-3 devices with N-1 or lesser versions of SD-WAN Controller or SD-WAN Validator:

```
Incompatible software versions between the Manager and Controller, Validator
 and WAN Edge have been detected. Upgrade the software immediately to avoid
 any disruptions.
```

Out of compliance alarm

An alarm is raised in the **Alarm Details** page in Cisco SD-WAN Manager when devices running versions older than N-2 are detected in the overlay. Multiple alarms may be raised if device versions change.

If the list of out-of-compliance devices contains five or fewer entries, the **Probable Causes** section displays the device hostnames. For more than five devices, the **Probable Causes** section displays only the count of out-of-compliance devices.

Unsupported devices

Starting with the Cisco Catalyst SD-WAN Manager Release 20.18.x release, Cisco SD-WAN Manager removes unsupported device families from the Zero Touch Provisioning (ZTP) settings page. These platform families include:

- Cisco vEdge Cloud
- Cisco ASR 1000 Series Aggregation Services Routers
- Cisco ASR 1002-X Series Aggregation Services Routers
- Cisco vEdge devices

Cisco ISR 1100 and ISR 1100X Series Integrated Services Routers default operating system recognition

Cisco SD-WAN Manager changes the default recognition of Cisco ISR 1100 and ISR 1100X Series Integrated Services Routers from Viptela operating system to Cisco IOS XE operating system. As a result, Cisco SD-WAN Manager removes the Migration menu if it detects that a Cisco ISR 1100 and ISR 1100X Series Integrated Services Router is running Cisco IOS XE operating system. However, the Migration menu continues to be displayed for devices running Viptela operating system.

Restrictions for software upgrade

Upgrade only

The software upgrade process can only install a later release (upgrade) not an earlier release (downgrade). For example you can upgrade from 17.15.1 to 17.16.1.

Migration of the device configuration only when installing a release

A device migrates the current active configuration to another release only when installing the new release. If you have a release that is installed but out of sync with recent configuration changes, you can trigger a fresh migration of the current configuration. Uninstall the release that is out of sync, then re-install the release.

Reactivating an earlier release

A device can have more than one release installed, but only one release is active at a given time.

If a device is running release A (example: 17.15.1), you can install a later release B (example: 17.16.1). After you activate release B, the inactive release A keeps its configuration in the state when release A was last active. Configuration changes you make while release B is active do not affect the configuration stored with release A.

If you keep release A installed on the device and later reactivate release A, the device uses the stored configuration reflecting the state when release A was last active.

Device version compatibility

The following restrictions are the restrictions for device compatibility when upgrading Cisco SD-WAN Manager to Cisco Catalyst SD-WAN Manager Release 20.18.x:

Device software version support

Cisco Catalyst SD-WAN Manager Release 20.18.x supports devices running up to N-2 long-lived software releases. Devices running software versions older than N-2 are not supported in the Cisco Catalyst SD-WAN overlay. For more information, see Device version compliance, on page 6.

Upgrade blocking

Cisco SD-WAN Manager prevents upgrades through the user interface if the Cisco Catalyst SD-WAN overlay contains devices with software versions older than N-2. For more information, see the section Upgrade behavior in Device version compliance, on page 6.

Post-Upgrade notification

After a Cisco SD-WAN Manager software upgrade to Cisco Catalyst SD-WAN Manager Release 20.18.x, Cisco SD-WAN Manager flags incompatible devices in the overlay through compliance notifications and alarms. For more information, see the section Device compliance notifications in Device version compliance, on page 6.

Removal of End-of-Life platforms in Cisco SD-WAN Manager

Cisco SD-WAN Manager removes unsupported device families from the **Zero Touch Provisioning** settings page. For more information, see the section Unsupported devices in Device version compliance, on page 6.

Cisco ISR 1100 and ISR 1100X Series Integrated Services Routers default operating system recognition

Cisco SD-WAN Manager changes the default recognition of Cisco ISR 1100 and ISR 1100X Series Integrated Services Routers from Viptela operating system to Cisco IOS XE operating system. This change helps prevent upgrade blocks for these devices and removes the migration menu when Cisco IOS XE operating system is detected. For more information, see the section Cisco ISR 1100 and ISR 1100X Series Integrated Services Routers default operating system recognition in Device version compliance, on page 6.

