Manage Device Software Images

- Set Up Software Image Management, on page 1
- Copy Software Images from Devices to the Image Repository (Create a Baseline), on page 4
- How Do I Find Out Which Images Are Used by Network Devices?, on page 5
- How Do I Know a Device Has the Latest Image?, on page 5
- View the Images That Are Saved in the Image Repository, on page 5
- Find Out Which Devices Are Using an Image, on page 6
- How Do I Know Whether I have Permission to Download Software from Cisco.com, on page 7
- Add (Import) Software Images to the Repository, on page 7
- Change the Device Requirements for Upgrading a Software Image, on page 10
- Verify That Devices Meet Image Requirements (Upgrade Analysis), on page 10
- Distribute a New Software Image to Devices, on page 11
- Activate a New Software Image on Devices, on page 17
- Activate, Deactivate, and Remove Cisco IOS XR Images from Devices, on page 20
- View and Upgrade FPD Images, on page 21
- Commit Cisco IOS XR Images Across Device Reloads, on page 21
- Roll Back Cisco IOS XR Images, on page 22
- Check the Network Audit for Software Image Operations, on page 22
- Delete Software Image Files from the Image Repository, on page 23

Set Up Software Image Management

Note

- Make Sure Devices Are Configured Correctly, on page 2
- Verify the FTP/TFTP/SFTP/SCP Settings on the Cisco EPN Manager Server, on page 2
- How to Control Images that are Saved to the Image Repository During Inventory Collection, on page 2
- Adjust Image Transfer and Distribution Preferences, on page 3

Make Sure Devices Are Configured Correctly

Cisco EPN Manager can transfer files to and from devices only if the SNMP read-write community strings configured on your devices match the strings that were specified when the devices were added to Cisco EPN Manager. In addition, devices must be configured according to the settings in How Is Inventory Collected?.

Note To improve security, Cisco EPN Manager no longer uses some of the SSH CBC (Cipher Block Chaining) ciphers that older Cisco IOS-XE and IOS-XR versions use, as they have been deemed weak. For devices running Cisco IOS-XE, ensure that you upgrade to version 16.5.x or later. And for devices running Cisco IOS-XR, upgrade to version 6.1.2 or later. Otherwise, several Software Image Management operations will fail.

Although we do not recommend doing so (since it weakens security), you also have the option to add the CBC ciphers that Cisco EPN Manager stopped using back to its SSHD service configuration file. To do so, first configure the CBC ciphers in the ciphers line of the file located in the **/etc/ssh/sshd_config** directory (as shown in the example below), then restart the sshd service using the **service sshd stop/start** command.

```
Ciphers aes128-ctr,aes192-ctr,aes256-ctr,
arcfour256,arcfour128,aes128-cbc,3des-cbc,
cast128-cbc,aes192-cbc,aes256-cbc
```

Note Software Image Management is not supported in the NAT environment. This means that image management features such as image import, upgrade, distribution, and activation, will not function in the NAT environment.

Verify the FTP/TFTP/SFTP/SCP Settings on the Cisco EPN Manager Server

If you will be using FTP, TFTP, SFTP, or SCP make sure that it is enabled and properly configured. See Enable FTP/TFTP/SFTP Service on the Server.

How to Control Images that are Saved to the Image Repository During Inventory Collection

Because collecting software images can slow the data collection process, by default, Cisco EPN Manager does not collect and store device software images in the image repository when it performs inventory collection. Users with Administration privileges can change that setting using the following procedure.

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **Inventory** > **Image Management**.

Step 2 To retrieve and store device images in the image repository when Cisco EPN Manager performs inventory collection, check the **Collect images along with inventory collection** check box.

Step 3 Click **Save**.

Adjust Image Transfer and Distribution Preferences

Use this procedure to specify the default protocols Cisco EPN Manager should use when transferring images from the software image management server to devices. You can also configure Cisco EPN Manager to perform, by default, a variety of tasks associated with image transfers and distributions—for example, whether to back up the current image before an upgrade, reboot the device after the upgrade, continue to the next device if a serial upgrade fails, and so forth. Users with Administration privileges can change that setting using the following procedure.

This procedure only sets the defaults. You can override these defaults when you perform the actual distribute operation.

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **Inventory** > **Software Image Management**.

Step 2 On the **Basic** tab, specify the tasks that Cisco EPN Manager should perform when distributing images:

Setting	Description	Default
Job Preferences		
Continue distribution on failure	If distributing images to multiple devices and distribution to a device fails, continues the distribution to other devices	Enabled
TFTP fallback	Inserts the TFTP fallback command into the running image so that it can be reloaded if image distribution fails Inserts the TFTP fallback command into the running image so that it can be reloaded if image distribution fails	Disabled
Backup running image	Before image distribution, backs up the running image to the TFTP server	Disabled
Insert boot command	Inserts the boot command into the running image, after image distribution	Disabled
Smart Flash Delete Before Distribution	Delete the unnecessary files from flash to free up the memory space before distribution	Disabled
Other Preferences		
Collect images along with inventory collection	Choose this option if you want the software image to be collected from the device and store in the image repository during inventory collection.	Disabled
Show latest images for the available major releases	Choose this option if you want to view the latest maintenance release.	Disabled
Show images with same feature support	Choose this option if you want to view the available images with the same features supported by the running image.	Disabled
Show available higher image versions	Choose this option if you want to view the available higher image versions for the running image.	Disabled
Remove the option to activate software during distribution jobs	Choose this option to remove the option to activate the software during distribution jobs.	Disabled

Setting	Description	Default
Copy operation to be initiated by the EPN Manager server	Choose this option if you want the copy operation to be initiated by the EPN Manager server.	Disabled

Step 3 Specify the default protocol Cisco EPN Manager should use when transferring images in the Image Transfer Protocol Order. Arrange the protocols in order of preference. If the first protocol listed fails, Cisco EPN Manager will use the next protocol in the list.

