Managing Device Software Images

Cisco DNA Center 1.1.2 Training

Copyright Page

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

THIS DOCUMENT IS CONSIDERED CISCO PROPERTY AND COPYRIGHTED AS SUCH. NO PORTION OF COURSE CONTENT OR MATERIALS MAY BE RECORDED, REPRODUCED, DUPLICATED, DISTRIBUTED OR BROADCAST IN ANY MANNER WITHOUT CISCO'S WRITTEN PERMISSION.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Managing Device Software Images

© Copyright 2018 Cisco Systems, Inc. All rights reserved.

Contents

What Should I Know Before I Start?

- Why This Process is Important
  - It Helps Ensure Device Behaviors, Consistency, and Security
- Standardized Device Image Concepts
  - Determining the Business Intent
  - Image Repository Concepts
  - Inheriting Image Standards
  - Managing Virtual Images
- The Use of the Image Repository under Tools on the Home Page
- Skills
- Terms

The Device Software Image Management Process

- Process Overview
- Process Steps
  - Task 1: Identify or Import a Software Image or SMU
  - Task 2: Standardize a Device Software Image or SMU
  - Task 3: Evaluate Automated Audit Results
  - Task 4: Upgrade Non-Compliant Devices
  - Task 5: Monitor the Upgrade Task and Review Results

Links

- To Product Information
- To Training
- To Contact Us

What Should I Know Before I Start?

Why This Process is Important

It Helps Ensure Device Behaviors, Consistency, and Security

For device security and optimal device performance, you can standardize device software images and validate that device images comply with those standards proactively. Image standardization helps you to ensure that devices have the features, technologies, and security or other critical updates, that you expect.

Cisco DNA Center provides a software image standardization process that includes:

- Flexible and granular organization of software images and image updates based on business intent.
- Automated device auditing to determine compliance with defined image standards.
- An upgrade process that comprises distribution of all image files based on the standards.

Note: You can perform software image and software maintenance update (SMU) upgrades on devices that Cisco DNA Center manages only.

This training addresses the tasks that you perform to standardize images, evaluate audit results to determine device compliance with image standards, and upgrade non-compliant devices.

Standardized Device Image Concepts

Determining the Business Intent

You standardize an image based on the key characteristics that address business intent.

- Are there devices in specific enterprise locations that require unique image standards from their counterparts in other locations?
- What role does the device have on the network?
- Which software image is optimal for the device based on its role and location?
- Is there a specific SMU associated with the image that also needs to be distributed to ensure that the device has the features it needs and runs as expected?

With this information, you can:

1. Determine whether you have the software images and SMUs that you need and import them as needed.
2. Based on device roles and locations, designate the image and any applicable SMU as optimal, referred to as a golden image in the system.

The system then references the golden image designations, referred to as tags, in its automated image auditing and compliance process, allowing it to identify, and notify you of, devices that do not have the optimal images or updates proactively.

In non-compliant situations, you can upgrade devices to the standardized image.

As device images, versions, and SMUs are updated, you can redefine image standards, as needed.

You standardize images in **Design** on the **Image Repository** tab, which lists all of the images that are available in the system.

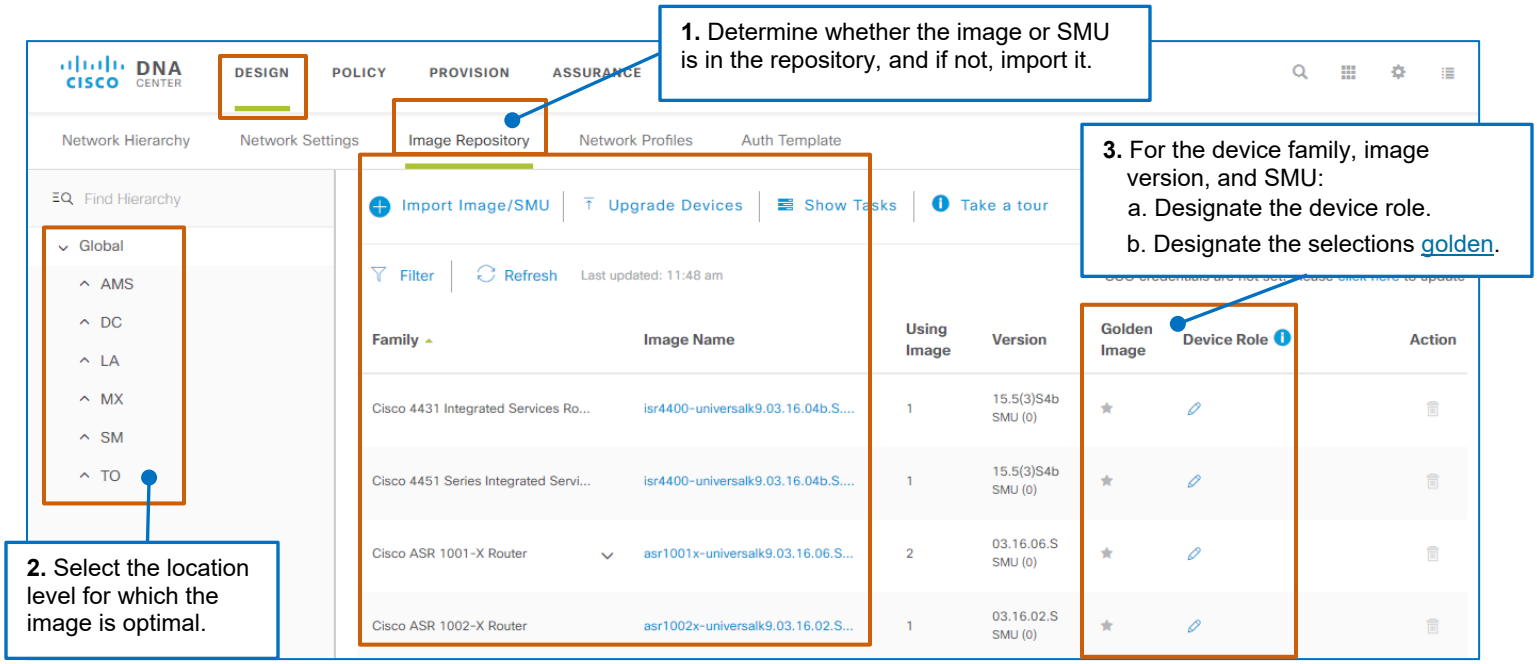
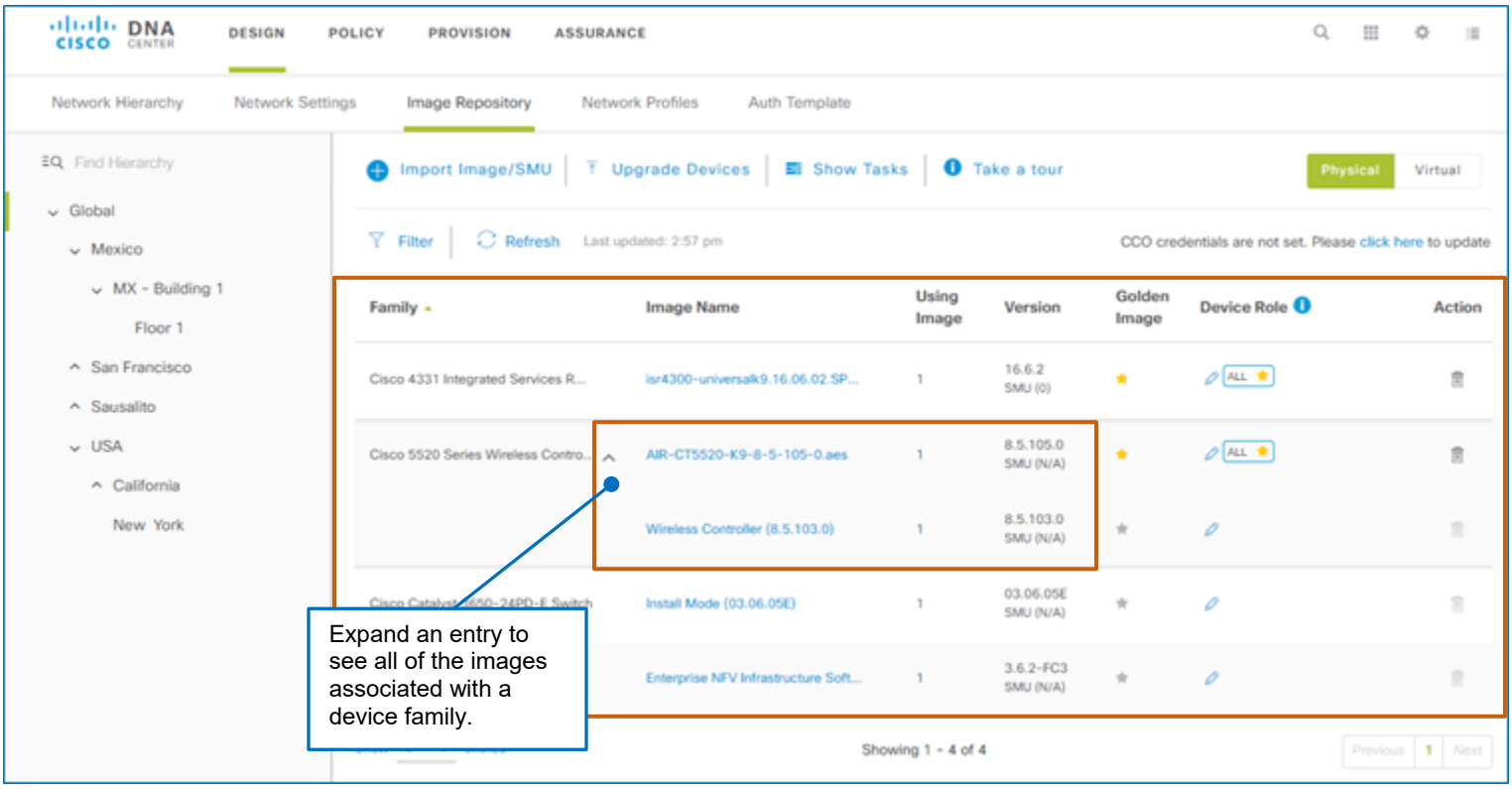


Image Repository Concepts

The image repository houses images and SMUs. When a device family has several images or SMUs, the repository groups them accordingly.

The **Version** column indicates the base image version number and, when SMUs are available, the number of SMUs that are associated with the image and version.



This way, you can determine whether the repository contains the image or SMU that a device requires. If the image or SMU is not available, you can import it to the repository.

Note: When the system is not managing a specific device family type or when images are significantly older versions, the system indicates that the image name is unknown.

You also can import image or SMU files from:

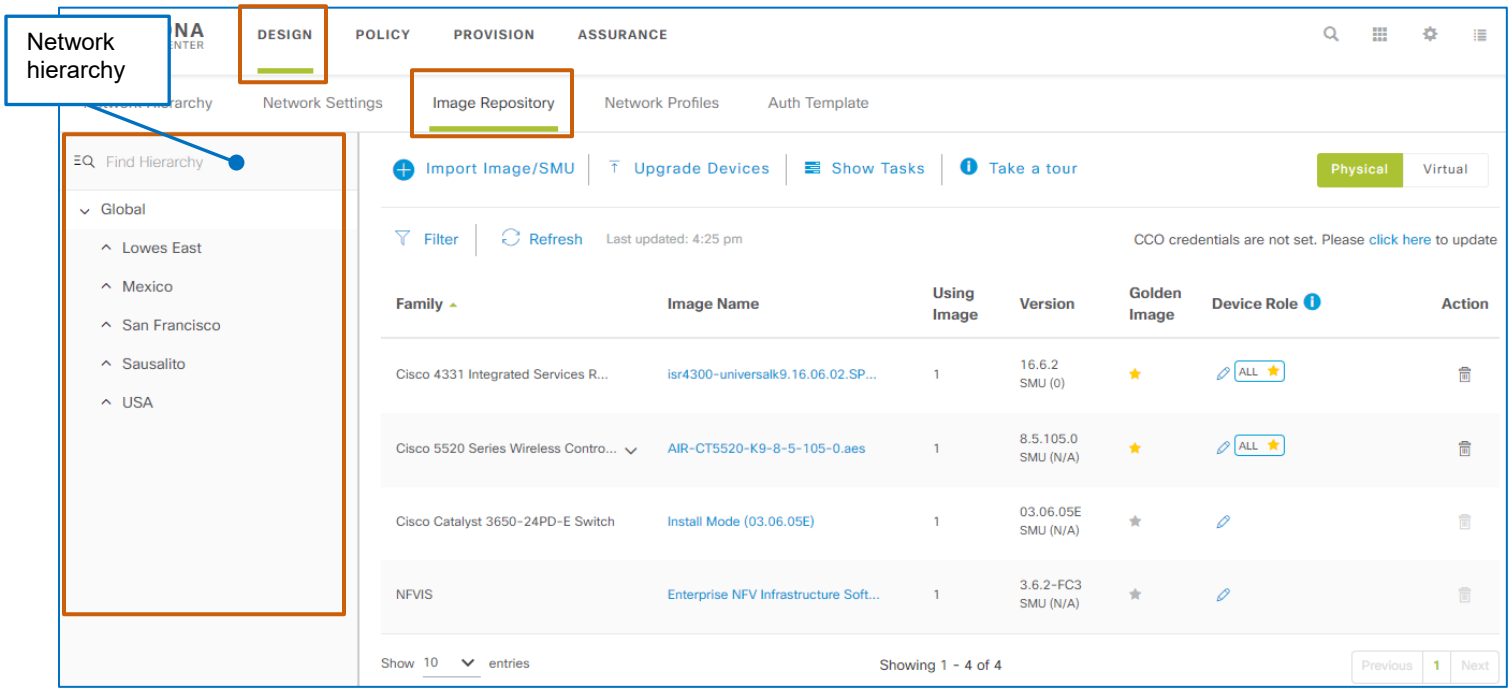
- Your local drive.
- An SFTP or external file server to which Cisco DNA Center has access.
- When system credentials are configured, Cisco.com.

