



Cisco Manage Software Images User Guide

[Home](#) » [Cisco](#) » Cisco Manage Software Images User Guide 

Contents

- 1 [Cisco Manage Software Images](#)
- 2 [Product Usage Instructions](#)
- 3 [About Image Repository](#)
- 4 [Integrity Verification of Software Images](#)
- 5 [View Software Images](#)
- 6 [Use a Recommended Software Image](#)
- 7 [Import a Software Image](#)
- 8 [Assign a Software Image to a Device Family](#)
- 9 [Upload Software Images for Devices in Install Mode](#)
- 10 [About Golden Software Images](#)
- 11 [Specify a Golden Software Image](#)
- 12 [Configure an Image Distribution Server](#)
- 13 [Change the Protocol Order of an Image Distribution Server](#)
- 14 [Add Image Distribution Servers to Sites](#)
- 15 [Provision a Software Image](#)
- 16 [Upgrade a Software Image with ISSU](#)
- 17 [List of Device Upgrade Readiness Prechecks](#)
- 18 [View Image Update Status](#)
- 19 [View Image Update Workflow](#)
- 20 [Auto Flash Cleanup](#)
- 21 [Documents / Resources](#)
 - 21.1 [References](#)
- 22 [Related Posts](#)





Product Information

Specifications

- Product Name: Cisco DNA Center
- Function: Manage Software Images, Integrity Verification of Software Images
- Supported Devices: IE3x00 series, IE9x00 series switches
- Primary Boot Option: Internal bootflash

Product Usage Instructions

Manage Software Images

Cisco DNA Center stores all software images, software maintenance updates (SMUs), subpackages, ROMMON images, etc., for devices in your network.

About Image Repository

Image Repository in Cisco DNA Center provides functions to manage software images and integrity verification of software images.

Integrity Verification of Software Images

The Integrity Verification application ensures that stored software images are not compromised by monitoring for unexpected changes or invalid values.

View Software Images

1. Click the menu icon and choose Design > Image Repository.
2. The Image Repository window displays details about device families, software images, and advisories.
3. Filter device families by clicking on the respective category or using the search/filter icon.
4. Click Sync Updates to synchronize image information from cisco.com for managed devices.
5. View progress in Show Tasks and update image information once the task is successful.

FAQ

- **Q: How can I ensure the integrity of software images?**

A: The Integrity Verification application compares checksum values during the import process to verify image integrity.

- **Q: What should I do if the Integrity Verification application cannot verify a software image?**

A: Refer to the Cisco DNA Center Administrator Guide for information on importing Known Good Values (KGV) files.

Manage Software Images

About Image Repository

Cisco DNA Center stores all the software images, software maintenance updates (SMUs), subpackages, ROMMON images, and so on, for the devices in your network. Image Repository provides the following functions:

- **Image Repository:** Cisco DNA Center stores all the unique software images according to image type and version. You can view, import, and delete software images.
- **Provision:** You can push software images to the devices in your network.

Before using Image Repository features, you must enable Transport Layer Security protocol (TLS) on older devices such as Cisco Catalyst 3000, 4000, and 6000. After any system upgrades, you must re-enable TLS. For more information, see “Configure Security for Cisco DNA Center” in the Cisco DNA Center Administrator Guide.

Note

In Release 2.3.3 and later, Cisco DNA Center supports only internal bootflash as the primary boot option for Software Image Management (SWIM) and Software Maintenance Updates (SMUs) on the IE3x00 series, and IE9x00 series switches.

If you have an earlier release of Cisco DNA Center (before Release 2.3.3), and if an IE3x00, or IE9x00 device in your network is already booted with a Secure Digital (SD) flash memory module, then ensure that you set the internal bootflash as the primary boot option on the device, using the `boot flash-primary` command.

To save and synchronize a running configuration from SD flash to bootflash, use the `sync` command.


Integrity Verification of Software Images

The Integrity Verification application monitors software images that are stored in Cisco DNA Center for unexpected changes or invalid values that could indicate your devices are compromised. During the import process, the system determines image integrity by comparing the software and hardware platform checksum value of the image that you are importing to the checksum value identified for the platform in the Known Good Values (KGV) file to ensure that the two values match.

On the Image Repository window, a message displays if the Integrity Verification application cannot verify the selected software image using the current KGV file. For more information about the Integrity Verification application and importing KGV files, see the Cisco DNA Center Administrator Guide.

View Software Images

After you run Discovery or manually add devices, Cisco DNA Center automatically stores information about the software images, SMUs, and subpackages for the devices.

1. **Step 1** Click the menu icon () and choose Design > Image Repository.

The Image Repository window summarizes the details about device families, software images, and advisories.