Note When distributing an image to a device, use the most secure protocols supported by the device (for example, SCP instead of TFTP). TFTP tends to time out when transferring very large files or when the server and client are geographically distant from each other. If you choose SCP for the image distribution, ensure that the device is managed in Cisco EPN Manager with full user privilege (Privileged EXEC mode); otherwise the distribution will fail due to copy privilege error (SCP: protocol error: Privilege denied).

Step 4 Click **Save**.

Add a Software Image Management Server to Manage Groups of Devices

To distribute images to a group of devices, add a software image management server and specify the protocol it should use for image distribution. You can add a maximum of three servers.

Step 1 Add the server.

a) Choose **Administration** > **Servers** > **Software Image Management Servers**.
b) Click the Add Row icon and enter the server name, IP address, and device group the server will support.
c) Click **Save**.

Step 2 Configure the server protocol settings.

a) Check the check box next to the server name, then click **Manage Protocols**.
b) Click the Add Row icon and enter the software image management protocol details (username, password, and so forth).
c) Click **Save**.

Copy Software Images from Devices to the Image Repository (Create a Baseline)

Depending on your system settings, Cisco EPN Manager may copy device software images to the image repository during inventory collection (see How to Control Images that are Saved to the Image Repository During Inventory Collection, on page 2). If you need to perform this operation manually, use the following procedure, which imports software images directly from devices into the image repository.

Before you begin, ensure that images are physically present on the devices (rather than remotely loaded).

Note If you are importing many images, perform this operation at a time that is least likely to impact production.

Step 1 Choose **Inventory** > **Device Management** > **Software Images**.

Step 2 Click the **Add/Import** icon.

Step 3 In the Import Images dialog box, complete the following:

a) In the **Source** area, select the devices (you may want to select one device group at a time).

b) In the **Collection Options** area, specify whether to import the files immediately or schedule the import for later.

Step 4 Click **Submit**.

How Do I Find Out Which Images Are Used by Network Devices?

To view a list of the images used by network devices, choose **Reports** > **Reports Launch Pad** > **Device** > **Detailed Software**.

To list the top ten images use by network devices (and how many devices are using those images), choose **Inventory** > **Device Management** > **Software Images**. Click **Software Image Repository** under **Useful Links**, then then click the **Image Dashboard** icon in the top-right corner of the page.

How Do I Know a Device Has the Latest Image?

If your device type supports image recommendations, you can use the following procedure to check if a device has the latest image from Cisco.com. Otherwise, use the Cisco.com product support pages to get this information.

Step 1 Choose **Inventory** > **Device Management** > **Network Devices**, then click the device name hyperlink to open the Device Details page.

Step 2 Click the **Software Image** tab and scroll down to the Recommended Images area. Cisco EPN Manager lists all of the images from Cisco.com that are recommended for the device.

For Cisco NCS 2000 and Cisco ONS devices, this choice is displayed on the right when you click the **Chassis View** tab.

Note The recommendations list is purely informational. To use any of the recommended images, you must get them from Cisco.com and add them to the image repository. See Add (Import) Software Images to the Repository, on page 7.

View the Images That Are Saved in the Image Repository

Use this procedure to list all of the software images saved in the image repository. The images are organized by image type and stored in the corresponding software image group folder.

Step 1 Choose **Inventory** > **Device Management** > **Software Images**. Cisco EPN Manager lists the images that are saved in the image repository within the **Software Image Summary** panel.

From here you can:

- Import new images into the image repository from network devices; file systems on client machines, IPv4 or IPv6 servers (URLs), FTP servers, and Cisco.com. You can use the web GUI to find out what images are available from Cisco.com, but images must be manually downloaded and then imported. See Add (Import) Software Images to the Repository, on page 7.
- Adjust the requirements that a device must meet in order to upgrade to this image. See Change the Device Requirements for Upgrading a Software Image, on page 10.
- Perform an upgrade analysis. See Verify That Devices Meet Image Requirements (Upgrade Analysis), on page 10.
- Copy new software images to devices. See Distribute a New Software Image to Devices, on page 11.
- Activate images, which makes a new image the device's running image. See Activate a New Software Image on Devices, on page 17.
- Commit Cisco IOS XR images, which persists the image across device reloads and creates a rollback point. See Commit Cisco IOS XR Images Across Device Reloads, on page 21.
- Delete images from the image repository (images can only be deleted using the manual process). See Delete Software Image Files from the Image Repository, on page 23.

Step 2 Go to Software Image repository and click a software image hyperlink to open the Image Information page that lists the file and image name, family, version, file size, and so forth.

From here you can:

- See which devices are using this image by checking the Device Details area at the bottom of the page.
- Adjust the requirements that a device must meet in order to upgrade to this image. (See Change the Device Requirements for Upgrading a Software Image, on page 10.)

Find Out Which Devices Are Using an Image

Step 1 Choose **Inventory** > **Device Management** > **Software Images**.

Step 2 In the **Software Image Summary** panel, locate the image that you are interested in by expanding the image categories in the navigation area or entering partial text in one of the Quick Filter fields. For example, entering **3.1** in the Version field would list Versions 3.12.02S, 3.13.01S, and so forth.

Step 3 Click the image hyperlink to open the Software Image Summary page. Cisco EPN Manager lists all devices using that image in the Device Details area.

How Do I Know Whether I have Permission to Download Software from Cisco.com

Cisco EPN Manager displays the recommended latest software images for the device type you specify, and it allows you to download the software images directly from Cisco.com. In order to download a EULA or K9 software image from Cisco.com, you must accept/renew the EULA agreement or K9 Agreement periodically.

Cisco EPN Manager does not display deferred software images. For detailed information, see the Cisco EPN Manager 2.1 Supported Devices list.