When an image or SMU is running on a device or devices that Cisco DNA Center is managing, and a system user designates it as golden, Cisco DNA Center uploads it to the repository automatically.

Inheriting Image Standards

During network design, system users configure a network hierarchy, which organizes network devices by their locations.

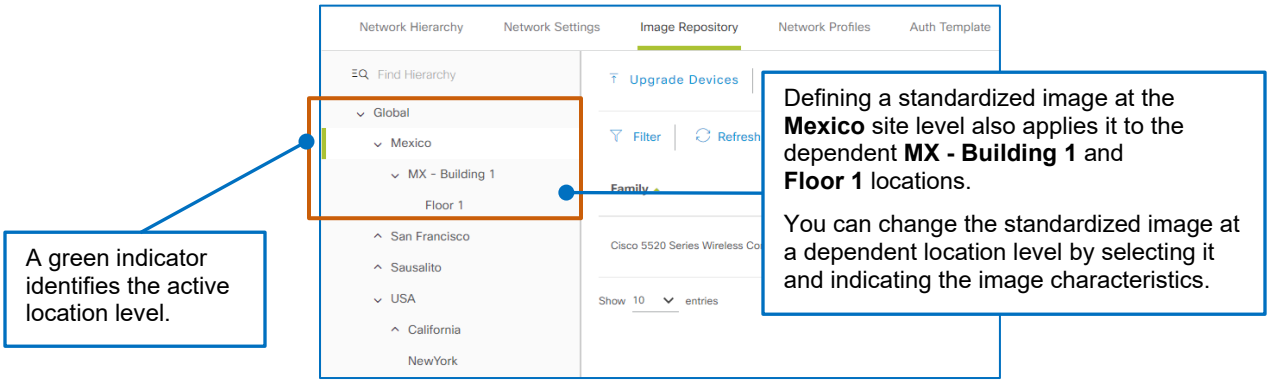
When you standardize images, which is also a network design function, you can define the image characteristics at any location level based on operational requirements.



When you standardize images, the system applies them to the active location level that you select in the hierarchy, and to all of the dependent locations organized below it, in a parent/child relationship.

Under **Design**, when you open the **Image Repository** tab, the system selects the **Global** level in the hierarchy by default. The page lists the running images on devices that Cisco DNA Center has discovered and is managing. When system users organize other sites below the **Global** level, they initially have a child relationship and inherit the **Global** level characteristics.

Then, you can define standardized images with varying characteristics and apply them at any level in the hierarchy based on operational requirements for the devices at that location.

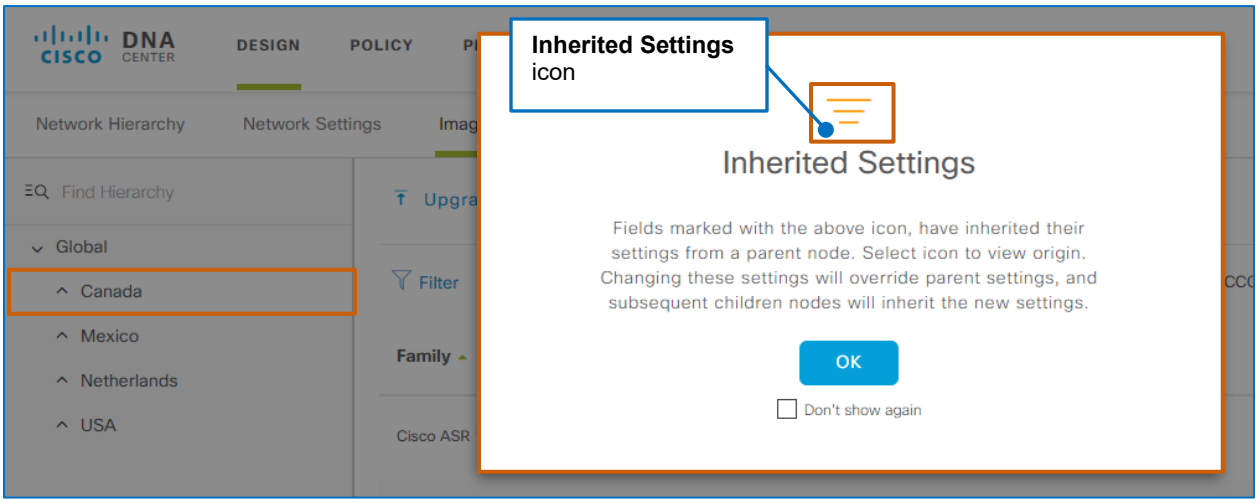


When you click a dependent location that has inherited standards from a parent level, a system message opens indicating the inherited standards. As a visual indicator, the icon above the **Inherited Settings** heading also appears beside images with settings inherited from a parent location.

Caution: When child sites have inherited global standard settings and a system user changes standards at a global level, the system applies the global level changes to those dependent child sites.

Use caution when changing global settings to help ensure that you do not overwrite standards that a child level needs to retain.

If you need to change a global standard, take note of any inherited standards at the child levels in case you need to reapply them.



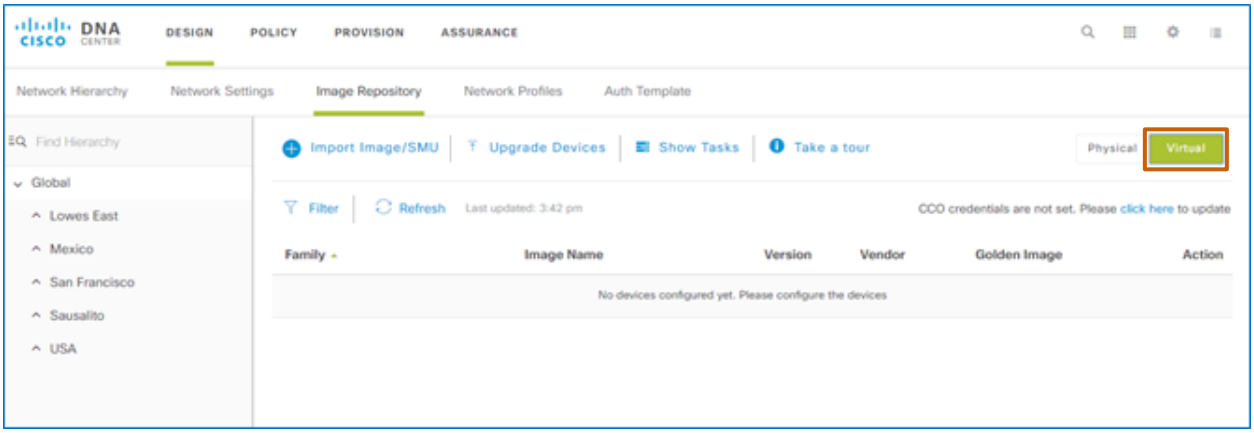
Managing Virtual Images

You also can import and standardize virtual device images to support, for example, virtual branch deployments.

You complete the same tasks to import, standardize, and upgrade images for virtual devices as you do when standardizing images for physical devices. Site parent/child level relationships and standards inheritance in the hierarchy are the same, also.

To standardize virtual images:

- To the right of the toolbar, click **Virtual**. The page toggles to the virtual image repository.



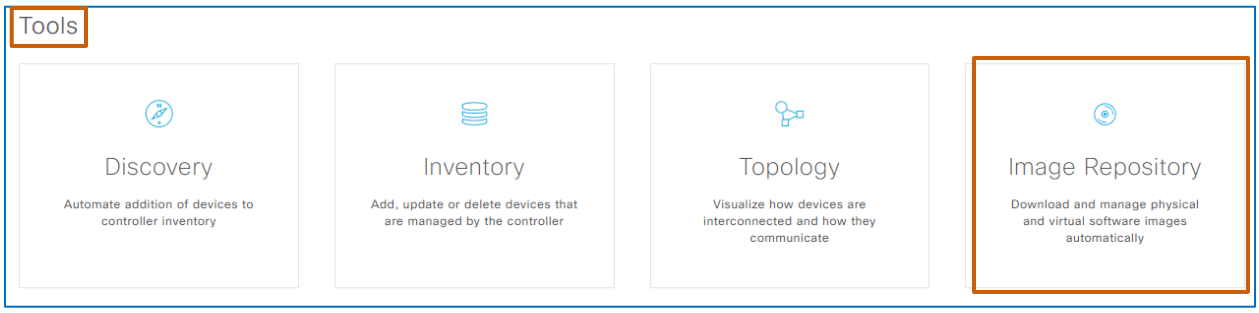
The Use of the Image Repository under Tools on the Home Page

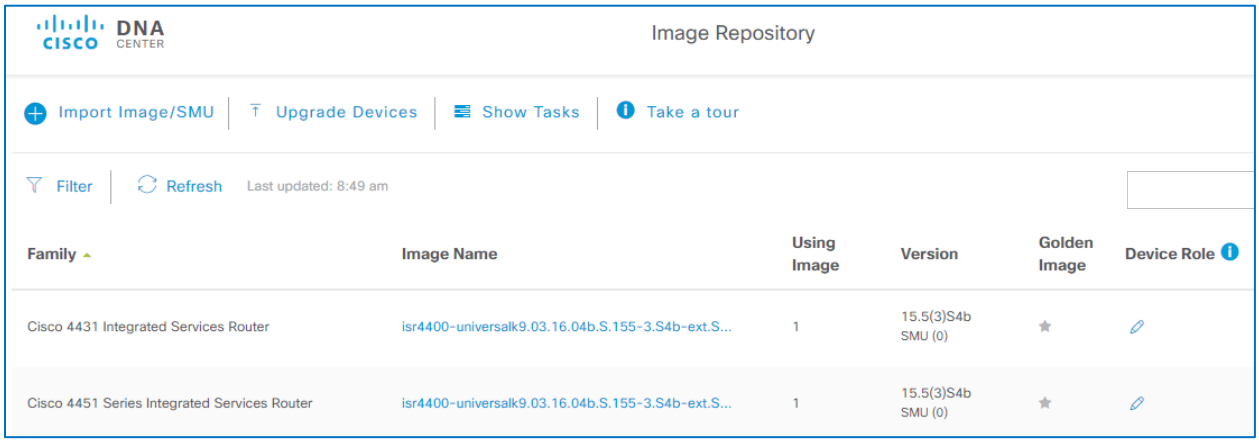
Cisco DNA Center also provides an **Image Repository** page, which you can access on the home page using the **Image Repository** link under **Tools**.

While you can take many of the same steps to standardize and manage software images on this page, we recommend that you use the **Design | Image Repository** tab, which provides access to the network hierarchy.

Important Note: If you take steps to standardize an image and designate it golden on the **Image Repository** page, the system will apply the standard at the global level and present the automated audit results based on that hierarchical level.

Note: If you import an image or SMU on this page, it will be available for use on the **Design | Image Repository** tab.





Skills

To manage software images, you need the following experience.

Proficient

- Cisco DNA Center user interface navigation and behaviors
- Knowledge of network operations
- For the devices that you are upgrading, those devices' roles, relationships, and importance to network operations
- For the devices that you are upgrading, knowledge of the services and technologies that those devices manage

Terms

Device Role

The device's function in the network, for example, a router can have an access, border, core, or distribution function on the network

Golden Image

A tag that indicates to the system that an image is optimal for running on a device family, device type, or device role, or at an enterprise site

Software Maintenance Update (SMU)

A software image update that contains specific corrections for an existing base image.

Upgrading software images with SMUs might or might not require a device reboot. The system notifies you of the reboot status before you initiate the upgrade process.