- **SUMMARY:** Shows the number of device families, devices, and device families without golden images in image repository.
- **TOTAL IMAGES:** Shows the number of running images, imported images, and golden images in image repository.
- **ADVISORIES:** Shows the number of critical and high advisories. The Image Families table shows the

details of Family Name, Devices, Images, Advisories, and Images Marked Golden for each device family.

Note When cisco.com credentials are not set, a warning alert is displayed.

2. **Step 2** Click Routers, Switches, Wireless Controllers, Security and VPN, Sensors, or Virtual Devices in the top of the window or click the search or filter icon in the Image Families table to filter device families.

By default, the Image Repository window shows all the device families.

3. **Step 3** Click Sync Updates and then click OK in the subsequent warning message to synchronize image information from cisco.com for all managed devices in Cisco DNA Center.
 - If cisco.com credentials are not set, you are prompted to specify them.
 - You can view the progress of task in Show Tasks. Once the task is successful, the image information is updated for all device families.
 - Note You can fetch image information only once in an hour.
4. **Step 4** Click Show Tasks to view status of all the tasks that are related to software images.

The Recent Tasks slide-in pane shows status of the last 50 tasks. From the Task Status drop-down list, choose All, Failed, In-Progress, or Successful to filter the tasks based on status.
5. **Step 5** Click Import Image to import a software image or software image update. For more information,
6. **Step 6** Click Update Devices to update a device in inventory.

In the Inventory window, choose a device and go to Actions > Inventory to edit, resync, reboot, or delete a device in inventory.
7. **Step 7** In the Image Families table, click Imported Images to view the details about imported software images.

The Imported Images row is always displayed as the first row in the table.

In the Imported Image Family window, the Images table shows Image Name, Version, Device Series Assigned, and Action for all the imported software images.

In the Action column, click Assign to assign a software image to a device family. For more information,
8. **Step 8** In the Image Families table, click the name of a device family to view all the software images associated with the particular device family.

In the Image Family window, the Images table shows the Image Name, Version, Devices, Advisories, Golden Image, Device Roles & Tags for all the software images.

In the Image Family window, do the following:

 - In the left pane, click Roles & Tags, Major Versions, or Golden Images or click the search or filter icon in the Images table to filter the software images.
 - In the Version column, click the Add On link to view the applicable SMUs, Subpackages, ROMMON, APSP, and APDP upgrades for the base image.

Subpackages are the additional features that can be added to the existing base image. The subpackage version that matches the image family and the base image version is displayed here.

AP Service Pack (APSP) and AP Device Pack (APDP) are images for upgrading APs associated with wireless controllers.
 - When a new AP hardware model is introduced, APDP is used to connect to the existing wireless network.
 - For associated APs, critical AP bug fixes are applied through APSP.

Note If you tag any SMU as golden, it is automatically activated when the base image is installed.

 - You cannot tag a subpackage as golden.
 - For ROMMON upgrades, the cisco.com configuration is mandatory. When a device is added, the latest ROMMON details are retrieved from cisco.com for applicable devices. Also, when the base image is imported or tagged, the ROMMON image is automatically downloaded from cisco.com.

- In the Device(s) column, click the number of devices to view the devices that are using the image.
In the Advisory column, click the number of critical or high advisories to view the advisories for a specific software image.
The Image Advisory slide-in pane shows Family Name, Version, and Advisories of the software image.
The advisories are classified as Critical, High, Medium, Low, and Informational.
Click CRITICAL, HIGH, or MEDIUM to view the advisories specific to each category.

To fix the advisories, do the following:

1. Click Fix Advisories.

The Image Update window appears.

2. Select a recommended software image to update the device.

If the recommended software image is not available in the image repository, you can download it from cisco.com.

3. Click Download and Mark Golden.

From the Download Image dialog box, do one of the following:

- Keep the Mark the image as golden after download check box checked (the default). Then, click Download. The software image is downloaded and marked as golden.
- Uncheck the Mark the image as golden after download check box and click Download. The software image is downloaded to the repository but is not marked as golden.

4. Click OK.

The software image is downloaded. You can view the progress in Show Tasks.

- In the Golden Image column, click the star icon to specify the software image as golden.
If the software image that you specify as golden is not already uploaded into the Cisco DNA Center repository, click the download icon to import the software image.
For more information about golden images, see About Golden Software Images, on page 7 and Specify a Golden Software Image, on page 8.

In the Device Roles & Tags column, do the following:

1. Click the edit icon to assign a device role or tag.

To assign a device role and/or tag, the corresponding software image must have been imported.

2. In the Assign Device Roles & Tags slide-in pane, select the device roles and tags for which you want to indicate that this is a golden software image.