Add (Import) Software Images to the Repository

Cisco EPN Manager displays the recommended latest software images for the device type you specify, and it allows you to download the software images directly from cisco.com. Cisco EPN Manager does not display deferred software images. For detailed information, see Cisco EPN Manager 3.1 Supported Devices list.

Note In order to download a K9 software image from cisco.com, you must accept/renew the https://software.cisco.com/download/eula.html K9 agreement periodically.

The following topics explain the different ways you can add software images to the image repository. For an example of how to troubleshoot a failed import, see Manage Jobs Using the Jobs Dashboard.

- Add a Software Image That Is Running on a Managed Device, on page 7
- Add a Software Image from an IPv4 or IPv6 Server (URL), on page 8
- Add a Software Image for an FTP Protocol Server (Protocol), on page 9
- Add a Software Image from a Client Machine File System, on page 9

Note

- For Cisco NCS and Cisco ONS devices, you can only import software images using the procedure in Add a Software Image from a Client Machine File System, on page 9.

Add a Software Image That Is Running on a Managed Device

This method retrieves a software image from a managed device and saves it in the image repository.

Note When distributing an image to a device, use the most secure protocols supported by the device (for example, SCP instead of TFTP). TFTP tends to time out when transferring very large files or when the server and client are geographically distant from each other. If you choose SCP for the image distribution, ensure that the device is managed in Cisco EPN Manager with full user privilege (Privileged EXEC mode); otherwise the distribution will fail due to copy privilege error (SCP: protocol error: Privilege denied).

Note that TFTP is supported only when copying images from the device to the server and not the other way around.

Limitations:

- For Cisco IOS-XR devices, direct import of images from the device is not supported by Cisco EPN Manager; SMU and PIE imports are also not supported on these devices.
- For Cisco IOS-XE devices, if the device is loaded with the 'packages.conf' file, then images cannot be imported directly from that device.

Step 1 Choose **Inventory** > **Device Management** > **Software Images**.

Step 2 Click the **Add/Import** icon.

Step 3 In the Import Images dialog:

a) Click **Device** and under Collection Options, choose one or more devices.
b) Select the **VRF Name** check-box and specify the VRF name if you want to enable collection via VRF.
c) In the Schedule area, schedule the job to run immediately, at a later time, or on a regular basis.
d) Click **Submit**.

Step 4 To view the status of the job, click the job link in the pop-up message or choose **Administration > Job Dashboard**.

Step 5 Verify that the image is listed on the Software Images page (**Inventory** > **Device Management** > **Software Images**).

Add a Software Image from an IPv4 or IPv6 Server (URL)

You can import software image from network-accessible IPv4 or IPv6 servers. The following file formats are supported: .bin, .tar, .aes, .pie, .mini, .vm, .gz, .ova, and .ros.

The file that you import must follow the recommended file naming convention. For example, the naming convention for .tar files is *image family*-*****-*image version*.**tar**. Here, the image family must be in capital case. Based on the naming convention, the name for the NCS540.tar file must be **NCS540-iosxr-k9-6.0.2.tar**.

Cisco EPN Manager supports to import Non-Cisco standard image.

Step 1 Choose **Inventory > Device Management > Software Images**.

Step 2 Click the **Add/Import** icon.

Step 3 In the Import Images dialog:

a) Click **URL**.
b) In the URL To Collect Image field, enter a URL in the following format (you can also use an HTTP URL where user credentials are not required):

http://*username***:***password***@***server-ip/filename*

c) In the Schedule area, schedule the job to run immediately, at a later time, or on a regular basis.
d) Click **Submit**.

Step 4 To view the status of the job, click the job link in the pop-up message or choose **Administration > Job Dashboard**.

Step 5 Verify that the image is listed on the Software Images page (**Inventory** > **Device Management** > **Software Images**).

Add a Software Image for an FTP Protocol Server (Protocol)

Step 1 Choose **Inventory > Device Management > Software Images**.

Step 2 Click the **Add/Import** icon.

Step 3 In the Import Images dialog:

a) Click **Protocol**.
b) Enter FTP in the Protocol field, then enter the FTP user name, password, server name or IP address, and file name. The following is a file name example:

/*ftpfolder*/asr901-universalk9-mz.154-3.S4.bin

c) In the Schedule area, schedule the job to run immediately, at a later time, or on a regular basis.
d) Click **Submit**.

Step 4 To view the status of the job, click the job link in the pop-up message or choose **Administration > Job Dashboard**.

Step 5 Verify that the image is listed on the Software Images page (**Inventory > Device Management > Software Images**).

Add a Software Image from a Client Machine File System

Before you begin

When you import the software image file, the browser session is blocked temporarily. If the upload operation exceeds the idle timeout limit of the browser session, then you will be logged out of Cisco EPN Manager and the file import operation will be aborted. So it is recommended that you increase the idle timeout limit before you begin with this import operation. To increase the idle timeout, see *Cisco Prime Infrastructure Administrator Guide*.

Step 1 Choose **Inventory > Device Management > Software Images**.

Step 2 Click the **Add/Import** icon.

Step 3 In the Import Images dialog:

a) Click **File**.
b) Click the **Browse** button and navigate to the software image file.
c) In the Schedule area, schedule the job to run immediately, at a later time, or on a regular basis.
d) Click **Submit**.

Note You must use the URL or Protocol options to import files of larger size (say, greater than 200 MB), as importing through the File option is not recommended.

Step 4 To view the status of the job, click the job link in the pop-up message or choose **Administration > Job Dashboard**.

Step 5 Verify that the image is listed on the Software Images page (**Inventory > Device Management > Software Images**).

Change the Device Requirements for Upgrading a Software Image

Use this procedure to change the RAM, flash, and boot ROM requirements that a device must meet for a software image to be distributed to the device. These values are checked when you perform an upgrade analysis (see Verify That Devices Meet Image Requirements (Upgrade Analysis), on page 10).

Note This operation is not supported on the Cisco NCS 2000 and Cisco ONS families of devices.