The Device Software Image Management Process

Process Overview

To upgrade device software images:

1. In **Design**, on the **Image Repository** tab, identify or import the software image or SMU, as needed.
2. Standardize an image and, if applicable, the associated SMU.
3. On the **Device Inventory** page, evaluate automated audit results.
4. Upgrade network device images, as needed.
5. Monitor the upgrade task and review results.

Process Steps

Task 1: Identify or Import a Software Image or SMU

When an image or SMU is running on a device or devices that Cisco DNA Center is managing, and a system user designates it as golden, Cisco DNA Center uploads it to the repository automatically.

When an image or SMU that you need is not available in the repository, you can import it.

Note: For more information, refer to the **Image Repository Concepts** topic.

To identify or import a software image or SMU, follow these steps:

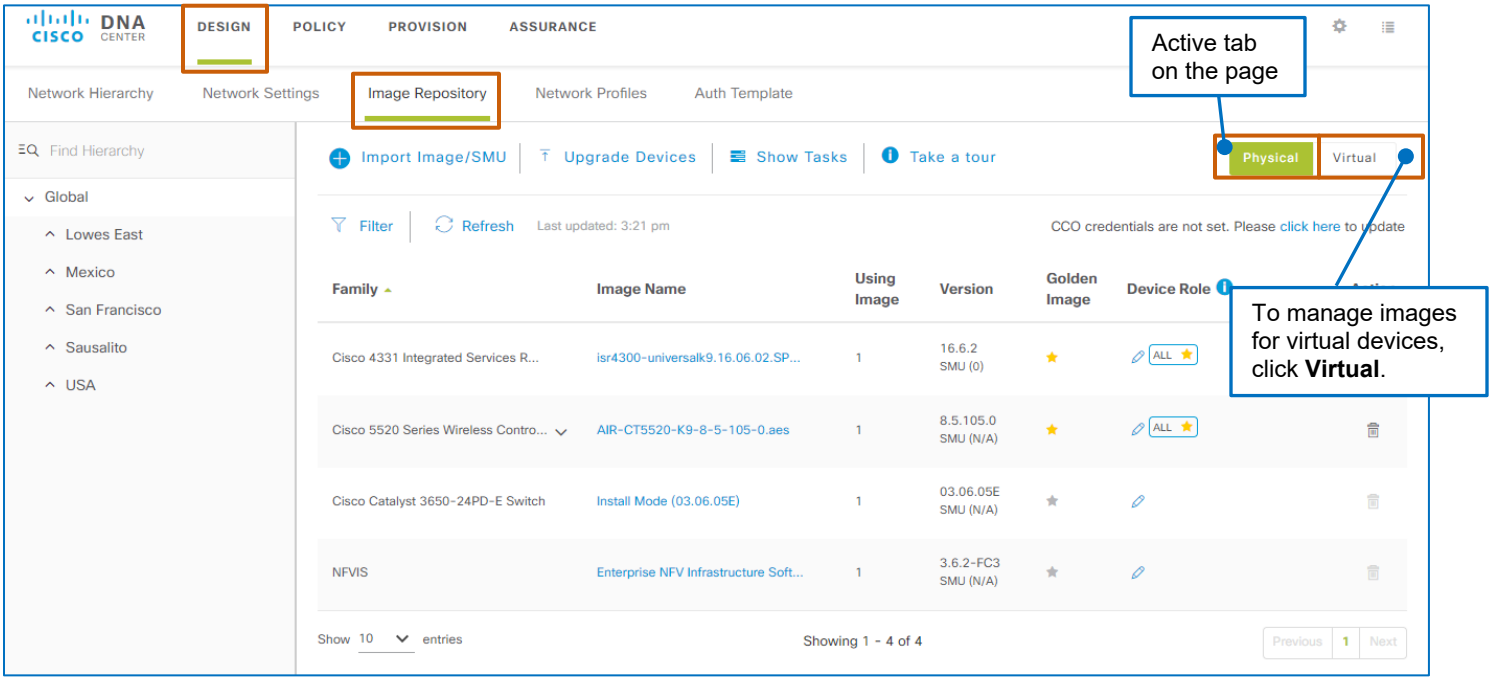
1. On the Cisco **DNA Center** home page, under **Design**, click **Designate golden images for device families**.

The system navigates to the **Design | Image Repository** tab. The tab lists the images that are available for physical devices by default.

Note: The steps that you take to identify and import images are the same for physical or virtual devices.

To manage images for virtual devices:

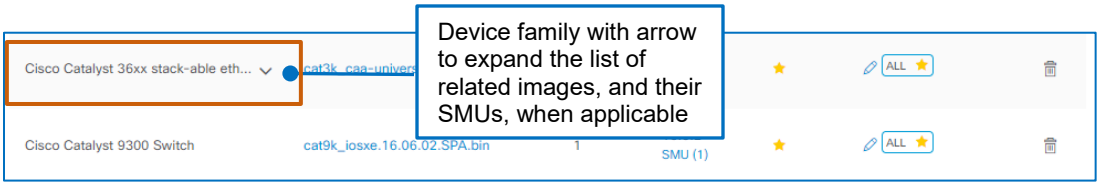
- Click **Virtual**.



2. To determine whether the image that you need to standardize is available in Cisco DNA Center, review the list of images and associated SMUs.

Cisco 4431 Integrated Services Ro...	isr4400-universalk9.03.16.02.S.1...	0	3.16.1 SMU (0)		ALL	
Cisco 4451 Series Integrated Servi...	isr4400-universalk9.03.16.02.S.1...	2	3.16.1 SMU (0)		ALL	
Cisco Catalyst 36xx stack-able eth...	cat3k_caa-universalk9.16.03.03....	1	16.3.3 SMU (N/A)		ALL	
Cisco Catalyst 9300 Switch	cat9k_iosxe.16.06.02.SPA.bin	1	16.6.2 SMU (1)		ALL	
Cisco Catalyst38xx stack-able eth...	Install Mode (16.6.2)	3	16.6.2 SMU (N/A)			
NFVIS	Enterprise NFV Infrastructure Soft...	1	3.6.2-FC3 SMU (N/A)			

Tip: An arrow indicates that there is more than one image available for a device family.

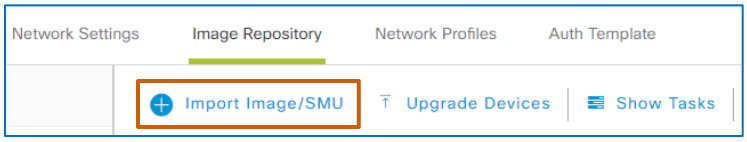


To review the complete list of image files:

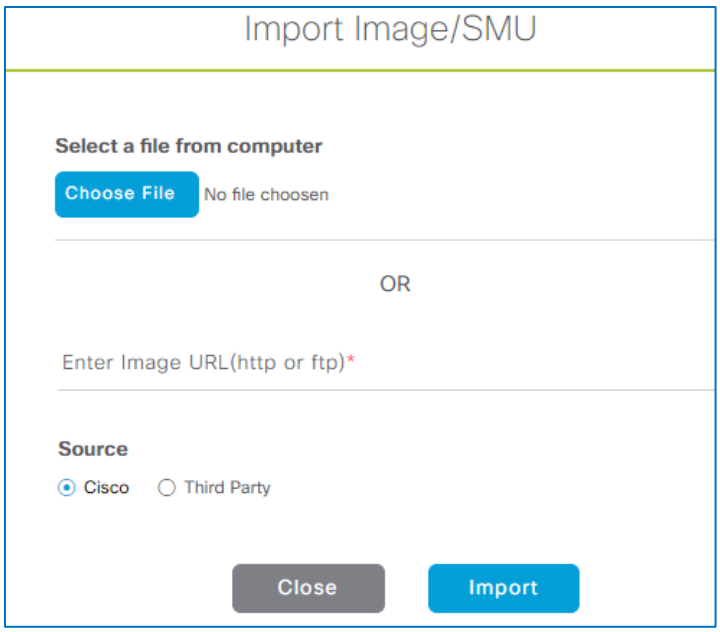
- Expand the device family row.

- If the image or SMU that you need is available in the repository, go to task 2 and standardize it.
- If the image or SMU that you need is not available in the repository, go to step 3.

3. To import an image or SMU file into the repository:
   a. On the toolbar, click **Import Image/SMU**.



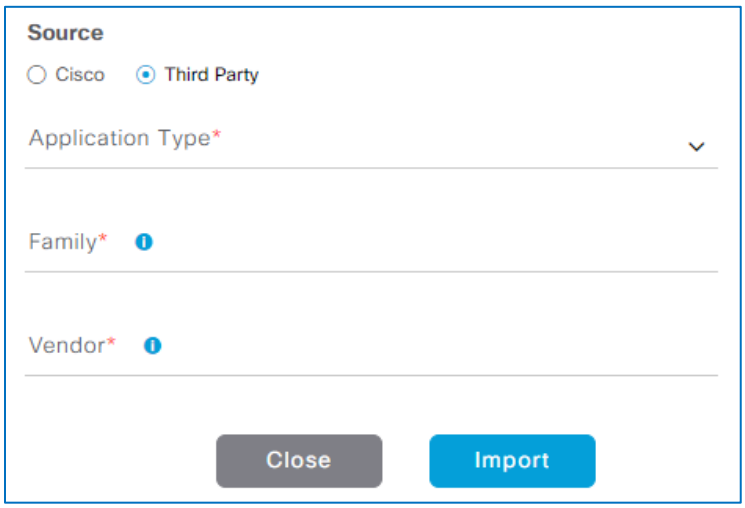
The **Import Image/SMU** dialog box opens.



- To import a file that is stored on your local machine's drive, under **Select a file from computer**, click **Choose File**, and then browse to and select the file.
- To import a file that is on a Web or ftp site, under **Enter Image URL**, type the Web address.

- To import a virtual image file from a third party vendor, indicate the file location by browsing to the file location or typing the IP address, and then:

  i. Under **Source**, select **Third Party**. The section expands to display required import information fields.



  ii. To select the application that is running the image that you need, in the **Application Type** drop-down list, select the application type.

  iii. To identify the image family, such as Windows or Linux, in the **Family** field, type the family name.

  iv. To identify the company that produces the software image, in the **Vendor** field, type the company name.

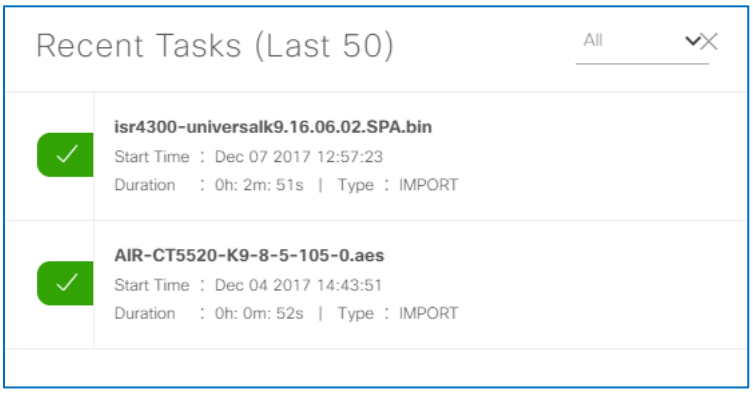
  Note: The system does not validate the family name or vendor name that you type.

b. Click **Import**.

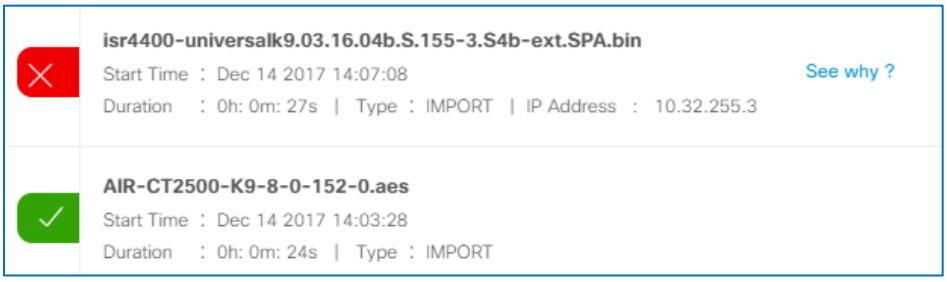
The dialog box closes and the system starts the task to import the image.

4. To monitor the progress and results of the import task, on the toolbar, click **Show Tasks**.

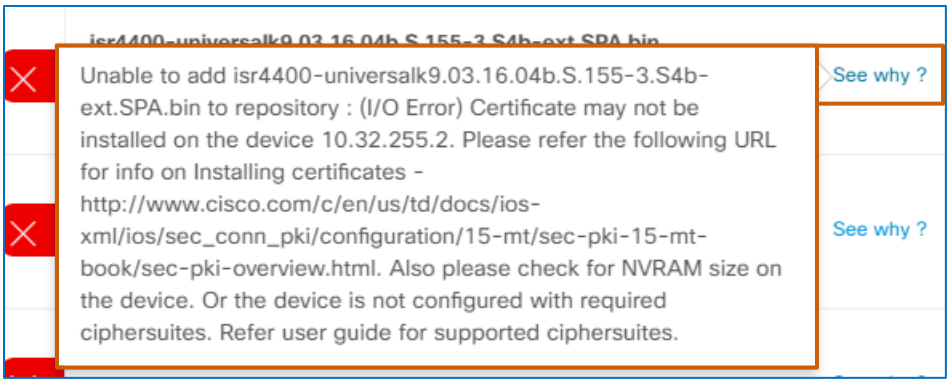
The **Recent Tasks** panel opens and lists the ongoing task.