- **Note** Device tags take precedence over device roles when both are selected for a software image.
- You can create and assign new device tags in Provision > Network Devices > Inventory.

3. Click Save.

Use a Recommended Software Image

Cisco DNA Center displays and allows you to select Cisco-recommended software images for the devices that it manages.

Note Only the latest Cisco-recommended software images are available for download.

- **Step 1** Click the menu icon () and choose System > Settings > [Cisco.com](https://cisco.com) Credentials.
- **Step 2** Verify that you have entered the correct credentials to connect to cisco.com.
- **Step 3** Click the menu icon () and choose Design > Image Repository.
Cisco DNA Center displays the Cisco-recommended software images according to device type.
- **Step 4** Designate the recommended image as golden. See Specify a Golden Software Image, on page 8 for more information.
- **Step 5** Push the recommended software image to the devices in your network. See Provision a Software Image, on page 11 for more information.

Import a Software Image

You can import software images and software image updates from your local computer or from a URL. Imported images are categorized based on different supervisors that are present in a specific device family. Categorization under different supervisors supports only the Cisco Catalyst 9400 series family. If you use FTP to import an image from an FTP server, use the FTP standard:
ftp://username:password@ip_or_hostname/path

1. **Step 1** Click the menu icon () and choose Design > Image Repository.
2. **Step 2** Click Import Image.
3. **Step 3** In the Import Image/Add-on slide-in pane, click the Select from computer radio button and click Choose a file to navigate to a software image or software image update stored locally.
Alternately, click the Enter URL radio button and enter the image URL in the Enter Image URL field to specify an HTTP or FTP source from which you want to import the software image or software image updates. **Note** Software images are compliant with Federal Information Processing Standard (FIPS). If FIPS mode is enabled in Cisco DNA Center, you cannot import images from URL. Import images from your computer or cisco.com.
4. **Step 4** If the image you are importing is for a third-party (non-Cisco) vendor, select Third party under Source. Choose an Application Type, describe the device Family, and identify the Vendor.
5. **Step 5** Click Import.
A window displays the progress of the import.
Click Show Tasks to verify that the image was imported successfully.
6. **Step 6** If you imported a SMU, Cisco DNA Center automatically applies the SMU to the correct software image, and an Add-On link appears below the corresponding software image.
Click the Add-On link to view the SMU.
7. **Step 7** In the Device Role field, select the role for which you want to mark this SMU as golden.
8. **Step 8** You can only mark a SMU as golden if you previously marked the corresponding software image as golden.

Note Cisco DNA Center does not allow you to import software images for the FTD devices that are managed by FMC. When you add FMC to inventory and it goes to the Managed state, the software images present in FMC are shown in Image Repository and are categorized based on device family.


Assign a Software Image to a Device Family

After importing a software image, you can assign or unassign it to available device families. The imported image

can be assigned to multiple devices at any time.

To assign an imported software image to a device family:



1. **Step 1** Click the menu icon () and choose Design > Image Repository.
2. **Step 2** Click Imported Images.
3. **Step 3** Click Assign in the corresponding image name row.
4. **Step 4** In the Assign Device Family window, choose the Device Series from [Cisco.com](https://www.cisco.com) or All Device Series and click Assign link to which you want to map the image.

Note: If [cisco.com](https://www.cisco.com) credentials are not set, specify the credentials in System > Settings > [Cisco.com](https://www.cisco.com) Credentials.

5. **Step 5** Select appropriate site from the Global hierarchy and click Assign and then click Save.
6. **Step 6** To unassign an image, choose a site from the Global hierarchy and click Unassign link in the Action column.
 - The software image is assigned to the device family and the number of devices using that image are shown in the Device(s) column. After assigning the image, you can mark it as a golden image. See Specify a Golden Software Image.
 - If the device family is marked as a golden image, you cannot delete that image from the device family.


Note For PnP devices, you can import a software image and assign it to a device family even before the device is available. You can also mark the image as a golden image. When the device is made available in the inventory, the image that is assigned to the device family is automatically assigned to the newly added devices of that device family.

When the image is imported and Cisco DNA Center has [cisco.com](https://www.cisco.com) credentials added, Cisco DNA Center provides the list of device families that are applicable for the image. You can select the required device family from the list. When the image is not available in [cisco.com](https://www.cisco.com) or when credentials are not added in Cisco DNA Center, you must design the right device family for the image.

Upload Software Images for Devices in Install Mode

The Image Repository page might show a software image as being in Install Mode. When a device is in Install Mode, Cisco DNA Center is unable to upload its software image directly from the device. When a device is in Install Mode, you must first manually upload the software image to the Cisco DNA Center repository before marking the image as golden, as shown in the following steps.