Step 1 Choose **Inventory > Device Management > Software Images**.

Step 2 In the **Software Image Summary** panel, locate and select the software image by clicking its associated hyperlink.

Step 3 Click the software image name hyperlink to open its image information.

Step 4 Adjust the device requirements:

- Minimum RAM (from 1 – 999999999999999)
- Minimum FLASH (from 1 – 999999999999999)
- Minimum Boot ROM Version

Step 5 Click **Save**.

Step 6 Click **Restore Defaults**, if you want to retain the previous requirements.

Verify That Devices Meet Image Requirements (Upgrade Analysis)

An upgrade analysis verifies that the device contains sufficient RAM or FLASH storage (depending on the device type) , the image is compatible with the device family, and the software version is compatible with the image version running on the device. After the analysis, Cisco EPN Manager displays a report that provides the results by device. The report data is gathered from:

- The software image repository, which contains information about minimum RAM, minimum Flash, and so on, in the image header.
- The Cisco EPN Manager inventory, which contains information about the active images on the device, as well as Flash memory, modules, and processor details.

Note Upgrade analysis is supported on all Cisco IOS-XR devices (such as Cisco NCS 1000, Cisco NCS 4000, Cisco NCS 5000, Cisco NCS 5500, and Cisco NCS 6000), except on Cisco ASR 9000 devices.

If you want to adjust the device requirements for an image, see Change the Device Requirements for Upgrading a Software Image, on page 10.

Step 1 Choose **Inventory > Device Management > Software Images**.

Step 2 Click **Upgrade Analysis** under **Useful Links**. (Do not select an image from the Software Images page.)

Step 3 In the Upgrade Analysis dialog:

a) Choose the source for the software images (the image repository or Cisco.com).
b) Select the devices you want to analyze.
c) Select the software images you want to analyze the devices against.
d) Click **Run Report**.

The report groups devices by their IP address.

Distribute a New Software Image to Devices

The image distribution operation copies a new software image to a specified location on a device. You can distribute images for similar devices in a single deployment, adjusting your choices per device. When you create the job, you determine whether the job runs immediately or at a scheduled time.

Note Cisco EPN Manager does not support using TFTP to distribute images from a server to devices.

When you select an image to be distributed, Cisco EPN Manager only displays devices that are suitable for the image. When you create the distribution job, you specify whether Cisco EPN Manager should:

- Activate the image in the same job or skip the activation. Delaying the activation lets you perform these tasks before activating the image:
  - Find out if there is insufficient memory, clear the disk space for distributing the image or package.
  - Do an upgrade analysis to check the suitability of the device for the chosen image.
- (Cisco IOS XR only) Commit the image in the same job or skip the commit.

Limitations:

- When you distribute image to Cisco IOS-XR devices (except Cisco ASR 9000 devices), the image is copied to the device storage before the install package is activated and committed. With Cisco ASR 9000 devices, however, the image is install-added on the device directly from Cisco EPN Manager without being copied to the device storage. This will reduce the space consumed by the images on the devices. Use the following command to move the image to inactive state instead of copying the image to the device storage:

`install add protocol://image path/image name`

- For Cisco ASR 9000 devices, only upto 16 device-package pairs can be activated at the same time. Also, the activation of the .tar images must contain the same maximum number of packages.
- During the distribution process, if the protocols used for distribution are not supported by the device, then distribution might fail. For example, if you use the SCP protocol to distribute an image to Cisco ASR 9000 devices, then the distribution fails, because copy of the image onto the device storage is not supported in the device's command line.

The image can be distributed to any file system on the device, including folders in the root directory. This is supported only for NCS 42XX, NCS520 (IOS-XE) and ASR907 devices. If you choose a file system that has a stand by flash, then the image is distributed to both the active flash and the stand by flash. This means that when you choose to distribute the image to active flash, you are not required to re-distribute the image to the stand by flash.

Note The option to distribute an image directly to a device folder is supported only on Cisco ASR907 and Cisco NCS42xx devices.

Cisco EPN Manager displays feedback and status as the operation proceeds. If you are distributing an image to many devices, you can stagger reboots so that service at a site is not completely down during the upgrade window. For image distribution to work efficiently, the device and server from which the distribution is performed must be in the same geographical location or site. The distribution job will return an error if the distribution takes more time due to network slowness or low speed.

Note When distributing an image to a device, use the most secure protocols supported by the device (for example, SCP instead of TFTP). TFTP tends to time out when transferring very large files or when the server and client are geographically distant from each other. If you choose SCP protocol for the image distribution, ensure that the device is managed in Cisco EPN Manager with full user privilege (Privileged EXEC mode); otherwise the distribution will fail due to copy privilege error (SCP: protocol error: Privilege denied).

Before You Begin

- When distributing an image to a device, use the most secure protocols supported by the device (for example, SCP instead of TFTP). TFTP tends to time out when transferring very large files or when the server and client are geographically distant from each other. If you choose SCP protocol for the image distribution, ensure that the device is managed in Cisco EPN Manager with full user privilege (Privileged EXEC mode); otherwise the distribution will fail due to copy privilege error (SCP: protocol error: Privilege denied).
- When distributing images to Cisco ME 1200 devices, you will need to activate the image on the device immediately after distribution. Ensure that the device is ready for an image activation.

Step 1 Choose **Inventory > Device Management > Software Images**.

Step 2 Click the blue **Distribute** icon in the Software Image Management Lifecycle widget. Cisco EPN Manager displays the devices that are appropriate for the images. You can configure the image for each device when you create a distribution job.

Note If the required device is not listed here, ensure that the Image Family associated with the file is same as the selected device's family.

To verify the device family, type, version, size use the **Image** tab in the Device Details page.

Step 3 From the **Image Selection** tab, select the image that you want to distribute on devices.

Note View the Image family, type, version, and size details for the selected image.

