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.

Step 1 From the top-left corner, 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.
- **TOTAL IMAGES**: Shows the number of running images, imported images, and golden images.
- **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.

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.

Note Third party(non-Cisco) devices are not shown in the **Image Repository** window, because image activation and image update features are not supported for third-party devices.

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.

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.

Step 5 Click **Import Image** to import a software image or software image update. For more information, see Import a Software Image, on page 5.

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.

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, see Assign a Software Image to a Device Family, on page 6.

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:

a) 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.

b) In the **Version** column, click the **Add On** link to view the applicable **SMUs**, **PSIRT SMU**, **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.

c) In the **Device(s)** column, click the number of devices to view the devices that are using the image.

d) 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**.

e) 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.

f) 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 From the top-left corner, click the menu icon and choose **System** > **Settings** > **Cisco.com Credentials**.

Step 2 Verify that you have entered the correct credentials to connect to cisco.com.

Step 3 From the top-left corner, 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
```

Step 1 From the top-left corner, click the menu icon and choose **Design** > **Image Repository**.

Step 2 Click **Import Image**.

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.

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**.

Note Image activation and Image update features are not supported for third party (non-Cisco) devices.

Step 5 Click **Import**.

A window displays the progress of the import.

Step 6 Click **Show Tasks** to verify that the image was imported successfully.

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.

Step 7 Click the **Add-On** link to view the SMU.

Step 8 In the **Device Role** field, select the role for which you want to mark this SMU as golden. See Specify a Golden Software Image, on page 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 the 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:

Step 1 From the top-left corner, click the menu icon and choose **Design** > **Image Repository**.

Step 2 Click **Imported Images**.

Step 3 Click **Assign** in the corresponding image name row.

Step 4 In the **Assign Device Family** window, choose the **Device Series from Cisco.com** or **All Device Series** and click **Assign** link to which you want to map the image.

Note: If cisco.com credentials are not set, specify the credentials in **System** > **Settings** > **Cisco.com Credentials**.

Step 5 Select appropriate site from the Global hierarchy and click **Assign** and then click **Save**.

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 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 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** window 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.

Step 1 From the top-left corner, click the menu icon and choose **Design** > **Image Repository**.

Step 2 In the **Image Name** column, find the software image of the device that is running in **Install Mode**.

Step 3 Click **Import** to upload the binary software image file for the image that is in Install Mode.

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.

Step 5 Click **Import**.

A window displays the progress of the import.

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.

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.

You cannot mark a SMU as golden unless the image to which it corresponds is also marked golden.

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 From the top-left corner, 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 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*.

Step 1 From the top-left corner, click the menu icon and choose **System** > **Settings** > **Device Settings** > **Image Distribution Servers**.

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.

Step 3 Click **Add** to add a new image distribution server.

The **Add a New Image Distribution Server** slide-in pane is displayed.

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.

Step 5 Click **Save**.

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:

a) Hover over the **i** icon next to the IP address of the SFTP server and click **Click here**.
b) In the **Compatibility Mode** slide-in pane, check the **Compatibility Mode** check box and enter a duration (from 1 minute to 90 days).
c) Click **Save**.

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**.

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.

Step 1 From the top-left corner, click the menu icon and choose **System** > **Settings** > **Device Settings** > **Image Distribution Servers**.