1. **Step 1** Click the menu icon () and choose Design > Image Repository.
2. **Step 2** In the Image Name column, find the software image of the device that is running in Install Mode.
3. **Step 3** Click Import to upload the binary software image file for the image that is in Install Mode.
4. **Step 4** Click Choose File to navigate to a software image stored locally or Enter image URL to specify an HTTP or FTP source from which to import the software image.
5. **Step 5** Click Import.
 - A window displays the progress of the import.
6. **Step 6** Click Show Tasks and verify that the software image you imported is green, indicating it has been successfully imported and added to the Cisco DNA Center repository.
7. **Step 7** Click Refresh.

- The Image Repository window refreshes. Cisco DNA Center displays the software image, and the Golden Image and Device Role columns are no longer dimmed.

About Golden Software Images

Cisco DNA Center allows you to designate software images and SMUs as golden. A golden software image or SMU is a validated image that meets the compliance requirements for the particular device type. Designating a software image or SMU as golden saves you time by eliminating the need to make repetitive configuration changes and ensures consistency across your devices.

You can designate an image and a corresponding SMU as golden to create a standardized image. You can also specify a golden image for a specific device role. For example, if you have an image for the Cisco 4431 Integrated Service Routers device family, you can further specify a golden image for those Cisco 4431 devices that have the Access role only.

Specify a Golden Software Image

You can specify a golden software image for a device family or for a particular device role. The device role is used for identifying and grouping devices according to their responsibilities and placement within the network.

- Step 1** Click the menu icon () and choose Design > Image Repository.
 - The software images are displayed according to device type.
- Step 2** From the Family column, select a device family for which you want to specify a golden image.
- Step 3** From the Image Name column, select the software image that you want to specify as golden.
- Step 4** If the software image that you specify as golden is already uploaded into the Cisco DNA Center repository, click the star icon in the Golden Image column.
 - The software image is marked as golden.
- Step 5** If the software image that you specify as golden is not already uploaded into the Cisco DNA Center repository, click the download icon in the Golden Image column.
 - This process might take some time.

Note Importing software images from devices is not allowed.
- Step 6** From the Download Image dialog box, do one of the following:
 - Keep the Mark the image as golden after download check box checked by default and click Download. The software image is downloaded and marked as golden.

Note If [Cisco.com](https://www.cisco.com) credentials are not set, you are prompted to specify them.



The in-progress software image download is shown in the Device Role column.

If the software image is downloaded and successfully marked as golden, the color of the star icon turns gold. If the software image download fails, the color of the star icon turns red and a Please Retry status is displayed.
 - Uncheck the Mark the image as golden after download check box and click Download. The software image is downloaded to the repository but is not marked as golden.
- Step 7** In the Device Role column, select a device role for which you want to specify a golden software image. Even if you have devices from the same device family, you can specify a different golden software image for each device role. Note that you can select a device role for physical images only, not virtual images.

Configure an Image Distribution Server


An image distribution server helps in the storage and distribution of software images. You can configure up to three external image distribution servers to distribute software images. You can also set up one or more protocols for the newly added image distribution servers.

For information about the supported servers, see the Server Requirements for Automation Data Backup section in the “Backup Server Requirements” topic in the Cisco DNA Center Administrator Guide.

1. **Step 1** Click the menu icon () and choose System > Settings > Device Settings > Image Distribution Servers.
2. **Step 2** In the Image Distribution Servers window, click Servers.
 - The table displays details about the host, username, SFTP, SCP, and connectivity of image distribution servers.
3. **Step 3** Click Add to add a new image distribution server.
 - The Add a New Image Distribution Server slide-in pane is displayed.
4. **Step 4** Configure the following image distribution server settings:
 - Host: Enter the hostname or IP address of the image distribution server.
 - Root Location: Enter the working root directory for file transfers.
Note For Cisco AireOS Wireless Controllers, image distribution fails if the configured path is longer than 16 characters.
 - Username: Enter a username to log in to the image distribution server. The username must have read/write privileges in the working root directory of the server.
 - Password: Enter a password to log in to the image distribution server.
 - Port Number: Enter the port number on which the image distribution server is running.
5. **Step 5** Click Save.
6. **Step 6** Because some legacy wireless controller software versions support only weak ciphers (such as SHA1-based ciphers) for SFTP, Cisco DNA Center should enable SFTP compatibility mode for SFTP connections from wireless controllers for software image management and wireless assurance. You can temporarily enable support for weak ciphers on the Cisco DNA Center SFTP server for up to 90 days. To allow weak ciphers:
 - Hover over the  icon next to the IP address of the SFTP server and click Click here.
 - In the Compatibility Mode slide-in pane, check the Compatibility Mode check box and enter a duration (from 1 minute to 90 days).
 - Click Save.
7. **Step 7** (Optional) To edit the settings, click the Edit icon next to the corresponding image distribution server, make the required changes, and click Save.
8. **Step 8** (Optional) To delete an image distribution server, click the Delete icon next to the corresponding image distribution server and click Delete.