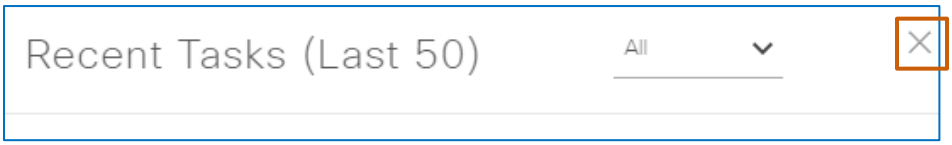
When the import is complete, the panel indicates success with green indicator or failure with a red indicator.



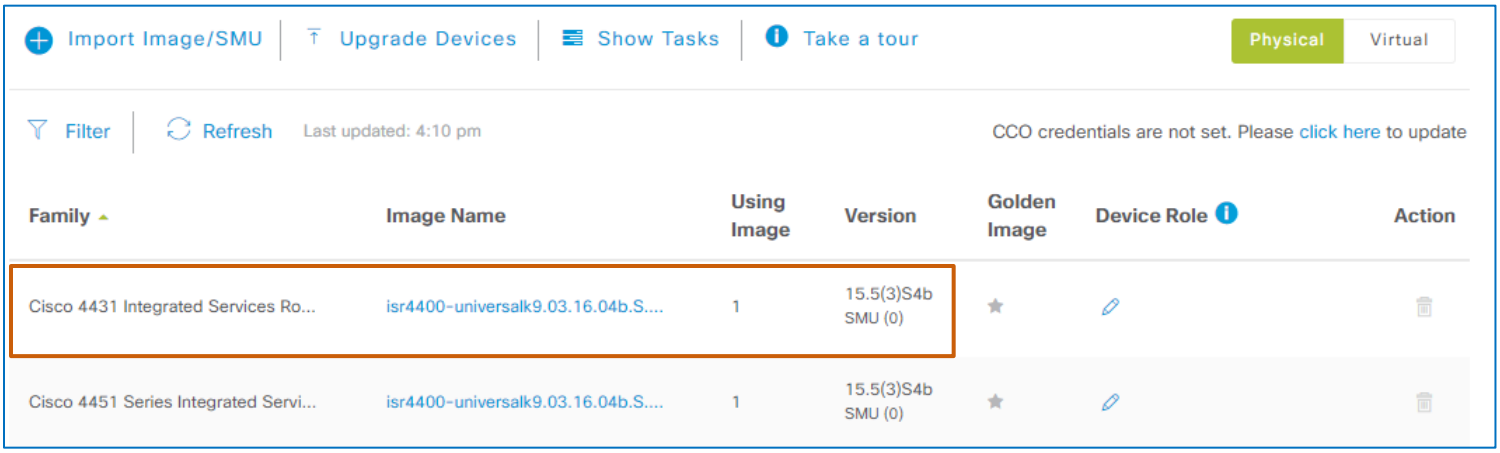
Tip: If an import fails, you can click **See why?** to open a tooltip that describes the problem and suggests ways to correct it.



5. On the **Recent Tasks** panel, click close.



Beside the applicable device family, the repository lists the image or SMU that you imported.



To standardize the image, go to task 2.

Task 2: Standardize a Device Software Image or SMU

You can standardize base software images and SMUs to help ensure that devices have the features, security, and updates that you expect.

Important Note: The system associates a SMU to the base image that it updates automatically.

When you standardize a SMU by designating it golden, you first must designate that its associated base image is golden.

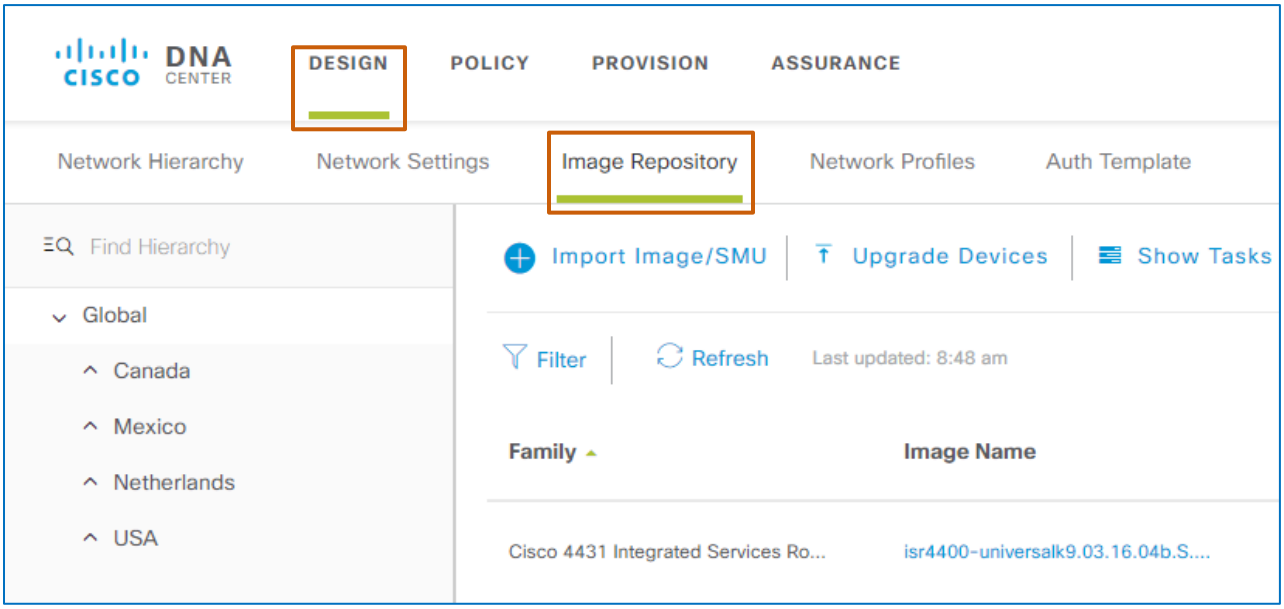
After standardizing a base software image and designating it golden, the steps that you take to designate an applicable image SMU as golden are the same as those for a base image.

Note: Only one SMU can be designated as golden for a base image.

When you standardize an image and its optimal SMU, the system deploys both the image and SMU when upgrading devices.

When a device has the base golden image but not the associated golden SMU, the system upgrades the SMU only.

You standardize images and SMUs in **Design**, on the **Image Repository** tab.



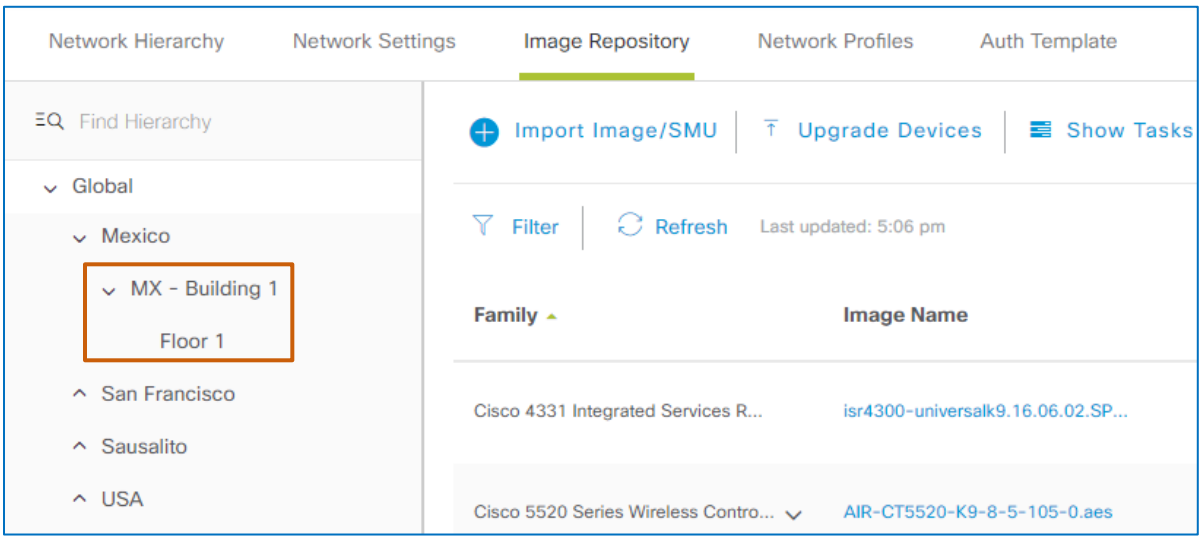
Important Note: Although you can take many of the steps in this task on the **Image Repository** page, we recommend that you standardize images by using this area of the application because it provides access to define standards at specific location levels.

For more information, refer to **The Image Repository Page** topic.

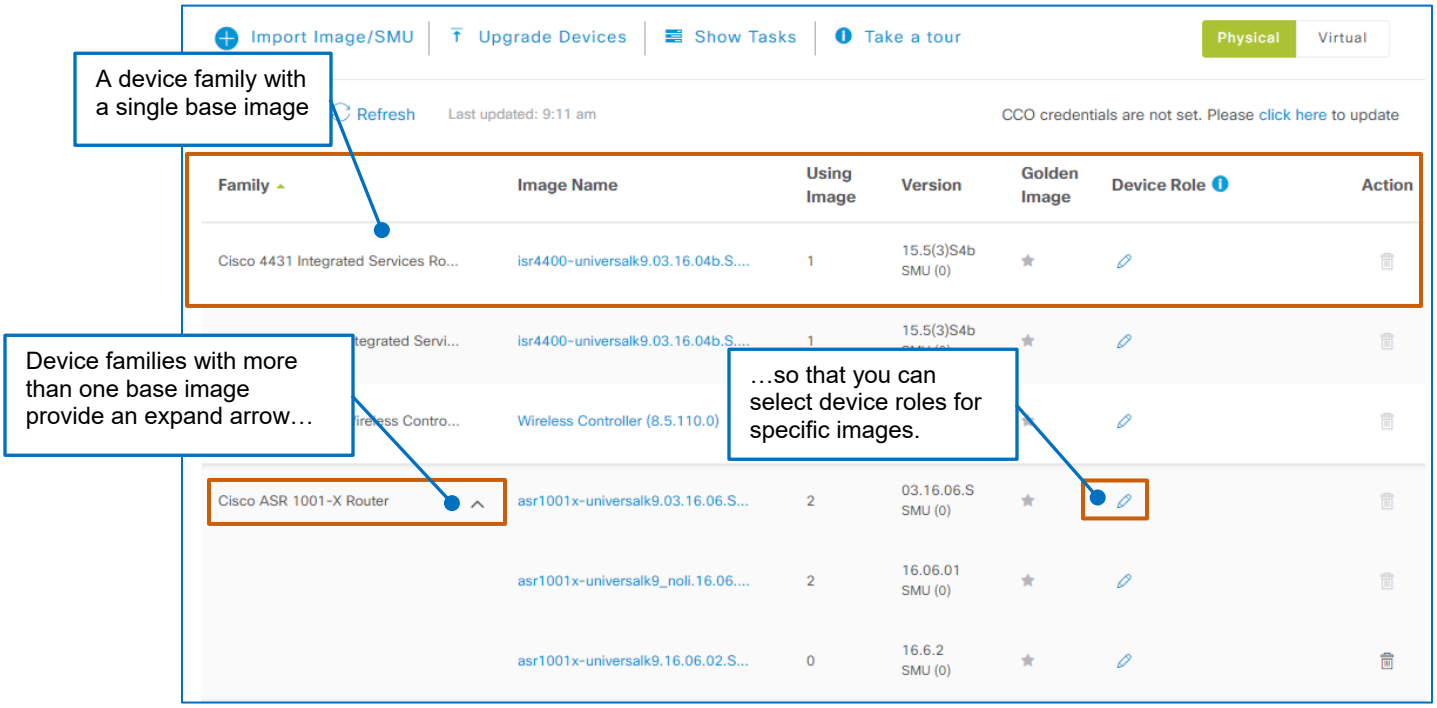
To standardize a device image or SMU, follow these steps:

1. To select the location level for which you need to standardize image characteristics, in the **Design | Image Repository** tab, in the network hierarchy list, select the location.