Step 4 From the **Device Selection** tab, select the devices for image distribution. You can further adjust the distribution settings for each device.

a) In the **Image Details Verification** tab, Cisco EPN Manager displays one row per device and image.

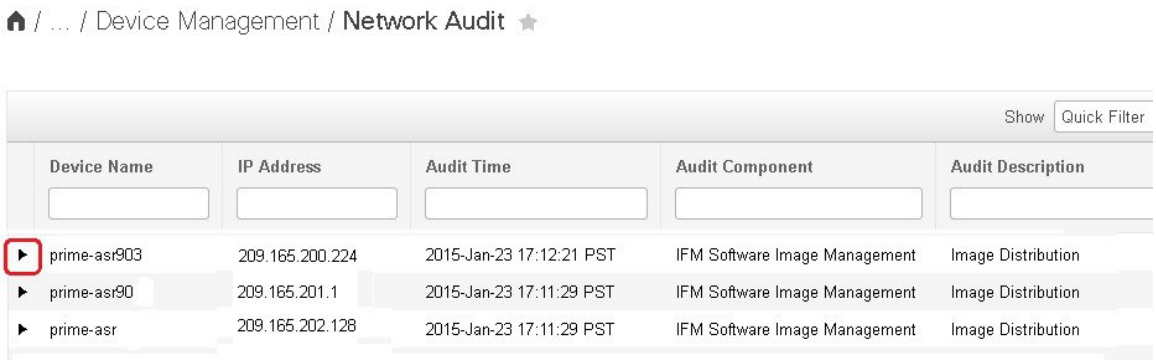
b) For each device, check the location where the image will be copied. Cisco EPN Manager chooses the location based on its memory calculations.

Note Locations are not supplied for the Cisco NCS 2000 and Cisco ONS families of devices.

To change the location, double-click the location value in the **Distribute Image** field and choose another location from the drop-down list.

After you click **Save**, Cisco EPN Manager calculates whether that location has adequate space for the image. If there is enough space, Cisco EPN Manager displays a green check mark (after you click **Save**). Otherwise you must choose another location, or select the **Smart Flash Delete Before Distribution** option in step 5. Note that running images are not deleted from the device.

The following is an example of a network audit event that is generated during image distribution.



Step 5 From the **Image Details Verification** tab, select the file system on the device where the image must be distributed using the **Distribute Location** drop-down menu. This field displays the folders available on the device. To distribute the image to new folders, create the folder on the device manually, and return to this step. Alternatively, you can create a new folder during the distribution process automatically by choosing the 'swim_configuration.xml' file under '/opt/CSCOlumos/swim' and providing any new folder name of your choice. The folder is automatically created under this directory. The **Verification State** field displays the status of the software chosen. Based on the status (Success or Failure) you can decide on the compatiblitiy state of the device chosen. For example, if the state is success then there is enough space to proceed with the distribution of an image.

Step 6 Configure the distribution settings.

In the **Image Deployment** tab area, configure the behavior for the distribution job—for example, in a bulk distribution job, whether to continue the distribution if it fails on a device. (The preferences are populated according to defaults set by the administrator. For more information, see Adjust Image Transfer and Distribution Preferences, on page 3).

Image Deployment Options:

- **Smart Flash Delete Before Distribution** - Delete any file (other than the running image) to recover disk space in case the device has insufficient memory (additional image files are deleted until adequate space is available in the selected flash).
- **Continue distribution on Failure** - Continue the distribution even if it fails on a device.
- **TFTP Fallback** - Reload an image if the distribution fails by inserting the TFTP failback command into the running image.
- **Insert Boot Command** - Insert the boot command into the running image after the image is distributed.
- **ISSU** - Activate In-Service Software Upgrade (ISSU) to update the software on the device with minimal service interruption.
- **Upgrade FPD Image** - Field Programmable Devices (FPDs) are hardware devices implemented on router cards that support separate software upgrades. Select this option to automatically choose FPD image packages for the upgrade during image distribution and activation processes. Additional features include:
  - Smart Flash Delete Before Distribution
  - Parallel Distribution
  - Continue distribution on failure
- **Interface Module Delay** - Adjusts the delay between the Online Insertion and Removal (OIR) of each Interface Module (IM).
- **Erase Running Image** - Erases the device's running image.
- **Distribute via VRF** - Check the Add Distribute via VRF checkbox to distribute images through VRF.
  - VRF Name - Enter an appropriate VPN routing and forwarding (VRF) name to be used during distribution of an image and for the file transfer.

    Note This field is available only when the "Distribute via VRF" checkbox is enabled.

    If multiple devices are selected, only the common VRF Name is displayed in the **VRF Name** field.

Table 1: Support for Image Deployment options

Devices	Smart Flash Delete Before Distribution	Continue distribution on Failure	TFTP Fallback	Insert Boot Command
Cisco IOS (ASR 901)	Y	Y	Y	Y
Cisco IOS-XE (ASR 903/920)	Y	Y	Y	Y
Cisco IOS XE (NCS 4200 / ASR 907)	Y	Y	-	Y
Cisco Nexus	Y	Y	Y	Y
Cisco IOS (ME36X / ME38X)	Y	Y	Y	Y

Devices	Smart Flash Delete Before Distribution	Continue distribution on Failure	TFTP Fallback	Insert Boot Command
Cisco IOS-XR	Y (for Cisco ASR 9000 Devices, the .tar images with version lesser than the running image will be deleted)	Y	-	-
Cisco NCS 2000 and Cisco ONS 15454	-	Y	-	-
Cisco NCS 4000	Y	Y	-	-
Cisco NCS 1000	Y	Y	-	-
Cisco NCS 6000	-	-	-	-

Table 2: Support for Image Deployment options

Devices	ISSU	Upgrade FPD Image	Interface Module Delay	Erase Running Image	Distribute via VRF
Cisco IOS (ASR 901)	-	-	-	-	Y
Cisco IOS-XE (ASR 903/920)	-	-	-	-	Y
Cisco IOS XE (NCS 4200 / ASR 907)	Y (only if device is in 'Install' mode)	-	Y (only if ISSU is available)	-	Y
Cisco Nexus	-	-	-	-	-
Cisco IOS (ME36X / ME38X)	-	-	-	Y	-
Cisco IOS-XR	Y	-	-	-	-
Cisco NCS 2000 and Cisco ONS 15454	-	-	-	-	-
Cisco NCS 4000	Y	Y	-	-	-
Cisco NCS 1000	-	Y	-	-	-
Cisco NCS 6000	-	-	-	-	-

Step 7 In the **Activate Job Options** window, choose the required settings as applicable:

- Activate Options: Sequential or Parallel
- Continue on failure: Continue the distribution even if it fails on a device.
- Commit: Commit the image on the device post distribution.