Change the Protocol Order of an Image Distribution Server

You can change the protocol order of an image distribution server. Protocol order helps in performing verification checks on the image distribution servers. By default, the software images are distributed using the first protocol in the protocol order.

1. **Step 1** Click the menu icon () and choose System > Settings > Device Settings > Image Distribution Servers.
2. **Step 2** In the Image Distribution Servers window, click Preferences.

- The default protocol order is shown.

3. **Step 3** Click the On/Off toggle button to enable or disable a protocol.

Note The HTTPS or SCP protocol must be enabled for image distribution. The SFTP protocol must be enabled for all protocol orders.

If the HTTPS protocol is disabled or image distribution has failed while using the HTTPS protocol, the software image will be distributed using the SCP protocol.

4. **Step 4** Drag and drop the protocols to change the protocol order.


5. **Step 5** Click Save.

Add Image Distribution Servers to Sites

You can associate SFTP servers located in different geographical regions to sites, buildings, and floors. All the devices under the network hierarchy use the associated image distribution server during a network upgrade.

Before you begin

You must configure an image distribution server. See [Configure an Image Distribution Server](#),

1. **Step 1** Click the menu icon () and choose Design > Network Settings.
2. **Step 2** In the left pane, choose the desired site to which you want to associate the image distribution server. **Step 2**
3. **Step 3** Click Add Servers.
4. **Step 4** In the Add Servers window, check the Image Distribution check box.
5. **Step 5** Click OK.
6. **Step 6** Click the Primary drop-down list and choose the image distribution server that you want to configure as primary.
7. **Step 7** Click the Secondary drop-down list and choose the image distribution server that you want to configure as secondary.
8. **Step 8** Click Save.

Provision a Software Image

Cisco DNA Center compares each device software image with the image that you have designated as golden for that specific device type. If there is a difference between the software image and the golden image, Cisco DNA Center specifies that the software image of the device is outdated. If this is the case, you can update the outdated software image.

Before pushing a software image to a device, Cisco DNA Center performs upgrade readiness prechecks on the devices, such as checking the device management status, disk space, and so on. If any prechecks fail, you cannot perform the software image upgrade. You need to correct any issues before you can upgrade the software image on the devices.

If all the prechecks succeed, you can distribute (copy) the new image to the device and activate it (that is, make the new image the running image). The activation of the new image requires a reboot of the device. Because a reboot might interrupt the current network activity, you can schedule the process for a later time.

After the software image is successfully upgraded, Cisco DNA Center performs upgrade postchecks, such as checking the CPU usage, route summary, and so on, to ensure that the state of the network remains unchanged.

Before you begin

- Make sure the device type has a designated golden image.

- If you need to update (distribute and activate) the software image immediately and the SWIM Events for ITSM (ServiceNow) bundle is enabled, you need to disable the bundle and its integration workflow (image update schedule approval in ServiceNow). To access the bundle, choose Platform > Manage > Bundles > SWIM Events for ITSM (ServiceNow). Click the Disable button in the SWIM Events for ITSM (ServiceNow) window. Wait a few seconds before proceeding to update the image, because the process to disable the bundle and workflow takes a few seconds.

1. **Step 1** Click the menu icon () and choose Provision > Network Devices > Inventory.

2. **Step 2** From the Focus drop-down list, choose Software Images. Select the device whose image you want to upgrade.

Note If the prechecks succeed for a device, the Outdated link in the Software Image column has a green check mark. If any of the upgrade readiness prechecks fail for a device, the Outdated link has a red check mark, and you cannot update the

software image for that device. Click the Outdated link and correct the errors before proceeding. See List of Device Upgrade Readiness Prechecks.

3. **Step 3** From the Actions drop-down list, choose Software Images > Update Image. The Image Upgrade window opens.

4. **Step 4** In the Analyze Selection step, do the following:

- Hover your mouse over the Info icon to view the validation criteria and the CLI commands that are used for validation.
- Click the toggle button to uncheck the validators that you do not want to run for the current workflow.
- Click Next.

5. **Step 5** In the Distribute step, choose whether you want to start the distribution now or schedule it for later.

Note If you associated the external image distribution server with a network hierarchy, the image distribution server distributes the image to all devices under the network hierarchy.