Upgrade Virtual Image on a Device

1. From the Cisco SD-WAN Manager 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 **Manager** or **Remote Server - Manager**, 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 Catalyst SD-WAN Getting Started Guide.
- If you want to perform a Cisco SD-WAN Manager cluster upgrade see, Upgrade Cisco SD-WAN Manager Cluster.
- Starting from Cisco vManage Release 20.11.1, 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 SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade**.
2. Click **WAN Edge**, **Control Components**, or **Manager** 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 SD-WAN Manager 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: **Manager**, **Remote Server**, or **Remote Server – Manager**.

Note

- The Remote Server option is introduced in Cisco vManage Release 20.7.1. If you chose **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, _, *, ., +, =, %, -, :, /, @, ?, ~

Note Software images created before upgrading the Cisco SD-WAN Manager to version Cisco Catalyst SD-WAN Manager Release 20.18.1 lack platform family and version details. To use these images after the upgrade, edit them in **Maintenance** > **Software Repository** and add the required platform family and version information.

b. For **Manager**, choose the image version from the **Version** drop-down list.

c. For **Remote Server – Manager**, choose the **Manager 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 SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade** and view the devices.
8. Click **WAN Edge**, **Controller**, or **Manager** 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

- If the control connection to Cisco SD-WAN Manager does not come up within the configured time limit, Cisco SD-WAN Manager automatically reverts the device to the previously running software image. The configured time limit for all Cisco Catalyst 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 Catalyst SD-WAN 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 SD-WAN Manager 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 software for Cisco SD-WAN Manager 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 SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade**.
2. Choose **WAN Edge**, **Control Components**, or **Manager**.
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 SD-WAN Manager reboots the device and activates the new software image.

If the control connection to Cisco SD-WAN Manager does not come up within the configured time limit, Cisco SD-WAN Manager automatically reverts the device to the previously running software image. The configured time limit for all Cisco Catalyst SD-WAN devices to come up after a software upgrade is 5 minutes, except for Cisco vEdge device, which have a default time of 12 minutes.

If the image activation fails, do not attempt to activate the image again. Remove the image from the device, then attempt to install and activate the image again.

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 `.nfvispkg` extension.

Procedure

Step 1 From theCisco SD-WAN Manager 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 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 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 SD-WAN Manager 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 upgrade if you check the **Activate and Reboot** check box, or by manually clicking **Activate** after choosing the CSP device again.

To verify if CSP device has rebooted and is running, use the task view window. Cisco SD-WAN Manager polls your entire network every 90 seconds up to 30 times and shows the status on th 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 Catalyst SD-WAN device:

1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade**.
2. Click **WAN Edge**, **Control Components**, or **Manager**.
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 Catalyst 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.

In case of error, see Error message during software upgrade or setting default software version.

To set a software image to be the default image on a device:

1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade**.
2. Click **WAN Edge**, **Control Components**, or **Manager**.
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 SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade**.
2. Click **WAN Edge**, **Control Components**, or **Manager**.
3. Choose one or more devices by checking the checkbox for the desired device or devices.
4. Click the download icon.

Cisco SD-WAN Manager 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 `Software_Upgrade.csv`

View Log of Software Upgrade Activities

1. From the Cisco SD-WAN Manager toolbar, click the **Tasks** icon.

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

1. From the Cisco SD-WAN Manager 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, FTP, or SCP. • **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-z, 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 the 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. For SCP, use the absolute directory path as the **Image Location Prefix**; for FTP or HTTP, use the relative path from the home directory. • **VPN**: Enter the VPN ID, either the transport VPN, management VPN, or service VPN

4. Click **Add** to add the remote server.

Enable devices to use a remote repository server

See Enable Software Updates by a Remote Repository Server.

Manage Remote Server

1. From the Cisco SD-WAN Manager 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 SD-WAN Manager 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, FTP, or SCP. • **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-z, 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 the 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. For SCP, use the absolute directory path as the **Image Location Prefix**; for FTP or HTTP, use the relative path from the home directory. • **VPN**: Enter the VPN ID, either the transport VPN, management VPN, or service VPN.

5. 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 SD-WAN Manager software repository.