- FPDs Upgrade: Field Programmable Devices (FPDs) are hardware devices implemented on router cards that support separate software upgrades. If you enable this option, FPD image packages will be used for the upgrade.

Step 8 Configure the image activation settings.

Device OS	Settings
Cisco IOS and Cisco IOS XE	Check **Insert Boot Command** if you want the image to be activated when the device reloads, and: • If you *do* want to reload the device at the end of the operation (and activate the image)—choose **Sequential**, or **Parallel** from the drop-down list. This option is not available for Cisco IOS XE devices. • If you *do not* want to reload the device at the end of the operation—Choose **OFF** from the drop-down list. If you did not check Insert Boot Command but you want to activate the image, choose **Sequential**, or **Parallel**. **Note** If You choose to perform an ISSU upgrade, choose **OFF** from the drop-down list. This option is only applicable to some Cisco IOS XE devices such as Cisco NCS42xx.
Cisco IOS XR , Cisco NCS 2000 and Cisco ONS	• If you *do* want to activate or reload the image, choose either **Sequential**, or **Parallel**. from the drop-down list. • If you *do not* want to activate the image, choose **OFF** from the drop-down list. **Note** If you choose to perform an ISSU upgrade, choose **OFF** from the drop-down list. This option is applicable to all Cisco IOS XR devices. **Note** If you choose **OFF** from the drop-down list, the **Only image downgrade** option is disabled. This option is applicable to all Cisco NCS 2000 devices.

The activation options are sometimes hidden because the ability to activate images during the distribution process has been disabled in the Admin settings. To activate images, please return to **Inventory > Device Management > Software Images** and click the **Activate** icon.

Step 9 (Cisco IOS XR devices) Configure the image commit settings. To commit the image in this job, check **Commit**. If you want to commit the image later, do not check **Commit** and then use the procedure in Commit Cisco IOS XR Images Across Device Reloads, on page 21.

Step 10 In the Schedule Distribution area, schedule the job to run immediately, at a later time, or on a regular basis.

Step 11 Click **Submit**.

Step 12 Choose **Administration > Job Dashboard** to view details about the image distribution job.

Note If the copy task takes longer than two hours, verify your connection speed from Cisco EPN Manager to the selected device.

What to do next

If you encounter the following image distribution error, please configure the device with the commands listed and try again:

Problem: You encounter the error- 'ssh connections not permitted from this terminal'.

Cause: Device is configured incorrectly.

Solution: Configure the device with the following commands

```
line vty 0 <number available in the device>
               transport input ssh
               transport output ssh
```

<number available in the device> -represents the unique identifier that varies from 15 to over 100 depending on the IOS version running on the device.

Note These commands are not supported on Cisco IOS-XR devices.

Activate a New Software Image on Devices

Note To activate Cisco IOS XR images, you can use this procedure or the procedure in Activate, Deactivate, and Remove Cisco IOS XR Images from Devices, on page 20 (which performs the deactivate operation on single devices).

When a new image is activated on a device, it becomes the running image on the disk. Deactivated images are not removed when a new image is activated; you must manually delete the image from the device.

If you want to distribute and activate an image in the same job, see Distribute a New Software Image to Devices, on page 11 .

To activate an image without distributing a new image to a device — for example, when the device has the image you want to activate—use the following procedure. The activation uses the distribution operation but does not distribute a new image.

Before you begin

- Before activating or reverting images on Cisco NCS 2000 devices, ensure that you disable all suppressed alarms on the device.
- If you choose the **ISSU** option to activate an image in Bundle Mode, you can verify if the device is currently in bundle mode by running this command **show version | in image** to check if the image is of the format '.bin'. You can also check the format of the image by looking at the filename of the image in the **Image** tab of the Device Details view.
- During activation using the ISSU option, if the device is in subpackage mode, for example, if the image is of the format ‘bootflash:ISSU/packages.conf”, ensure that you use the same folder to activate the image.

Step 1 Choose **Inventory > Device Management > Software Images**.

Step 2 Click the **Activate** icon in the Software Image Management Lifecycle widget.

Step 3 **Note** You cannot perform the activation operation when the standby version is lower than the active version.

In the **Activation Source** tab, choose **Activate from Library** or **Activate from Completed Distribution Jobs** or **Activate from Standby/Alternate Images** as required .

Step 4 If you choose Activate from Completed Distribution Jobs, go to Job selection tab and select the distributed success or partial success jobs. Then, go to **Activate Preview** tab and select the Device list displayed with image name and flash details. Click the **Activate Job Options** tab.