6. **Step 6** (Optional) To add new custom prechecks and postchecks, click the add a new check link, and in the Add a New

Custom Check window, do the following:

- Enter the Name for the custom check.
- In the When drop-down list, choose pre, post, or both.
- In the Select a Test Device drop-down list, choose the device you want to check.
- Click Open Command Runner and enter the CLI commands.
- Expand the Additional Criteria area.
- In the Operation drop-down list, choose Distribution.
- In the Device Series drop-down list, choose the series of the device you want to check.

7. **Step 7** Click Save.

8. **Step 8** Click Next.

In the Activate step, choose whether you want to start the activation now or schedule it for later.

9. **Step 9** Check the Initiate Flash Cleanup after Activation check box to remove all the previous software images saved on the device.

Note Cisco DNA Center stores only the running software image and removes all the previous software images saved on the device.

10. **Step 10** To choose the validators you want to run for the current workflow, do the following:

- Hover your mouse over the Info icon to view the validation criteria and the CLI commands that are used

for validation.

- Click the toggle button to uncheck the validators that you do not want to run for the current workflow.

11. **Step 11** (Optional) To add new custom prechecks and postchecks, click the add a new check link, and in the Add a New Custom Check window, do the following:

- Enter the Name for the custom check.
- In the When drop-down list, choose pre, post, or both.
- In the Select a Test Device drop-down list, choose the device you want to check.
- Click Open Command Runner and enter the CLI commands.
- Expand the Additional Criteria area.
- In the Operation drop-down list, choose Activation.
- In the Device Series drop-down list, choose the series of the device you want to check.
- Click Save.

12. Click Next.


13. **Step 13** In the Summary window, review the configuration settings. To make any changes, click Edit.

14. **Step 14** To proceed, click Submit.

(Optional) To check the status of the update, from the Actions drop-down list, choose Software Images > Image Update Status.

Import the ISSU Compatibility Matrix

In-Service Software Upgrade (ISSU) is a process that upgrades an image on a device with no or minimal service interruption. ISSU is supported only within or between long-lived releases, such as 17.3.x to 17.3.y or 17.3.x to 17.6.y. For an example of the Cisco IOS XE ISSU compatibility matrix for Catalyst Switches, see <https://software.cisco.com/download/home/286315874/type/286326638/release/17.6.2>. You can download and import the ISSU compatibility matrix that corresponds to the target release in Cisco DNA Center to upgrade devices with ISSU.

1. **Step 1** Click the menu icon () and choose Design > Image Repository.
2. **Step 2** Click Import Images.
3. **Step 3** In the Import Image/Add-on slide-in pane, click the Select ISSU compatibility matrix radio button and click Choose a file to navigate to an ISSU compatibility matrix file stored locally.
4. **Step 4** Click Import.
5. **Step 5** Click Show Tasks to view the ISSU compatibility matrix file import status.


Upgrade a Software Image with ISSU

Upgrading devices using the In-Service Software Upgrade (ISSU) eliminates the need to reboot and reduces service interruption.

Before you begin

- Before you upgrade a device using the ISSU, you must import the ISSU compatibility matrix file.
- If you need to update the image immediately, the bundle and its integration workflow (image update schedule approval in ServiceNow) must first be disabled. To access the bundle, choose Platform > Manage > Bundles > SWIM Events for ITSM (ServiceNow). Click the Disable button in the SWIM Events for ITSM (ServiceNow) window. Wait several seconds before updating the image, because the process to disable the bundle and

workflow takes several seconds.

1. **Step 1** Click the menu icon () and choose Provision > Network Devices > Inventory.
2. **Step 2** From the Focus drop-down list, choose Software Images and choose the device whose image you want to upgrade.
3. **Step 3** From the Actions drop-down list, choose Software Images > Update Image.
The Image Upgrade window appears.
4. **Step 4** In the Analyze Selection window, enable the ISSU upgrade:
 - Choose the device that you want to upgrade with ISSU.
 - **Note** The To Image column shows the ISSU validation status.
 - ISSU shown in amber: ISSU validation failed because the selected image is not ISSU compatible.
 - ISSU shown in gray: ISSU validation succeeded and the device supports ISSU.
 - From the ISSU drop-down list, choose Enable ISSU Upgrade.
 - Click Next.
5. **Step 5** From the Distribute window, choose whether you want to start the image distribution Now or schedule it for later.