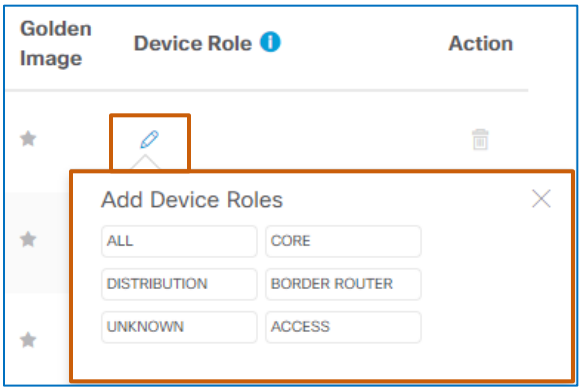
Important Note: Dependent locations in the hierarchy inherit the standards characteristics that you apply at a parent location level.
For more information, refer to the **Inheriting Image Standards** topic.



2. To define the device's function in the network at the location level that you selected in step 1:
   - When the role applies to all of the devices in the device family, in the device family row, in the **Device Role** field, click the pencil icon , and then go to step 2a.
   - When the role applies to a specific base image/SMU running on specific devices in the device family, expand the device's **Family** row, beside the applicable base image/SMU, in the **Device Role** field, click the pencil icon , and then go to step 2a.



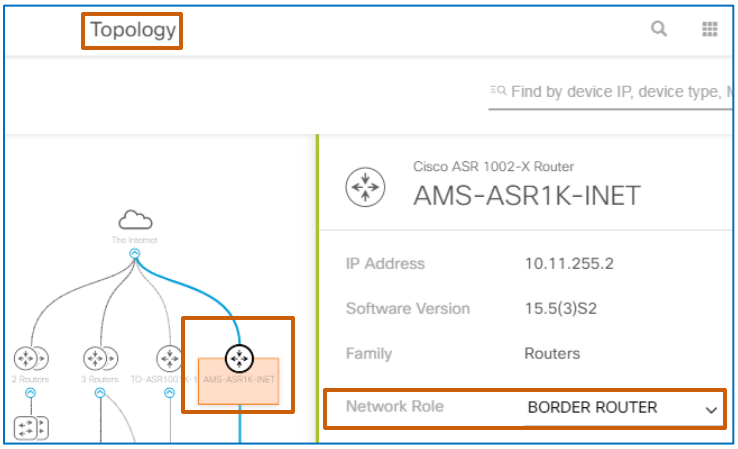
The **Add Device Roles** pop-up window opens.



a. To indicate the device's function in the network topology, in the **Add Device Roles** pop-up window, select the function.

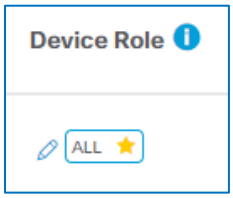
Important Note: During device discovery, the system automatically assigns a network role to the device, which indicates the device's function, and indicates it in the topology.

To best align the device's network role with its device role, review the network topology to determine the role of the device or devices that belong to the device family, and indicate that role as the device role in the image repository.



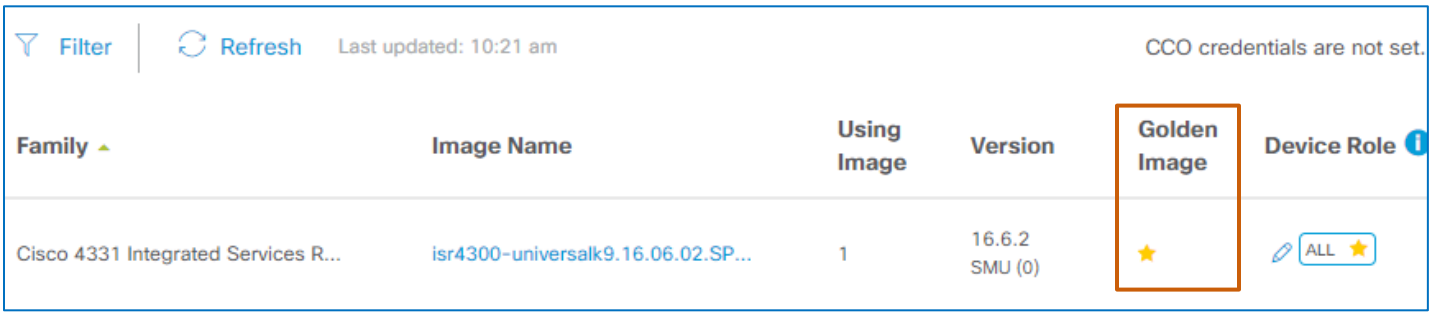
b. Close the pop-up window.

The role that you assigned appears beside the pencil icon, and the star icon displays a yellow color code, which indicates that the role is standardized as part of the golden image.



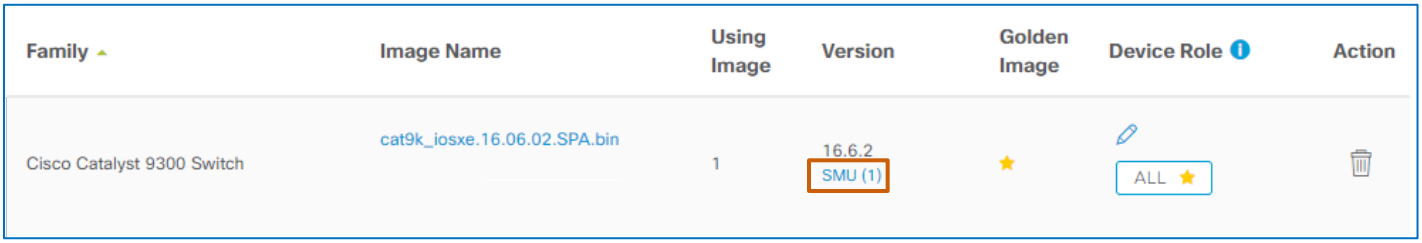
3. To designate the optimal base software image that should run on devices at the location and with the role that you selected, in the applicable row, in the **Golden Image** field, click the star icon.

The star icon displays a yellow color code and the system automatically downloads the image to the repository.

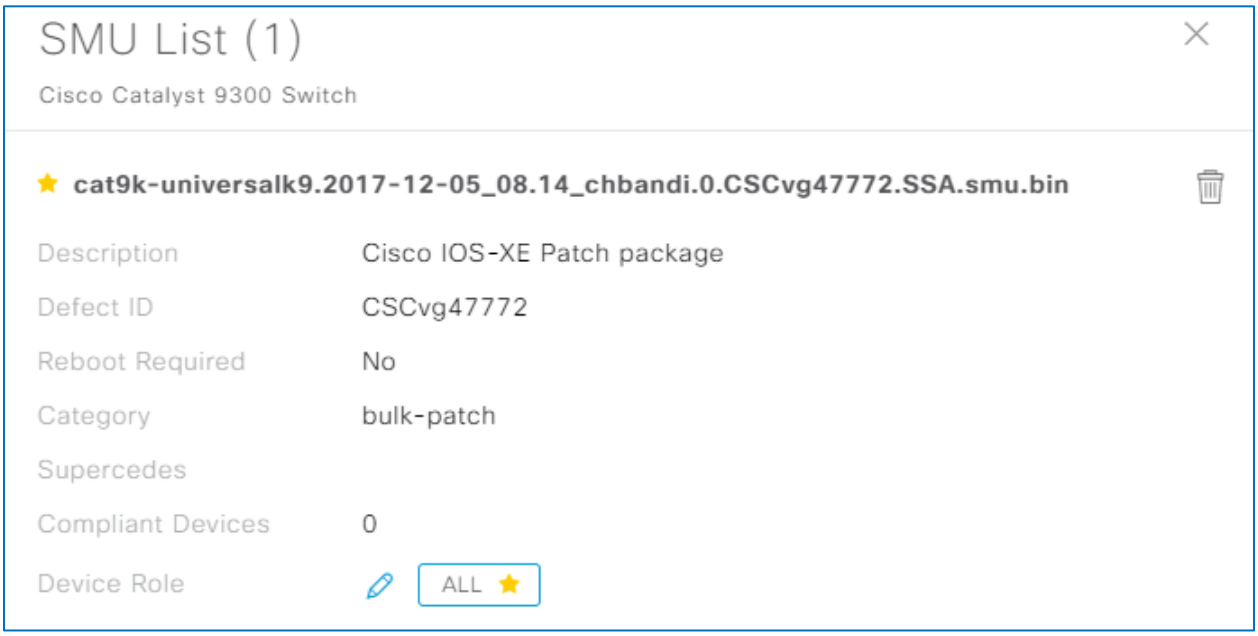


Note: When you indicate that an image is golden, it automatically attempts to import that image so that it is available for use.

4. When applicable, to designate a SMU related to the image as optimal:
   a. Under **Version**, below the version number, click the SMU (#) link.



The **SMU List** panel opens and lists all of the SMUs that are available in the system for the software image.



b. In the panel, beside the optimal SMU name, click the golden image indicator, and then close the panel.

This action prompts the system to audit devices for the base image and SMU combination and apply them during image upgrades.

5. To continue:
   - To standardize another image, return to step 1.
   - To evaluate the audit results based on the standardized images that you defined, go to task 3.

Task 3: Evaluate Automated Audit Results

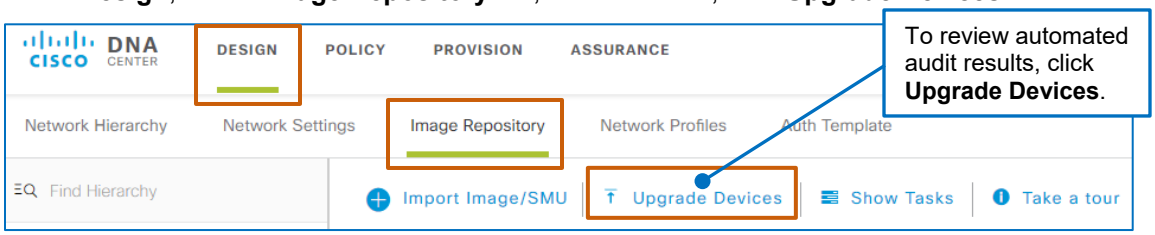
When system users define standardized images and SMUs, the system automatically audits devices for compliance.

During the audit, the system compares the standards for the golden base image and SMU with those that are running on each device, including its location and role to determine compliance.

Note: The system runs audits on device families only when system users designate golden image standards for them.

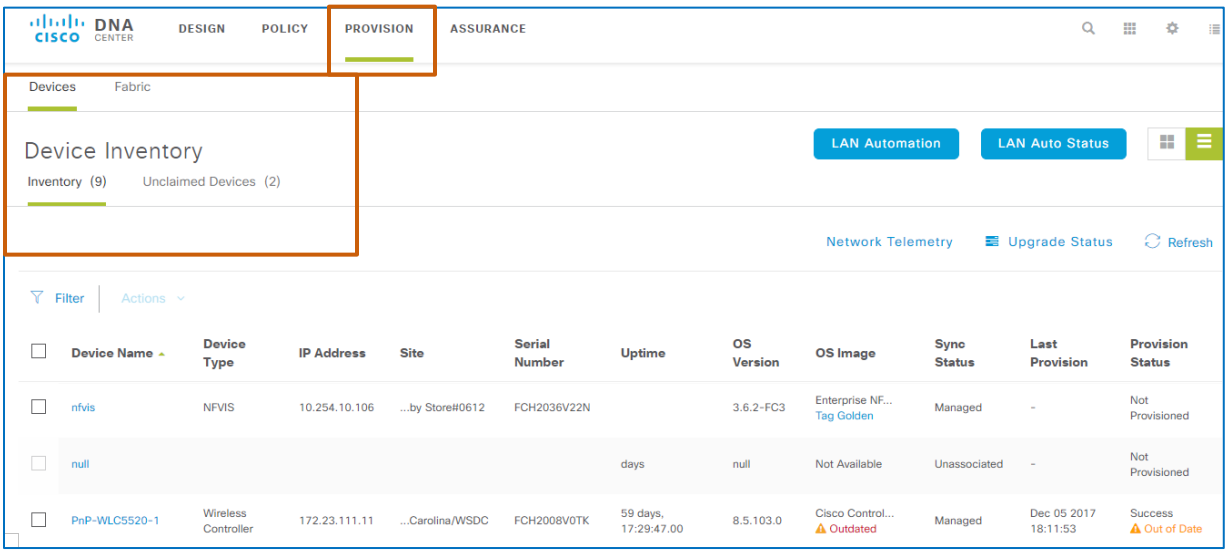
To evaluate automated audit results, follow these steps:

1. In **Design**, on the **Image Repository** tab, on the toolbar, click **Upgrade Devices**.



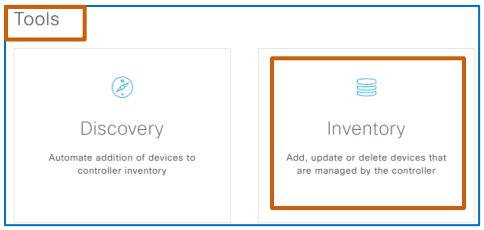
The system navigates to **Provision**, and the **Devices** tab, **Device Inventory | Inventory** subtab is active by default.