Step 2 In the **Image Distribution Servers** window, click the **Preferences** tab.

The default protocol order is displayed.

Step 3 In the Protocol Order area, click the **On/Off** protocol 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 fails while using the HTTPS protocol, the software image is distributed using the SCP protocol.

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

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, on page 9.

Step 1 From the top-left corner, click the menu icon and choose **Design** > **Network Settings** > **Network**.

Step 2 Expand the **Image Distribution** area to select SFTP servers to act as Image Distribution servers.

Step 3 Check the **Add image distribution servers** check box to view the fields.

Step 4 From the **Primary** drop-down list, choose the image distribution server that you want to configure as primary.

Step 5 Click the + icon and from the **Secondary** drop-down list, choose the image distribution server that you want to configure as secondary.

Step 6 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. See Specify a Golden Software Image, on page 8.
- Enabling ITSM in Cisco DNA Center enforces an ITSM approval process for better control of Cisco DNA Center software image updates. To enable enhanced control of configuration changes, on the **System** > **Settings** > **Visibility and Control of Configurations** window, click **ITSM Approval** to schedule the image update approval in ITSM. For more information, see "Enable Visibility and Control of Configurations" in the *Cisco DNA Center Administrator Guide*.

Note If you have enabled Visibility of Configurations, the system cannot generate a configuration preview for image upgrade. This is expected behavior for SWIM workflows.

- If you must upgrade the software image immediately, you can disable **ITSM Approval** in the **Visibility and Control of Configurations** window, or you can disable the Cisco DNA Center Automation Events for ITSM (ServiceNow) bundle. To access the bundle, choose **Platform** > **Manage** > **Bundles** > **Cisco DNA Center Automation Events for ITSM (ServiceNow)**.

Step 1 From the top-left corner, click the menu icon and choose **Provision** > **Network Devices** > **Inventory**.

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.

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

You are redirected to the **Image Update** workflow.

Step 4 In the **Image Update** window, enter a unique name in **Task Name** field.

Step 5 In the **Software Distribution Checks** window, click the toggle button to enable or disable prechecks and postchecks for the software distribution.

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. See Add Image Distribution Servers to Sites, on page 10.

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

a) Hover your mouse over the information icon to view the validation criteria and the CLI commands that are used for the validation.

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

c) (Optional) To add new custom prechecks and postchecks, do the following:

1. Click **add a custom check** to launch the **New Custom Check** window.
2. Enter the **Name** for the custom check.
3. From the **When** drop-down list, choose **pre**, **post**, or both.
4. From the **Select a Test Device** drop-down list, choose the device you want to check.
5. Click **Open Command Runner**, and enter the CLI commands.
6. Expand **Add Known Command-Patterns to Ignore During Checks** to add a command pattern that is used to ignore the matching output for the checks.

   To add a command pattern, do the following:

   - To create a new pattern, enter a desired name and string or pattern.
   - To use an existing pattern, click **most commonly used patterns**, select the desired pattern, and click **Add Selected**.
   - Click **Test All Patterns**.

7. Expand the **Additional Criteria** area.

   From the **Operation** drop-down list, choose **Distribution**, **Activation**, or both.
8. From the **Device Series** drop-down list, choose the desired device series and click **Save**.

d) (Optional) To reorder the sequence of the checks, drag and drop a check in the desired order.

Note At the top of the workflow window, place your cursor over the blue progress bar to identify your current step and to switch back to any of the previous steps.

Step 6 In the **Software Activation Checks** window, click the toggle button to enable or disable prechecks and postchecks for the software activation.

(Optional) Click the **Skip Activation** toggle button to skip activation for the current image update.

To add new custom prechecks and postchecks, follow substep c of Step 5.

Step 7 In the **Device Activation Order** window, do the following:

a) To move the devices to sequential order, select the desired devices and click **Move to Sequential Update Order**.
b) In the **Sequential** tab, select the devices and click **Reorder List**.

To reorder the sequence of the devices, drag and drop the devices in the order you want and click **Finish Reorder**.

Note By default, the device activation order is set to parallel as first. Click **Edit** to change the activation order.

c) Click the **Abort on Update Failure** toggle button to end the activation process on the remaining devices upon activation failure of the first device in the order.