Add Software Images to the Repository

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

The Cisco SD-WAN Manager software repository allows you to store images in three ways:

- On the local Cisco SD-WAN Manager server, to be downloaded over a control plane connection: Here, the software images are stored on the local Cisco SD-WAN Manager server, and they are downloaded to the Cisco Catalyst 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 SD-WAN Manager server might not be able to monitor the software installation on the device even though it is proceeding correctly.



Note From Cisco Catalyst SD-WAN Manager Release 20.18.1, image uploads to the Cisco SD-WAN Manager repository fail when disk space limits are exceeded. In a cluster environment, the disk space is assessed on all nodes simultaneously. Even if one node is experiencing low disk space, the image upload will fail for all nodes.

When the total utilized space exceeds the limit, you may delete the existing image data on the local server. If this does not resolve the issue or if there is no existing image data to delete, please contact your network administrator for further assistance in freeing up disk space. The administrator can ensure that the total used space at /opt/data/ remains below 80%.

- On the local Cisco SD-WAN Manager server, to be downloaded over an out-of-band connection: Here, the software images are stored on the local Cisco SD-WAN Manager server, and they are downloaded to the Cisco Catalyst 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 SD-WAN Manager server is able to 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 SD-WAN Manager server sends this URL to the Cisco Catalyst SD-WAN device, which establishes a connection to the file server to download the software images. In a multitenant Cisco Catalyst SD-WAN deployment, only the provider can register a remote server with Cisco SD-WAN Manager and add locations of software images on the remote server to the Cisco SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager server.

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

   b. To store the image on a remote Cisco SD-WAN Manager server and have it be downloaded to Cisco Catalyst SD-WAN devices over an out-of-band management connection, choose **Remote Server - Manager**. The **Upload Software to Remote Server - Manager** dialog box opens.
      1. In the **Manager Hostname/IP Address** field, enter the IP address of an interface on the Cisco SD-WAN Manager 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 Cisco SD-WAN Manager server.
      3. 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 SD-WAN Manager.

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 SD-WAN Manager menu, choose **Maintenance** > **Software Respository**.

The **Software Repository** window displays the images avaialable in the repository.

The **Software Version** column lists the version of the software image, and the **Controller Version** column lists the version of Cisco SD-WAN Control Components that is equivalent to the software version. The Cisco SD-WAN Control Components version is the minimum supported version. The software image can operate with the listed Cisco SD-WAN Control Components version or with a higher version.

The **Software Location** column indicates where the software images are stored, either in the repository on the Cisco SD-WAN Manager 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 20.6.1 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.

Add Virtual Images to the Repository

1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository**.
2. Click **Virtual Images**.
3. Click **Add New Virtual Image** and choose one of the following options:
   - **Remote Server (preferred)**: Choose this option to link to an image that has been uploaded to a remote server.

Note Before choosing this option, ensure that you have registered a remote server with Cisco SD-WAN Manager. For more information on how to register a remote server, see Register Remote Server.

The **Add Virtual Image with Remote Server Details** slide-in pane appears. (This option does not store the image on the local Cisco SD-WAN Manager server).

For Cisco vManage Release 20.11.1 and later, follow these steps:

a. Click **Add New Virtual Image** and choose **Remote Server (preferred)**.

b. In the **Image Name** field, enter the file name of the image.

c. In the **Image description** field, enter a description of the image.

d. (Optional) Click the **Add Tags** field and choose tags for the virtual image file.

e. In the **Select service type** field, choose **App-Hosting**.

The following applications are supported:

- **UTD-Snort-Feature**
- **DRE-Optimization-Feature**
- **ThousandEyes-Enterpeise-Agent**
- **Cybervision-Enterprise-Agent**

For standard filenames, Cisco SD-WAN Manager automatically displays the attributes of the image file.

For non-standard filenames, enter the following manually:

- **App type**: Choose an application type from the drop-down list.
- **Enter version**: Enter the version as free text.

  Cisco SD-WAN Manager automatically chooses the x86_64 architecture. You can choose a different architecture if necessary from the drop-down list.

f. Click the **Remote Server Name** field and choose a remote server.

g. In the **Image File Path** field, enter a path from the root directory of the remote server.

If you do not enter a path, Cisco SD-WAN Manager uses the root directory.

h. (Optional) To provide another server that contains the image, click **Add Remote Server**, and enter the details of the additional server.

i. Click **Add**.

- **Manager**: Choose this option to upload a file to the local Cisco SD-WAN Manager repository using a control-plane connection. This option is useful for uploading small files.