Step 5 In the **Activate Job Options** window, choose the required settings and go to Step 10:

- Continue on failure: Continue the activation even if it fails on a device.
- Commit: Commit the image on the device post distribution.
- Insert boot command: Inserts the boot command into the running image after the image is distributed. This is a pre-requisite for activating devices with the ISSU option.
- Activate Options: Sequential or Parallel
- Continue on failure: Continue the distribution even if it fails on a device.
- Commit: Commit the image on the device post distribution.
- FPDs Upgrade: Field Programmable Devices (FPDs) are hardware devices implemented on router cards that support separate software upgrades. If you enable this option, FPD image packages will be used for the upgrade.
- ISSU options:
  - Device Upgrade Mode: Your options are:
    - **Bundle Mode**: If you choose the **ISSU** option to activate an image, choose the Bundle Mode to use a monolithic Cisco IOS image to boot. This ensures that the boot variable of the device pointing to a .bin file gets the device running in the Bundle mode. If you choose this option, you must reload the device after activation. To verify if the device is in bundle mode, run this command **show version | in image** to check if the image is of the format '.bin'. You can also check the format of the image by looking at the filename of the image in the **Image** tab of the Device Details view.
    - **Install Mode**: During activation using the ISSU option, use this option if the device is in the subpackage mode, for example, if the image is of the format ‘bootflash:/ISSU/packages.conf’, the device is run in the Install mode. Ensure that you use the same folder to activate the image. Changing the folder location will cause a failure of the activate operation. If you choose the Install Mode for a device which is already running in the Image Mode, the device is activate without reloading (ISSU) and the boot image continues to point to the packages.conf file. In all other scenarios, the devices are reloaded.

      Note Ensure that the current boot variable in the device is 'bootflash:/ISSU/packages.conf' to avoid any duplicate boot variables.

    - **Currently Exists**: If you want the device to be activated in the same mode that it is currently operating in (Install or Bundle), choose this option to activate the image using the same mode.
  - Interface Module Delay: The time (in seconds) specified in this option adjusts the delay between the Online Insertion and Removal (OIR) of each Interface Module (IM). This option is enabled only when the Insert

boot command and the ISSU options are enabled, and when a supported device is selected. It is recommended to set the value of the delay to 1200 seconds or more to ensure sufficient time for the upgrade.

Step 6 If you choose Activate from Library in the Activation Source tab, then click the **Image Selection** tab.

Step 7 If you choose Activate from Standby Image, then go to Step 9.

Step 8 In the **Image Selection** tab, choose the software images that you want to distribute.

Step 9 Click the **Device Selection** tab to choose the devices that you want to activate the image.

a) You can click the **Select devices by** toggle button to choose devices from **Group** or **Device** option.
b) If you choose **Group** option, select the Device groups and choose the devices listed under **Choose Devices** pane. The selected devices are listed under the **Selected Devices** pane.

By default, the devices for which the selected image is applicable are shown. For example, if you choose the **Activate from Standby/Alternate Images** option in Step 3, then the Device Selection tab displays only devices such as, Cisco NCS 2000, Cisco ONS 15454 devices, and Cisco ME1200 devices, which support activation of standby/alternate images.

Step 10 Click the **Activate Image** tab, and verify whether the selected devices and software images are mapped correctly for activation. While using standby images for activation, click the **Verify Image Selection** tab.

Note When you are activating a standby/alternate image, if the version of the standby/alternate image is lower than that of the image running on the device, the Verification Status Message column displays in red that you are downgrading to a lower version.

Step 11 Click the **Activate Job Options** tab, and choose the required Activate Job options.

If you choose the **ISSU** option from the **Activate** drop-down list, the software image in the device will get upgraded without need for rebooting the device.

While activating a standby image, if the selected device supports a downgrade, then the **Only image downgrade** check box is displayed. Selecting this check box ensures that the devices are downgraded only if they support the downgrade operation (for example in case of Cisco NCS 2000 devices) and any specified upgrade operation will fail.

Step 12 Click **Submit** to activate the software image in the selected devices.

See table below for information on Cisco devices and the protocols they support for image distribution:

Table 3: Cisco Devices and Supported Image Distribution Protocols

Cisco Devices	TFTP	FTP	SCP	SFTP	HTTPS
Cisco ASR1000	Yes	Yes	No	Yes	No
Cisco ASR9000	Yes	No	No	Yes	No
Cisco IOS-XR (except Cisco ASR9000 devices)	Yes	Yes	Yes	Yes	No
Cisco NCS42xx, Cisco ASR9XX, or Cisco ASR 1000	Yes	Yes	Yes	No	No
Cisco ME1200	Yes	Yes	No	Yes	No

Cisco NCS2000 and Cisco ONS devices	No	Yes	No	No	Yes

Activate, Deactivate, and Remove Cisco IOS XR Images from Devices

You can perform activate, deactivate, and delete operations on specific devices from the **Chassis View** page. That view lists all the running image on the disk.

Before you begin

Before activating or reverting images on Cisco NCS 2000 devices, ensure that you disable all suppressed alarms on the device.

Step 1 Open the **Chassis View** page and click the **Image** tab.

Step 2 Expand the **Applied Images** area to display all of the images that are installed on the device.

- Active—Images that devices are actively using.
- Inactive—Images that are added to the boot device but are not activated.
- Available—Images that are physically present on the device but have not been added to the boot device.

Step 3 Use the **Show** drop-down list to filter the list of images on the device. Identify the image you want to manage, and double-click its Status field. The field changes to an editable row.

Step 4 Choose the operation you want to perform from the **Status** drop-down list, then click **Save**. . Your options are:

- Active
- Deactivate
- Remove
- Add
- Add and Activate
- Available

Step 5 Click **Apply** above the images table.

Step 6 Choose **Administration** > **Job Dashboard** to view details about the image activation job.

View and Upgrade FPD Images

Field Programmable Devices (FPDs) are hardware devices implemented on router cards that support separate software upgrades. You can configure FPD image packages to be automatically chosen for the upgrade during image distribution and activation processes. Before performing an upgrade, you can view FPD details such as the device name, card type, hardware version, etc.

To do this:

Step 1 Choose **Configuration > Network Devices**.

Step 2 Locate and select the device with the FPD images.

Step 3 Click the **Images** tab.

You can now view the FPD device name, location, available card types and their hardware versions, the ATR values, the status of the image, and the running and programmed values.