d) To enable the ISSU upgrade, choose the device that you want to upgrade. From the **ISSU** drop-down list, choose **Enable ISSU Upgrade**.

Step 8 In the **Schedule Task and Clean Up** window, do the following:

a) Click the **Now** radio button to start the activation or distribution immediately.
b) Click the **Later** radio button, and define the date, time, and time zone to schedule the activation or distribution later.
c) (Optional) Click the **After Distribution** toggle button to trigger the software activation process immediately after the software distribution.
d) (Optional) Check the **Initiate Flash Cleanup After Activation** check box to initiate a flash cleanup of the device's memory.

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

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.

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

Step 11 To proceed, click **Submit**.

Step 12 (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.

Step 1 From the top-left corner, click the menu icon and choose **Design** > **Image Repository**.

Step 2 Click **Import Images**.

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.

Step 4 Click **Import**.

Step 5 Click **Show Tasks** to view the ISSU compatibility matrix file import status.

Note In Cisco DNA Center 2.3.7 and later, compatibility matrix files are automatically downloaded for ISSU-supported devices' running images and golden tagged images available in cisco.com.

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. See Import the ISSU Compatibility Matrix, on page 13.
- Enabling ITSM in Cisco DNA Center enforces an ITSM approval process for better control of Cisco DNA Center software image updates. To enable enhanced control of configuration changes, on the **System** > **Settings** > **Visibility and Control of Configurations** window, click **ITSM Approval** to schedule the image update approval in ITSM. For more information, see "Enable Visibility and Control of Configurations" in the *Cisco DNA Center Administrator Guide*.

Note If you have enabled Visibility of Configurations, the system cannot generate a configuration preview for image upgrade. This is expected behavior for SWIM workflows.

- If you must upgrade the software image immediately, you can disable **ITSM Approval** in the **Visibility and Control of Configurations** window, or you can disable the Cisco DNA Center Automation Events for ITSM (ServiceNow) bundle. To access the bundle, choose **Platform** > **Manage** > **Bundles** > **Cisco DNA Center Automation Events for ITSM (ServiceNow)**.

Step 1 From the top-left corner, click the menu icon and choose **Provision** > **Network Devices** > **Inventory**.

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

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

The **Image Upgrade** window appears.

Step 4 In the **Analyze Selection** window, enable the ISSU upgrade:

a) 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.

b) From the **ISSU** drop-down list, choose **Enable ISSU Upgrade**.
c) Click **Next**.

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:

a) Hover your cursor over the Info icon to view the validation criteria and the CLI commands that are used for validation.
b) Click the toggle button to uncheck the validators that you do not want to run for the current workflow.
c) (Optional) To add new custom prechecks and postchecks, do the following:

1. Click **add a new check** to launch the **Add a New Custom Check** window.
2. Enter the **Name** for the custom check.
3. Click the **When** drop-down list and choose **pre**, **post**, or **both**.
4. From the **Select a Test Device** drop-down list, choose a device for which you want to run the custom checks.
5. Click **Open Command Runner** and enter the CLI commands.
6. Expand the **Additional Criteria** area.
7. Click the **Operation** drop-down arrow and choose **Distribution**.
8. Click the **Device Series** drop-down arrow and choose the device series for which you want to run the custom checks.
9. Click **Save**.
10. If you want to edit a custom check, click the corresponding More icon, choose **Edit**, make the required changes, and click **Save**.
11. If you want to delete a custom check, click the corresponding More icon, choose **Delete**, and in the **Confirm Delete** message, click **Delete**.

Note
- If associated with a network hierarchy, the external image distribution server distributes the image to all devices in the network hierarchy. See Add Image Distribution Servers to Sites, on page 10.
- If **ITSM Approval** is enabled in Cisco DNA Center, you can update the image (distribute and activate) only after receiving the approval.

Step 6 Click **Next**.

Step 7 In the **Activate** window, choose whether you want to start the activation **Now** or schedule it for later.

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:

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

c) (Optional) To add new custom prechecks and postchecks, do the following:

1. Click **add a new check** link to launch the **Add a New Custom Check** window.
2. Enter the **Name** for the custom check.
3. Click the **When** drop-down list and choose **pre**, **post**, or **both** as required.