The **Upload VNF's Package to Manager** dialog box opens.

a. Drag and drop the virtual image file to the dialog box or click **Browse** to select the virtual image file from a directory on the local Cisco SD-WAN Manager server.

b. In the **Description** field, enter the description.

c. In the drop-down list, choose **Image Package** or **Scaffold**.

d. Click the **Add Tags** field and choose tags for the virtual image file.

e. Click **Upload** to add the virtual image file to the repository.

- **Remote Server - Manager**: Choose this option to store the virtual image file on a remote Cisco SD-WAN Manager server and download the virtual image file to Cisco Catalyst SD-WAN devices over an out-of-band management connection.

  The **Upload VNF's Package to Remote Server - Manager** dialog box opens.

  a. In the **Manager Hostname/IP Address** field, enter the IP address of an interface on the Cisco SD-WAN Manager server that is in a management VPN (typically, VPN 512).

  b. Drag and drop the virtual image file to the dialog box or click **Browse** to select the virtual image file from a directory on the local Cisco SD-WAN Manager server.

  c. In the **Description** field, enter the description of the virtual image file.

  d. In the drop-down list, choose **Image Package** or **Scaffold**.

  e. Click the **Add Tags** field and choose tags for the virtual image file.

  f. Click **Upload**.

Note To upload virtual images using the **Manager** or **Remote Server - Manager** options, use files with extensions, .tar, .gz, .tar or .qcow2. For more information on the steps to upload virtual images with extensions .tar, gz, .tar or .qcow2, see Upload VNF Images, on page 21

Upload VNF Images

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

Procedure

Step 1 From the Cisco SD-WAN Manager 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 SD-WAN Manager server and download it to CSP devices over a control plane connection, click **Manager**. The **Upload VNF's Package to Manager** 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 SD-WAN Manager 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.

   Note
   - 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 available for installing on the CSP devices.

- To store the image on a remote Cisco SD-WAN Manager server and then download it to CSP devices, click **Remote Server - Manager**. The **Upload VNF's Package to Remote Server-Manager** dialog box appears.

  a. In the **Manager Hostname/IP Address** field, enter the IP address of an interface on Cisco SD-WAN Manager 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 SD-WAN Manager 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
     - 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.

Note

- 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 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, NICs for a HA link.
- Additional Storage–If more storage is required, specify predefined disks (qcow2), storage volumes (NFVIS layer)

Procedure

Step 1 From the Cisco SD-WAN Manager 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 package. 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.
Version	Optional	Version number of a program.
Type	Mandatory	Type of VNF to choose. Supported VNF types are: Router, Firewall, Load Balancer, and Other.

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 gets 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 configuration file to choose. Supported values are: Standalone, HA Primary, 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:

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 Custom Packaging Details for Shared VNF topic and 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 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 **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 the VM operation. If the size unit is GiB, the maximum disk size can be 256 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-ROM. By default, it's local.
Format	Optional	Choose a disk image format. The supported formats are: qcow2, raw, and vmdk. By default, it's raw.

Field	Mandatory or Optional	Description
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 virtio.

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.
Monitored	Mandatory	VM health monitoring for those VMs 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 seconds.
Serial Console	Optional	The serial console that is supported or not. The options are: enable or disable. By default, it's disabled.
Privileged Mode	Optional	Allows special features like promiscuous 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 VM's low latency (for example, router and firewall). Otherwise, shared resources 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 supported by a VM. The maximum numbers of CPUs supported are 8.
Default RAM	Mandatory	The RAM supported by a VM. The RAM can range 2–32.
Disk Size	Mandatory	The disk size in GB supported by a VM. The disk size can range 4–256.
Max number of VNICs	Optional	The maximum number of VNICs allowed for a VM. The number of VNICs can from range 8–32 and by default, the value is 8.
Management VNIC ID	Mandatory	The management VNIC ID corresponding to the management interface. The valid range is from 0 to 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–maximum number of VNICs. It shouldn't conflict with 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 cidata.

Field	Mandatory or Optional	Description
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

Procedure

Step 1 From the Cisco SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager software repository:

Procedure

Step 1 From the Cisco SD-WAN Manager 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

Procedure

Step 1 From the Cisco SD-WAN Manager 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**.



Note 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.