Step 4 Once you have reviewed the FPD image details, click the **Upgrade FPD Image** button, to configure the upgrade settings.

Step 5 Schedule the upgrade to run immediately, at a later date and time, or on a regular basis.

Step 6 Click **Submit**.

Commit Cisco IOS XR Images Across Device Reloads

Note For Cisco IOS XR devices, we recommend that you do not commit the package change until the device runs with its configuration for a period of time, until you are sure the change is appropriate.

When you commit a Cisco IOS XR package to a device, it persists the package configuration across device reloads. The commit operation also creates a rollback point on the device which can be used for roll back operations.

If you want to distribute, activate, and commit an image in the same job, use the procedure described in Distribute a New Software Image to Devices, on page 11 .

To commit an activated image, use the following procedure.

Note If you are only working on a single device, perform the commit operation from the Device Details page (click the **Image** tab, choose the image, and click **Commit**).

Step 1 Choose **Inventory > Device Management > Software Images**.

Step 2 Click the **Commit** icon in the Software Image Management Lifecycle widget.

Step 3 Select the devices with the image you want to commit and click **Submit**. (Images can only be committed if they have been activated.)

Step 4 Select the software image you want to activate, then click **Submit**.

Step 5 In the Schedule Distribution area, schedule the commit job to run immediately, at a later time, or on a regular basis.

Step 6 Click **Submit**.

Step 7 Choose **Administration > Job Dashboard** to view details about the image activation job.

Roll Back Cisco IOS XR Images

Rolling back a Cisco IOS XR image reverts the device image to a previous installation state—specifically, to an installation rollback point. If an image has been removed from a device, all rollback points associated with the package are also removed and it is no longer possible to roll back to that point.

A rollback job can only be performed on one device at a time. You cannot perform a rollback for multiple devices in the same job.

Note The rollback feature is only supported on Cisco IOS-XR devices such as Cisco ASR 9000 devices.

Step 1 Choose **Inventory** > **Device Management** > **Network Devices**, then click the device name hyperlink for the device with the image you want to roll back.

Step 2 Click the **Image** tab and expand the Rollback Info area.

Step 3 Select the software image Commit ID you want to roll back to, and click **Rollback**. The Rollback Scheduler opens.

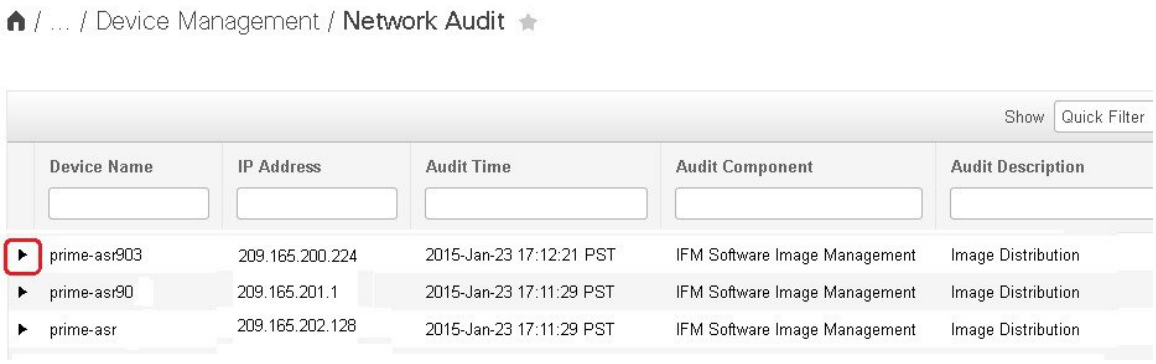
Step 4 If you want to commit the image after the rollback operation completes, check **Commit After Rollback**.

Step 5 In the Schedule Rollback area, schedule the rollback job to run immediately or at a later time, and click **Submit**.

Check the Network Audit for Software Image Operations

To get historical information about device software image changes, check the Network Audit. For more information on the Network Audit feature, see .

Step 1 Choose **Inventory** > **Device Management** > **Network Audit**. To filter the results to show only image management operations, enter **software image** in the Audit Component field.



Step 2 Expand an event drawer to get details about a device change. For example, if you expand the drawer highlighted in the above figure, you can see that the image listed in the job was successfully distributed to the device.

Device/Module ID	544544
Distribution Option : ActivatePatches	Yes
Distribution Option : BackUpCurrentImageFetch	No
Distribution Option : CfgXferProtocolOrder	TELNET, SSH
Distribution Option : Commit	No
Distribution Option : DeviceUpgradeMode	currentlyExists
Distribution Option : HaltUponError	No
Distribution Option : ISSUUpgrade	No
Distribution Option : ImgXferProtocolOrder	SCP,SFTP,FTP,TFTP
Distribution Option : InsertBootCommand	No
Distribution Option : JobDirectory	/opt/CSCOlumos/conf/ifm/swim/jobs
Distribution Option : RebootImmediately	No
Distribution Option : RebootMode	Sequential
Distribution Option : SCPDirectory	/localdisk/sftp
Distribution Option : SkipDistribution	No
Distribution Option : TftpDirectory	/localdisk/sftp
Distribution Option : TftpFallback	No
Distribution Option : UpgradeMode	Sequential
Distribution Option : UseSSH	Yes
Operation	Starting distribution of image to device
Running Image File Name	asr903rsp1-universalk9_npe.03.13.00.S.154-3.S-ext.bin
Running Image File Name	asr903rsp1-universalk9_npe.03.13.00.S.154-3.S-ext.bin

Delete Software Image Files from the Image Repository

Software images can only be *manually* deleted from the image repository; Cisco EPN Manager does not perform any automatic purging of the image repository. If you have sufficient privileges, you can use the following procedure to delete software image files from the image repository.

Step 1 Choose **Inventory** > **Device Management** > **Software Images**.

Step 2 From the **Software Images Summary** panel on the left, select the images that you want to delete.

Step 3 Click **Delete**.