Note: The inventory also includes the **Unclaimed Devices** tab, which lists devices that are available for the Plug and Play device deployment and configuration process.



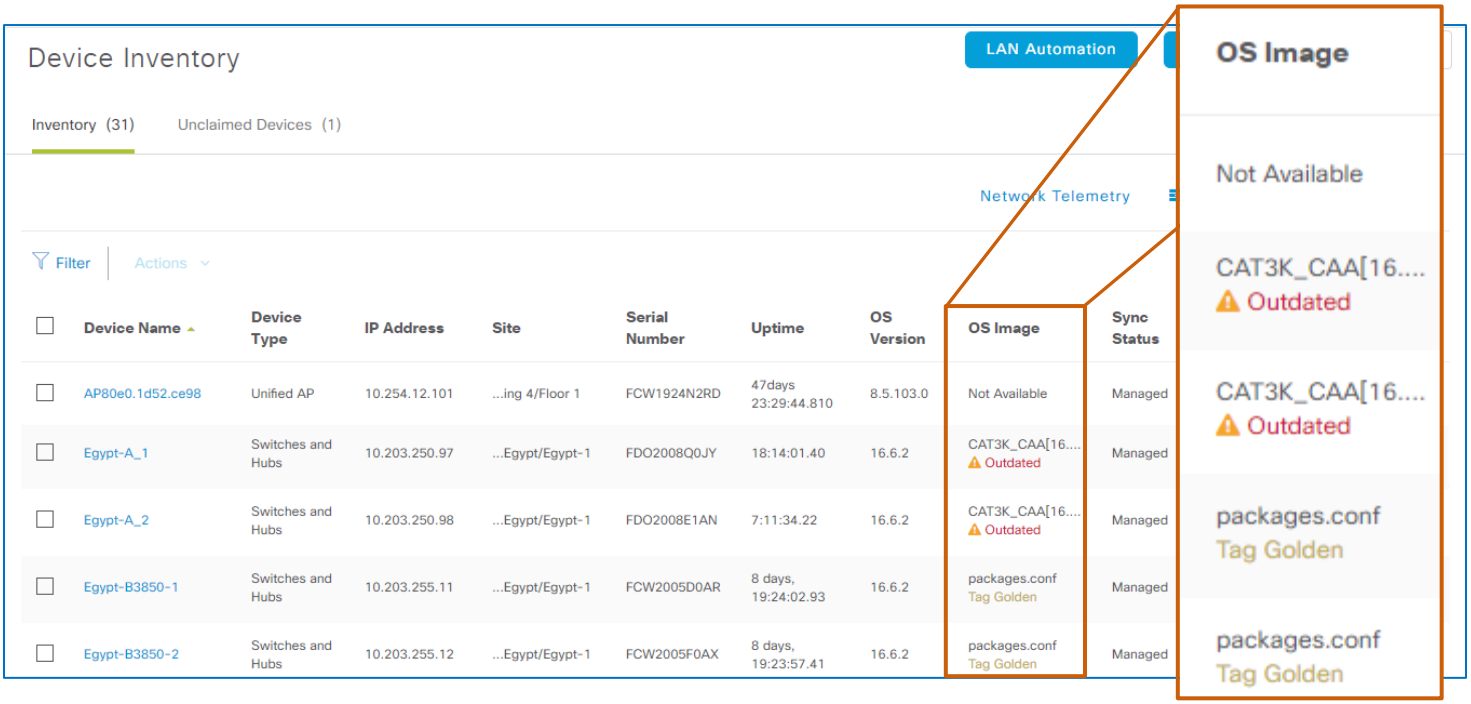
Note: Because you might need to upgrade images on non-compliant devices, the system navigates to the area of the application that supports running the upgrade task.

This page differs from the device inventory that you can access on the home page under **Tools**. That page does not provide audit results or support upgrade tasks.

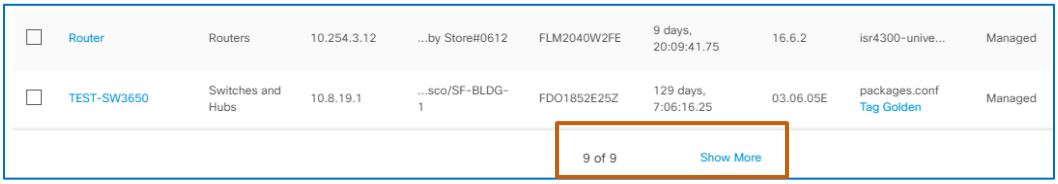


2. On the **Device Inventory** page, on the **Inventory** tab, in the **OS Image** column, below the image name, review the image audit results.

Note: The system does not support access point images.
In those cases, under **OS Image**, the system indicates **Not Available**.



Important Note: Below the list, ensure you are seeing all of the images that are available in the inventory during your compliance review.



Audit results include:

- **Tag Golden**
  Indicates that a standardized image has not been defined for the device.
- **Outdated**
  Indicates that there is a standardized image available for the device and that the device is not running the standardized image.
- **No result**
  The device is using the applicable standardized image.

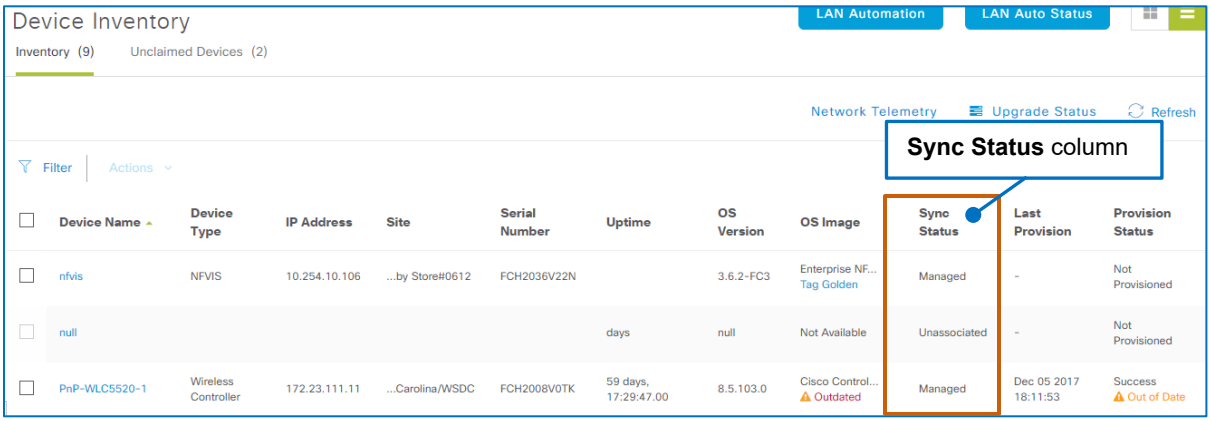
3. To address the audit results:
   - For devices with images that indicate **Tag Golden**, to define standardized image characteristics for the family that contains the device, you can perform the steps to standardize an image, and then, to evaluate audit results, return to step 1.
   - To upgrade non-compliant devices, go to task 4.

Task 4: Upgrade Non-Compliant Devices

When you initiate the upgrade process, the system performs a series of validation steps to confirm that devices can accept the upgrade. It also performs validation steps after the upgrade to confirm the upgrade's success or report any problems.

Note: To accept upgrades, devices need to be in a managed state.

To determine a device's management state, refer to the **Sync Status** column.

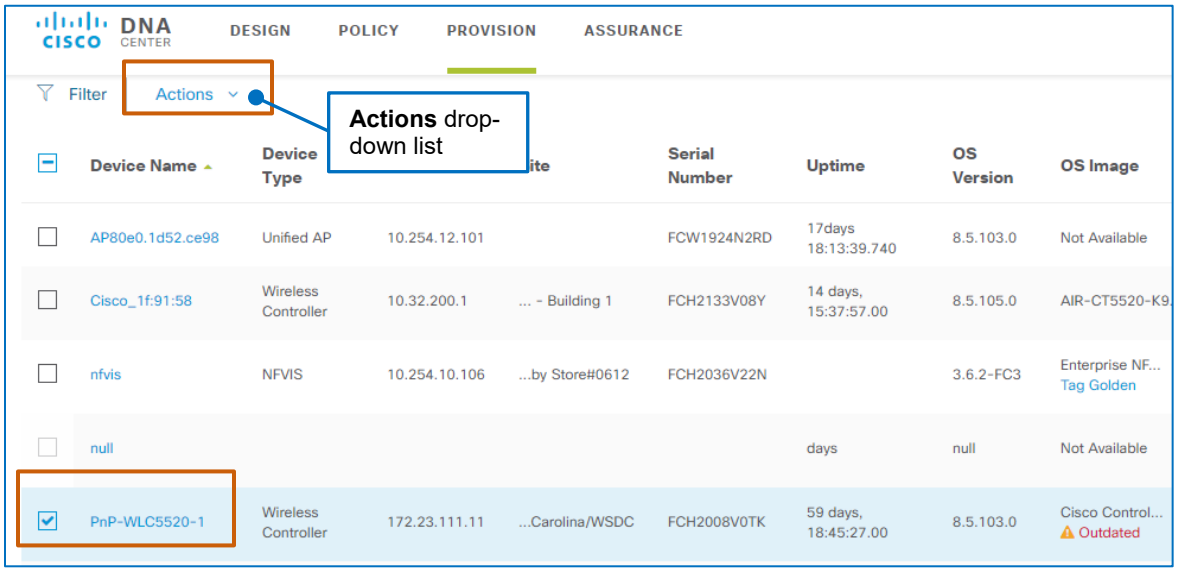


To upgrade non-compliant devices, follow these steps:

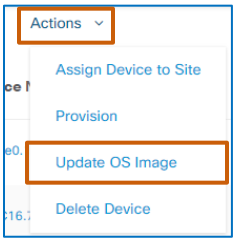
1. In the list, beside the **Device Name** field of each non-compliant device, select the check box.

   Note: When you upgrade multiple devices, the system upgrades the devices in parallel. Depending on the number of devices, the system performs the upgrade in batches until the task is complete.

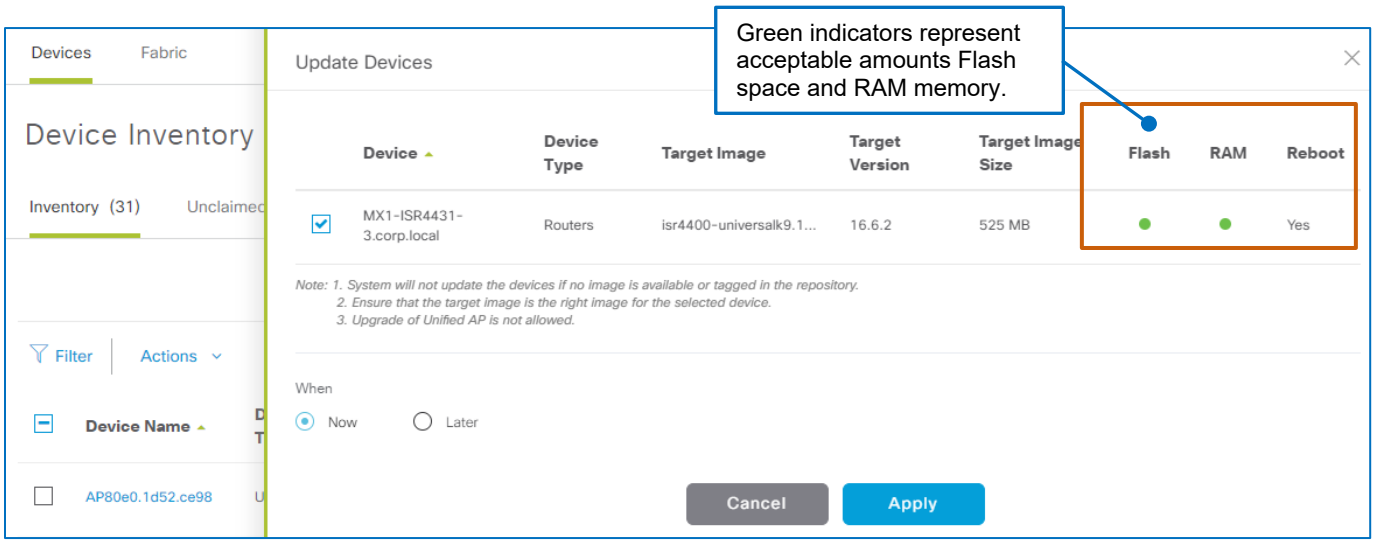
   This action makes the **Actions** drop-down list available.