To choose the validators you want to run for the current workflow and add new custom checks, do the following:

- Hover your cursor over the Info icon to view the validation criteria and the CLI commands that are used for validation.
- Click the toggle button to uncheck the validators that you do not want to run for the current workflow.
- (Optional) To add new custom prechecks and postchecks, do the following:
 - Click add a new check to launch the Add a New Custom Check window.
 - the Name for the custom check.
 - Click the When drop-down list and choose pre, post, or both.
 - From the Select a Test Device drop-down list, choose a device for which you want to run the custom checks.
 - Click Open Command Runner and enter the CLI commands.
 - Expand the Additional Criteria area.
 - Click the Operation drop-down arrow and choose Distribution.
 - Click the Device Series drop-down arrow and choose the device series for which you want to run the custom checks.
 - Click Save.
- If you want to edit a custom check, click the corresponding More icon, choose Edit, make the required changes, and click Save.
- If you want to delete a custom check, click the corresponding More icon, choose Delete, and in the Confirm Delete message, click Delete.

NotIf associated with a network hierarchy, the external image distribution server distributes the image to all devices in the network hierarchy.

If the SWIM Events for ITSM (ServiceNow) bundle is enabled, you need to update the image (distribute and activate) at a later time.

6. **Step 6** Click Next.
7. **Step 7** In the Activate window, choose whether you want to start the activation Now or schedule it for later.
8. **Step 8** Check the Initiate Flash Cleanup after Activation check box to remove all the previous software images

saved on the device.

Note Cisco DNA Center stores only the running software image and removes all the previous software images saved on the device.

To choose the validators you want to run for the current workflow and add new custom checks, do the following:

- Hover your cursor over the Info icon to view the validation criteria and the CLI commands that are used for validation.
- Click the toggle button to uncheck the validators that you do not want to run for the current workflow.
- (Optional) To add new custom prechecks and postchecks, do the following:
- Click add a new check link to launch the Add a New Custom Check window.
- Enter the Name for the custom check.
- Click the When drop-down list and choose pre, post, or both as required.
- Click Select a Test Device drop-down list and choose a device for which you want to run these custom checks.
- Click Open Command Runner and enter the CLI commands.
- Expand the Additional Criteria area.
- Click the Operation drop-down list and choose Activation.
- Click the Device Series drop-down list and choose the device series for which you want to run these custom checks.
- Click Save.
- If you want to edit a custom check, click the corresponding More icon, choose Edit, make the required changes, and click Save.
- If you want to delete a custom check, click the corresponding More icon, choose Delete, and click Delete in the Confirm Delete message.

9. **Step 9** Click Next.

10. **Step 10** In the Summary window, review the configuration settings. (To make any changes, click Edit.)


11. **Step 11** From the Actions drop-down list, choose Software Images > Image Update Status and check the status of the update.

List of Device Upgrade Readiness Prechecks

Precheck	Description
File transfer check	Checks if the device is reachable through HTTPS and SCP. The default order of protocols is HTTPS first and then SCP.
NTP clock check	Compares device time and Cisco DNA Center time to ensure successful Cisco DNA Center certificate installation.
Flash check	Verifies if there is enough disk space for the update. If there is not enough disk space, a warning or error message is returned. For information about the supported devices for Auto Flash cleanup and how files are deleted, see Auto Flash Cleanup .
Config register check	Verifies the config registry value.
Crypto RSA check	Checks whether an RSA certificate is installed.
Crypto TLS check	Checks whether the device supports TLS 1.2.
IP Domain name check	Checks whether the domain name is configured.

Precheck	Description
Startup config check	Checks whether the startup configuration exists for the device.
NFVIS Flash check	Checks whether the golden image is ready to be upgraded in the NFVIS device.
Service Entitlement check	Checks whether the device has a valid license.


View Image Update Status

- Step 1** Click the menu icon () and choose Provision > Network Devices > Inventory.
- Step 2** From the Focus drop-down list, choose Software Images.
- Step 3** From the Actions drop-down list, choose Software Images > Image Update Status.
By default, the Image Update Status window shows all the image update tasks.
- Step 4** To filter the tasks based on the update status, click In Progress, Success, or Failure.
- Step 5** In the left pane, click Task Names or Image Versions to filter the tasks based on operations or image versions.
The Status column shows the current status of the tasks. For in-progress tasks, a progress bar shows the progress of the image update.
- Step 6** Click the device name to view detailed information about a task. For more information,
- Step 7** Click Upcoming Tasks to view the tasks that are scheduled for a later time.
The Upcoming Tasks slide-in pane appears.
- Step 8** Click the number of devices in the Devices Scheduled column to view the devices for which the image update task is scheduled.
- Step 9** Select the devices for which tasks failed by checking check boxes and click Retry to retry the image

update.