4. Click **Select a Test Device** drop-down list and choose a device for which you want to run these custom checks.
5. Click **Open Command Runner** and enter the CLI commands.
6. Expand the **Additional Criteria** area.
7. Click the **Operation** drop-down list and choose **Activation**.
8. Click the **Device Series** drop-down list and choose the device series for which you want to run these custom checks.
9. Click **Save**.
10. If you want to edit a custom check, click the corresponding More icon, choose **Edit**, make the required changes, and click **Save**.
11. If you want to delete a custom check, click the corresponding More icon, choose **Delete**, and click **Delete** in the **Confirm Delete** message.

Step 9 Click **Next**.

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

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 From the top-left corner, 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, see View Image Update Workflow, on page 17.

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 is displayed. From this window, you can schedule an image update task immediately or later. For more information, see Provision a Software Image, on page 11.

View Image Update Workflow

Step 1 From the top-left corner, 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**.

Step 4 In the **Image Update Status** window, click the name of a device to view detailed information about the image upgrade.

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.

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 the 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 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 the primary external image distribution server, the software image is distributed through the secondary image distribution server. If the distribution fails through both external servers, the software image is distributed through the internal Cisco DNA Center server.
- **Post Distribution Operation**: Performs all postchecks 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 in the CLI. Unpack image is performed only when the image is in install mode.
- **AP Pre-Image Download** (only for APs): Shows details about the distribution process of all the APs associated with the device.

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 prechecks chosen for software image activation.
- **Image Activation**: Executes the **install-activate** command in the CLI. This step shows detailed information about the image activation process.

  Note For Cisco Catalyst 9000 Series stack switches, the Validate Stack precheck verifies the state of all the stack members in a switch. If any stack member is not running the golden image, the **auto-upgrade** command is executed.
- **Staggered AP Upgrade** (only for APs): Shows details about the activation process of all the APs associated with the device.
- **Install Commit** (only for Polaris): Executes the **install-commit** command in 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 postchecks chosen for software image activation.

Note

- For Cisco Catalyst 9800 Embedded Wireless Controller devices and Cisco Catalyst 9000 Series Switches running on 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, the **install-add** command is executed first in the CLI. Subsequently, the **install-activate** and **install-commit** commands are executed. If the device is in Uncommitted state, the **install-commit** command is executed directly.
- The **install-activate** and **install-commit** commands are executed sequentially in separate milestones during activation, so you can cancel, roll back, or commit the update.

Step 8 Expand **PSIRT SMU Activation** to view the status of the following tasks that are associated with the PSIRT SMU Activation operation and time taken to complete each task.

- **Pre Activation Script Execution**.
- **Activation**.
- **Post Activation Script Execution**.

Step 9 Expand **APSP Distribution** to view the status of the following tasks that are associated with the Distribution operation and time taken to complete each task.

- **Image Integrity Verification**: Compares the software and hardware platform checksum value of the software image with checksum value identified for the platform in the Known Good Values (KGV).
- **Pre Distribution Operation**: Performs all prechecks chosen for software image distribution.
- **Distribution**: Distributes the software image through primary external image distribution server.
- **Post Distribution Operation**: Performs all post checks chosen for software image distribution.
- **Image Checksum Verification On Device**: Verifies the checksum value of software image on device.
- **Unpack Image (only for Polaris)**: Executes the install-add command in the CLI. Unpack image is performed only when the image is in install mode.
- **AP Pre-Image Download (only for APs)**: Shows details about the AP pre-image download task for all the APs associated with the device.

Step 10 Click the **Tasks** tab, which shows the status and details of prechecks and postchecks that are associated with the task.

Step 11 In the **Differences** column, click the number of differences, corresponding to each script, to view the differences between prechecks and postchecks.

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**.

Note Auto 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.