2. In the **Actions** drop-down list, select **Update OS Image**.

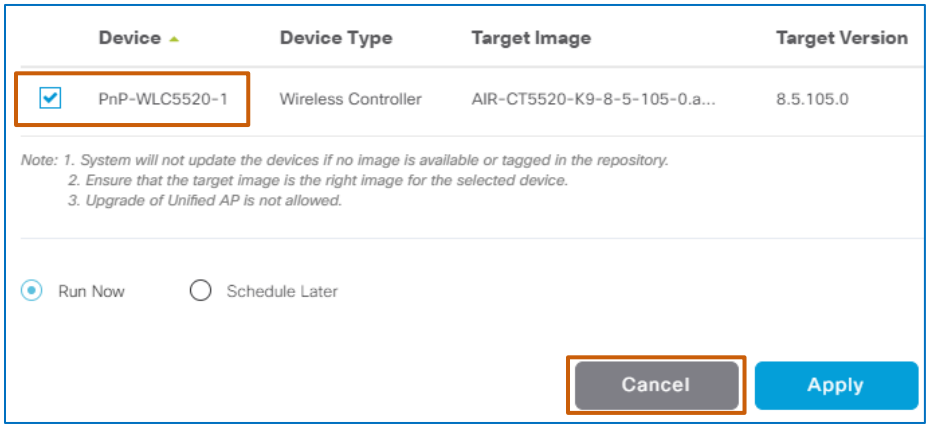


The **Update Devices** panel opens. The panel lists each device that you selected and indicates whether each device has enough Flash space and RAM to support the upgrade, and whether the device will reboot to complete the upgrade process.



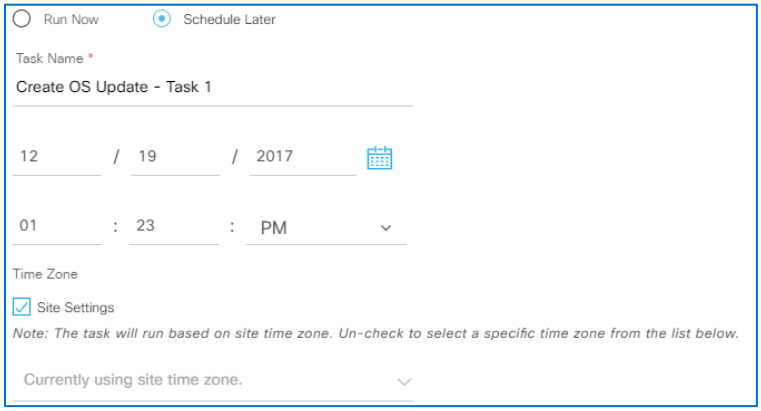
3. On the **Updated Devices** panel, in the list, to determine whether each device contains enough Flash space and RAM to support the upgrade, review the **Flash** and **RAM** columns, and:
   - When green color code appears for both items, which indicate enough Flash space and RAM, the system can upgrade those devices.
   - When a red indicator appears for either item, and you proceed with the upgrade, the system does not attempt to upgrade those devices.
4. Determine whether you want to continue initiating the upgrade process.
   - To continue, go to step 6.
   - To cancel the upgrade, go to step 5.

5. To cancel an upgrade on a device:
   - For a single device, in the **Panel**, click **Cancel**.
   - In a series of devices, beside each device that you determine not to upgrade, clear the check box beside the device name.

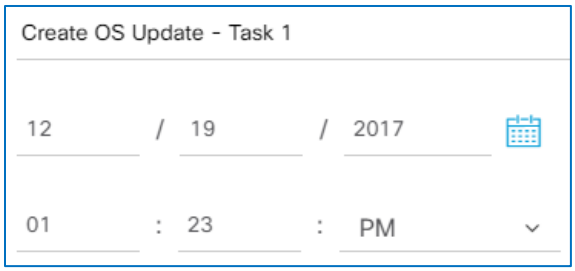


6. To schedule the upgrade task:
   - To run the upgrade immediately, accept the default selection of **Run Now**, and the go to step 8.
   - To schedule the upgrade to occur at a specific time, click **Schedule Later**, and then go to step 7.

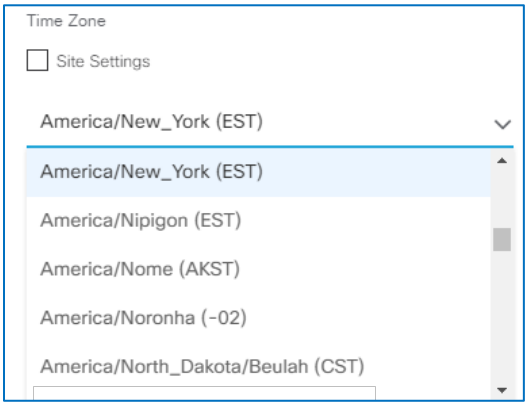
     The **Create OS Update** section expands.



7. To define the upgrade schedule:
   a. In the date and time fields, type or select the date and time that you want the system to perform the upgrade based on the time zone that you select in step 7b.



   b. To indicate the time zone that the system applies to the time and date:
      - To accept the time zone that a system user applied to the device's location when designing the network, accept the default selection of the **Site Settings** check box, and then go to step 8.
      - To select a different time zone, clear the **Site Settings** check box, in the drop-down list, select the time zone, and then go to step 8.



8. To continue the upgrade process, click **Apply**. The **Updated Devices** panel closes automatically.

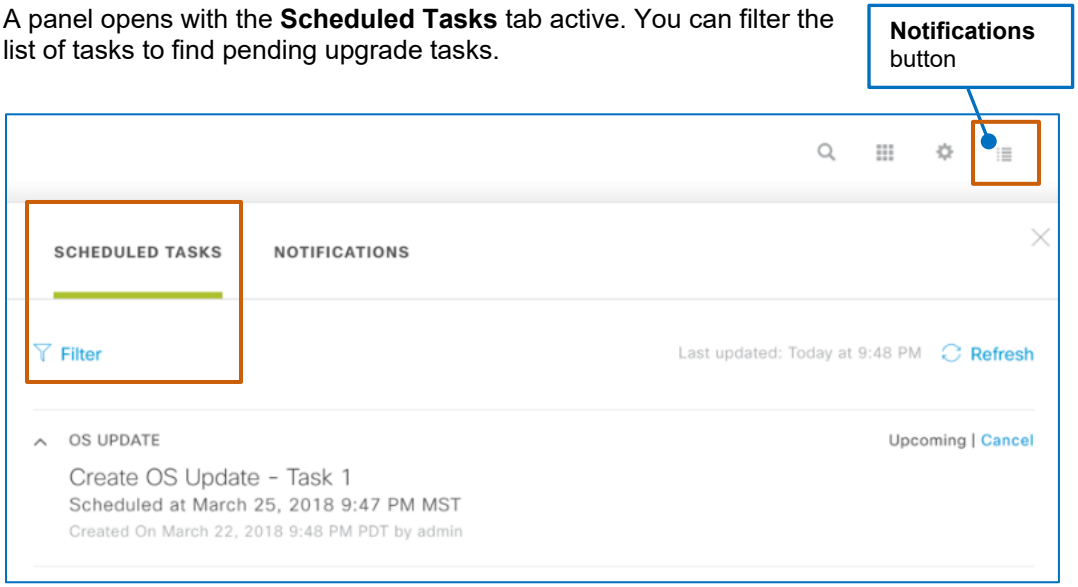
   When you run the task immediately, the system initiates it when you click **Apply**.

   When you schedule upgrades to occur at a later time, for example, during a maintenance window, the system adds the task to the **Scheduled Tasks** list.

   Tip: To see the list of scheduled tasks:

   - On the application toolbar, click **Notifications**.

   A panel opens with the **Scheduled Tasks** tab active. You can filter the list of tasks to find pending upgrade tasks.



9. To monitor the progress of the upgrade task and review the upgrade results, on the toolbar, go to task 5.

Task 5: Monitor the Upgrade Task and Review Results

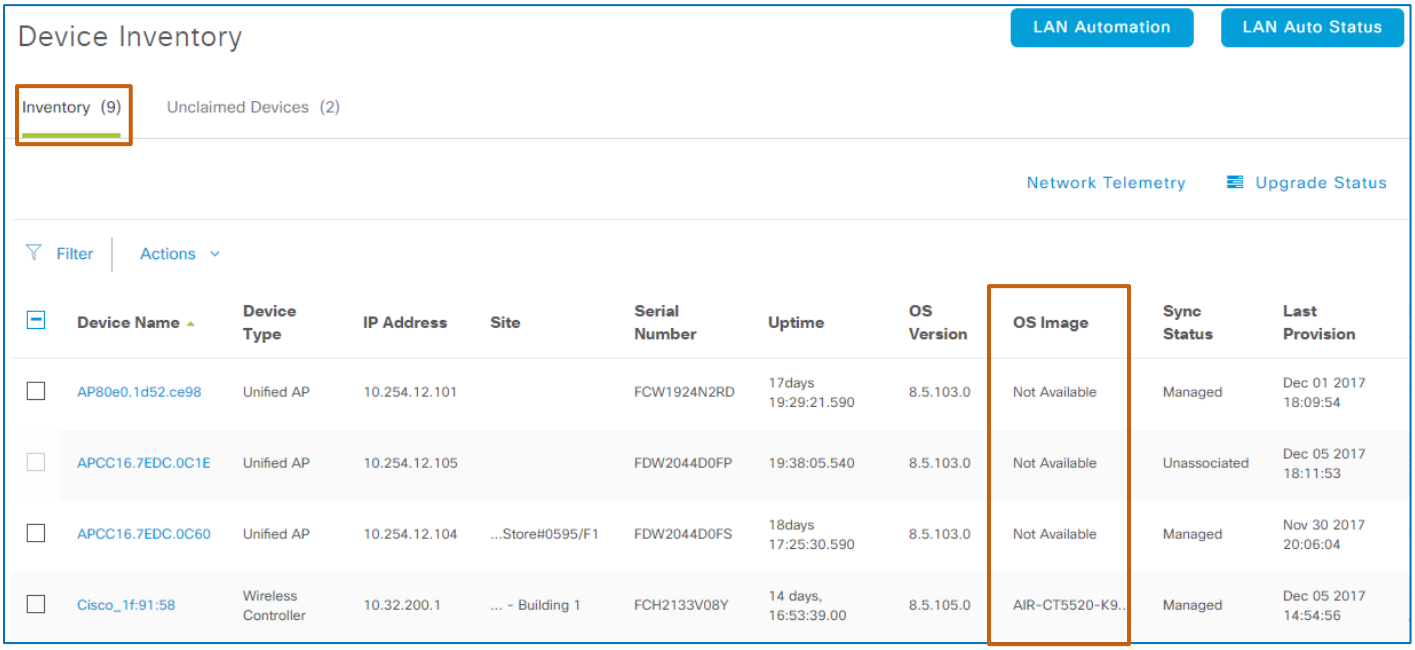
You can monitor upgrades while they are running and review the results to determine whether the upgrade process is successful, in progress, experiencing issues, or failing.

To monitor an upgrade task and review its results, follow these steps:

1. On the **Inventory** subtab:
   - To determine whether the **Outdated** status appears or has been removed from the devices receiving the upgrade, on the **Inventory** tab, review the device list.

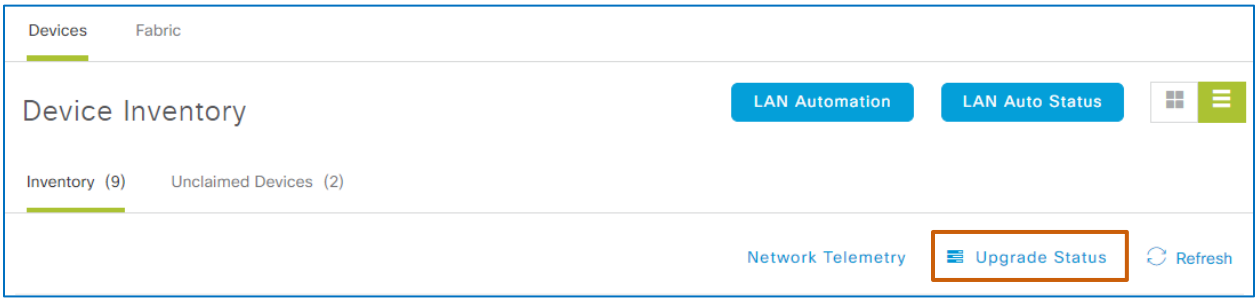
     When the **Outdated** status no longer appears in the **OS Image** column below the image name of the upgraded device, the upgrade is complete and successful.

     You have completed the software image management process.