The Image Upgrade window appears. From this window, you can schedule an image update task immediately or later. For more information,

View Image Update Workflow

1. **Step 1** Click the menu icon () and choose Provision > Network Devices > Inventory.
2. **Step 2** From the Focus drop-down list, choose Software Images.
3. **Step 3** From the Actions drop-down list, choose Software Images > Image Update Status.
4. **Step 4** In the Image Update Status window, click the name of a device to view detailed information about the image upgrade.
5. **Step 5** Click the Operations tab.

The slide-in pane shows the status of each task that is associated with the Distribution and Activation operations and the time taken to complete each operation.

6. **Step 6** Expand Distribution to view the status of the following tasks that are associated with the Distribution operation and the time taken to complete each task.
 - Verify Image Availability (only for legacy devices): Verifies the software image in Image Repository
 - Image Integrity Verification (KGV): Compares the software and hardware platform checksum value of the software image with the checksum value identified for the platform in the Known Good Values (KGV).
 - Pre Distribution Operation: Performs all the prechecks chosen for software image distribution.
 - Distribution: Distributes the software image through the primary external image distribution server. If the software image distribution fails through primary external image distribution server, the software image is distributed through secondary image distribution server. If the distribution fails through both the external servers, the software image is distributed through the internal Cisco DNA Center server.
 - Post Distribution Operation: Performs all the post checks chosen for software image distribution.
 - Image Checksum Verification On Device: Verifies the checksum value of the software image on the device.
 - Unpack Image (only for Polaris): Executes the install-add command from the CLI. Unpack image is performed only when the image is in install mode.
 - AP Pre-Image Download (only for access points): Shows details about the distribution process of all the access points associated with the device.
7. **Step 7** Expand Activation to view the status of the following tasks that are associated with the Activation operation and the time taken to complete each task.
 - Pre Activation Operation: Performs all the prechecks chosen for software image activation.
 - Image Activation: Executes the install-activate command in CLI. This shows detailed information about the image activation process.

Note For Cisco Catalyst 9000 Series stack switches, the Validate Stack prechecks verifies the state of all the stack members in a switch. If a stack member is not running the golden image, run the auto-upgrade command.
 - Staggered AP Upgrade (only for access points): Shows details about activation process of all the access points associated with the device.
 - Install Commit (only for Polaris): Executes the install-commit command from the CLI.

- **Remove Inactive Images:** Removes all the previous software images saved on the device and stores only the running image.
- **Collect Running Image Details:** Collects the running image details.
- **Verify Image Activation:** Verifies whether the software image is upgraded properly.
- **Post Activation Operation:** Performs all the postchecks chosen for software image activation.
- **Note**For Cisco Catalyst 9800 Embedded Wireless Controller devices and Cisco Catalyst 9000 Series Switches running on Cisco IOS-XE software, the software image is upgraded in three steps (by executing three commands)—install-add (Unpack Images step in Distribution), install-activate (Image Activation step in Activation), and install-commit (Install Commit step in Activation).
- If the device is in Inactive state, run the install-add command from the CLI. Subsequently run the install-activate and install-commit commands. If the device is in Uncommitted state, run the install-commit command directly.
- Run the install-activate and install-commit commands sequentially in separate milestones during activation, so that you can abort, roll back, or commit the update.

8. **Step 8**Click the Tasks tab.

9. **Step 9**The Tasks tab shows the status and details of prechecks and postchecks that are associated with the task. Click the number of differences in the Differences column, corresponding to each script, to view the differences between prechecks and postcheck.

Auto Flash Cleanup


During the device upgrade readiness precheck, the flash check verifies whether there is enough space on the device to copy the new image. If there is insufficient space:

- For devices that support auto flash cleanup, the flash check fails with a warning message. For these devices, the auto cleanup is attempted during the image distribution process to create the sufficient space. As a part of the auto flash cleanup, Cisco DNA Center identifies unused .bin, .pkg, and .conf files and deletes them iteratively until enough free space is created on the device. Image distribution is attempted after the flash cleanup. You can view these deleted files in System > Audit Logs.

NoteAuto flash cleanup is supported on all devices except Nexus switches and wireless controllers.

- For devices that do not support auto flash cleanup, the flash check fails with an error message. You can delete files from the device flash to create space before starting the image upgrade.

Documents / Resources

	<p>Cisco Manage Software Images [pdf] User Guide IE3x00 series, IE9x00 series, Manage Software Images, Software Images, Images</p>
---	--

References

- [User Manual](#)

Manuals+. Privacy Policy

This website is an independent publication and is neither affiliated with nor endorsed by any of the trademark owners. The "Bluetooth®" word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. The "Wi-Fi®" word mark and logos are registered trademarks owned by the Wi-Fi Alliance. Any use of these marks on this website does not imply any affiliation with or endorsement.