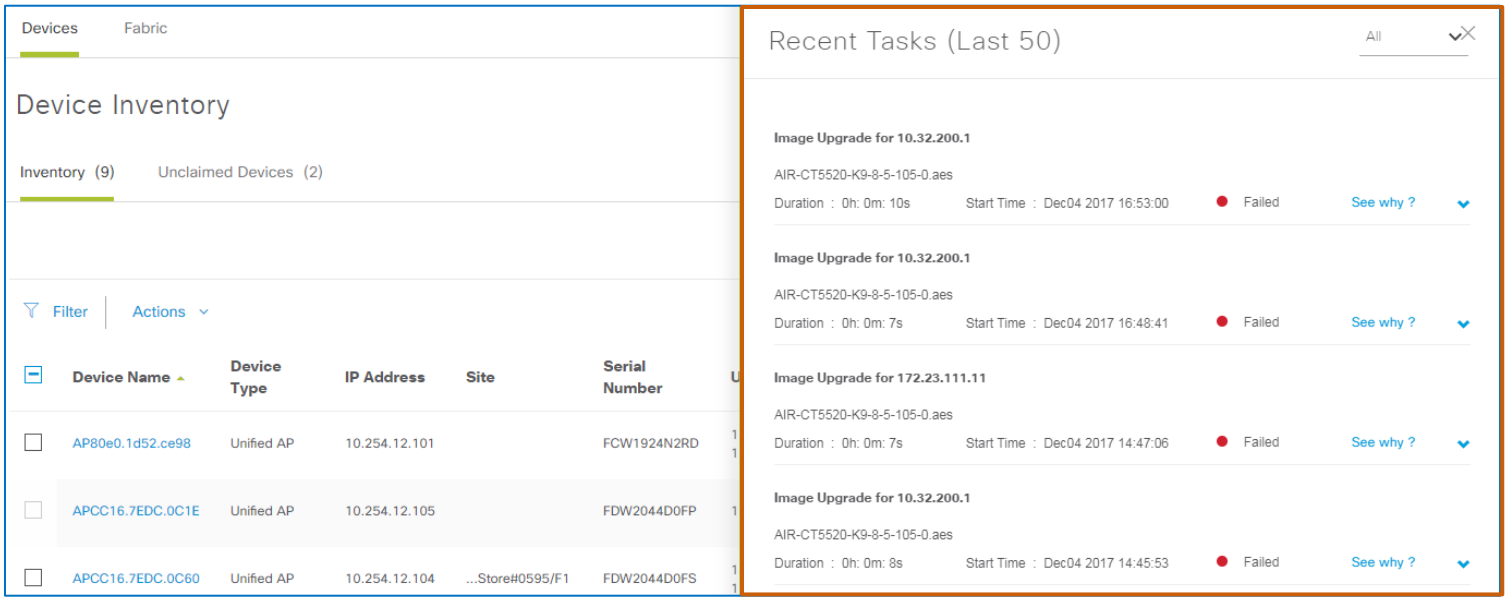
OR

   - On the toolbar, click **Upgrade Status**, and then go to step 2.



The **Recent Tasks** panel opens and lists each device on which an upgrade task is running or has been run.

Note: When more than one device is included in an upgrade task, the system updates each device's status when its upgrade process is complete.

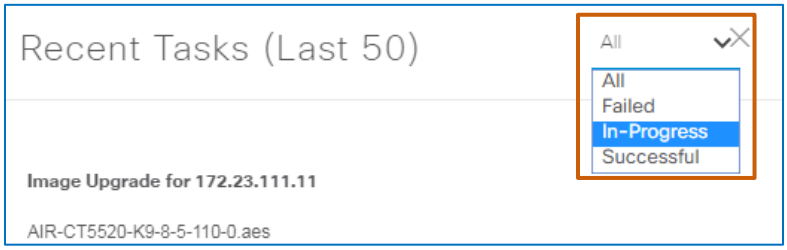


2. In the panel, review the list of devices and their upgrade statuses, including:
   - **Successful**
     Indicates that the upgrade is complete and the device is running the golden image or SMU
   - **In-Progress**
     Indicates that the system is in the process of upgrading the device
   - **Failed**
     Indicates that during the upgrade process, an issue has occurred and the upgrade is not completed

Tip: You can filter the list to see only those tasks that are currently running.

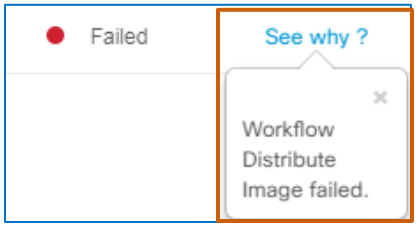
To filter the list:

- In the **All** drop-down list, select **In-Progress**.



3. To review task details:
   - For **Successful** statuses, go to step 4.
   - For **In-Progress** statuses, go to step 4.
   - For **Failed** statuses, click the **See why ?** link.

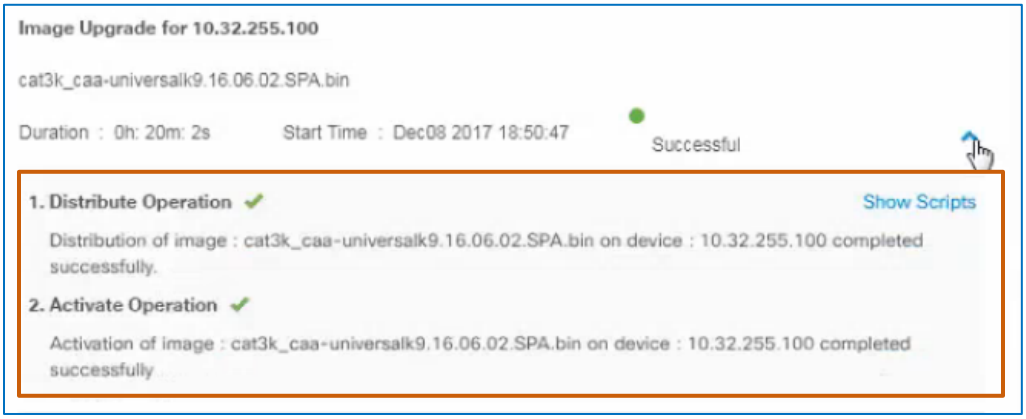
     A pop-up window opens with a synopsis of the issue.



4. To see more information on a status or to review the scripts that the task ran, or review the commands that the task ran, to the right of the row, click the down arrow.

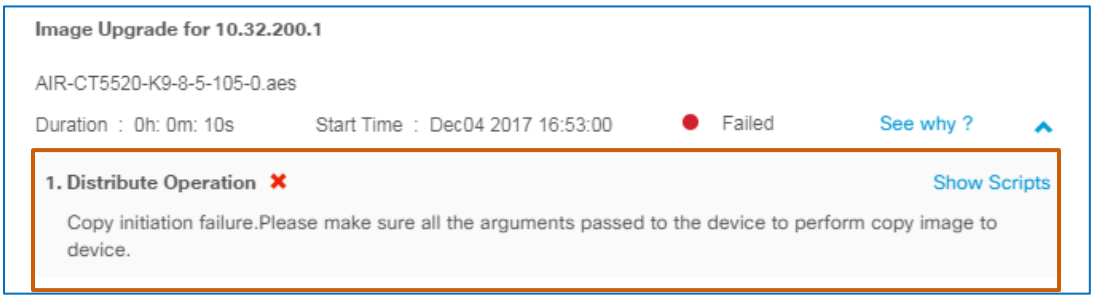
   The panel expands to display more information.

   In successful upgrades, the details indicate the results of the distribution and activation operations that the task runs.



   For upgrades that are in progress, beside each device, the details indicate the operations that are pending or complete on the device as part of the upgrade process.

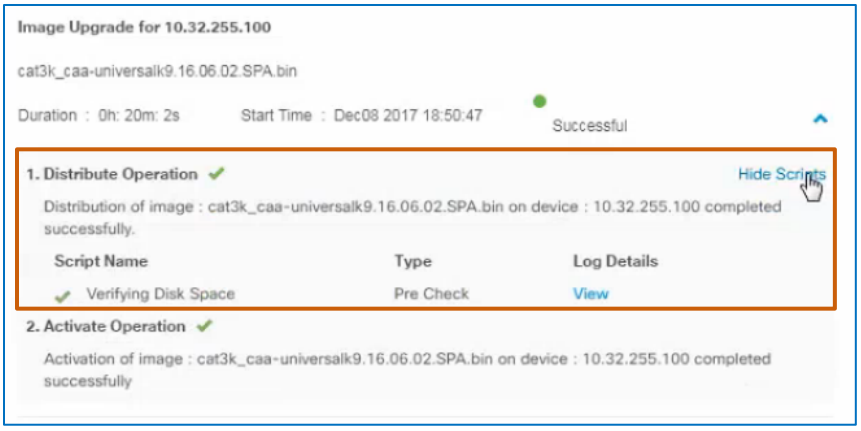
   In failure situations, the details indicate the point at which the failure occurred and suggestions that might correct the issue.



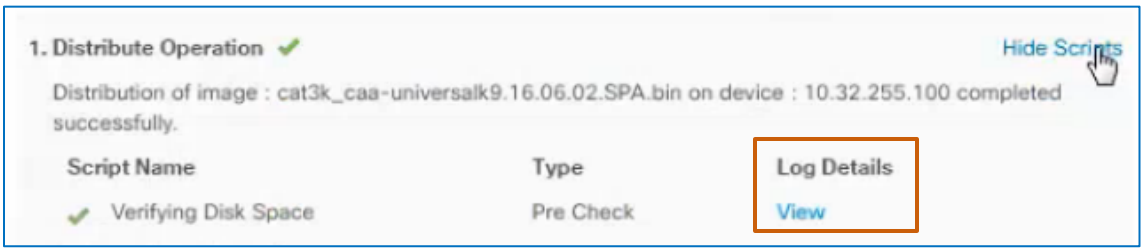
   a. To see the scripts that the system ran during the upgrade process, click **Show Scripts**.

Note: Scripts are available for image and SMU upgrade distribution tasks and for SMU upgrade activation tasks.

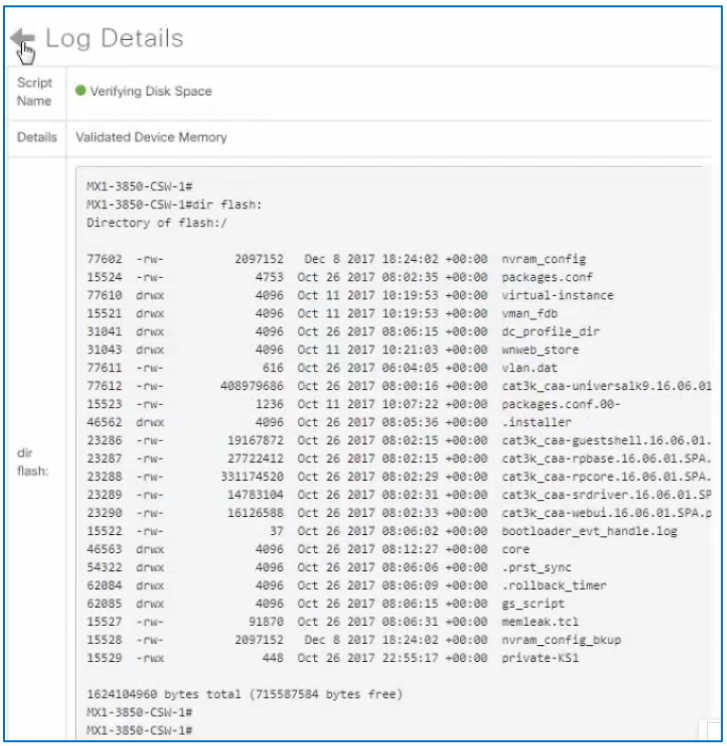
The section expands to display the script information.



i. To see detailed information, below **Log Details**, click **View**.

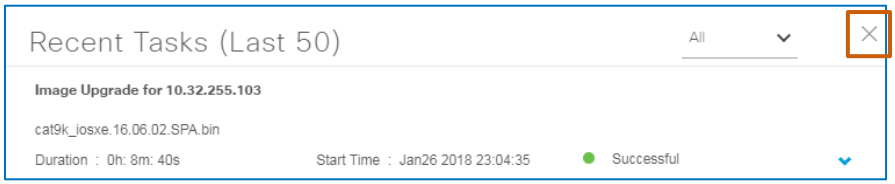


The panel toggles to display **Log Details**.



ii. To close the log details, click the arrow icon.

b. On the **Recent Tasks** panel, click close.



You have completed the process to manage device software images in Cisco DNA Center.

Links

To Product Information

Visit the Cisco Web site to learn more about Cisco DNA Center.

Visit the Cisco Web site to review or download the **Cisco Digital Network Architecture Center User Guide, Release 1.1**.

To Training

Visit the Cisco Web site to access other Cisco DNA Center learning opportunities.

Visit the Cisco Web site to access learning opportunities for other Cisco products.

To Contact Us

Send us a message with questions or comments about this training.

Note: Please send messages that address the training content only.

Follow your regular business process to request technical support or address technical or application-related questions.