Managing Device Software Images

Cisco DNA Center 1.2.8 Training

Copyright Page

Managing Device Software Images

Contents

Want More?

What Should I Know Before I Start?

Why These Tasks Are Important

They Help Ensure Expected Device Behaviors, Consistency, and Security

Various events can require you to upgrade or apply corrections to device software images, such as:

- The release of a new feature or technology that the current running image does not support.
- PSIRT alerts that notify you of security issues.
- The need to standardize device images among devices in a family or at a specific location.
- End-of-life notifications.

Cisco DNA Center provides the following image management functions so that you can keep devices up-to-date and running optimally and as expected:

- Importing device software image or add-on packages, when needed.
- Standardizing software images and add-on packages for device families and locations.
- Reviewing automated audit results to determine device compliance with standardization.
- Evaluating the readiness of devices to receive image upgrades or add-on packages.
- Upgrading devices and evaluating the upgrade results after distribution and activation.

Note: You can perform software image and add-on package upgrades on devices that Cisco DNA Center manages only.

Cisco DNA Center lists and, after importing, stores device software images, and, through an image standardization process, makes them available for device provisioning. Cisco DNA Center also stores add-on packages, which are updates to running software images. Add-ons provide the ability to respond to changing conditions, such as security issues, quickly and with minimal operational impact.

Configuration Change: When you perform upgrades, the process inherently makes the device configuration changes that the new running image or package requires.

In some cases, devices also must reboot to begin running the new image.

To help ensure device consistency, you can standardize device software images and validate that device images comply with those standards proactively. Standardization also helps to ensure that devices have the features, technologies, and security or other critical fixes, that you expect.

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

- Flexible and granular organization of software images and image add-ons.
- Automated device auditing to determine compliance with defined image standards.
- An upgrade process that applies the standards and separates the distribution and activation tasks.

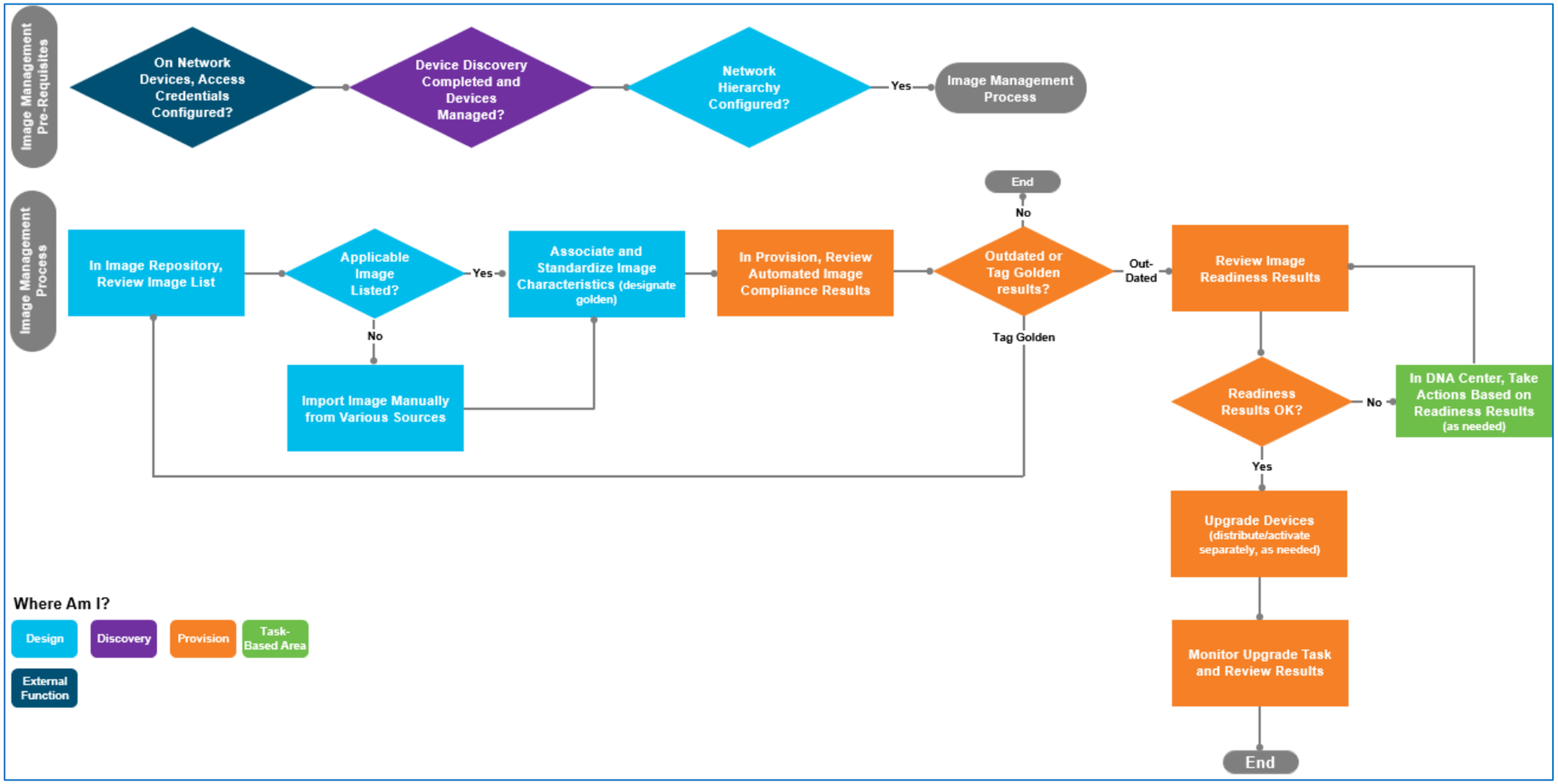
This training addresses key concepts for effective image management and the tasks that you perform to:

- Import and standardize images
- Evaluate audit results to determine device compliance with image standards
- Evaluate device readiness to receive upgrades
- Upgrade devices and evaluate upgrade results

Important Note: The functionality that you can see and the tasks that you can perform depend on the system's licensing and configuration and on your system user role.

The Image Management Process Flow Diagram

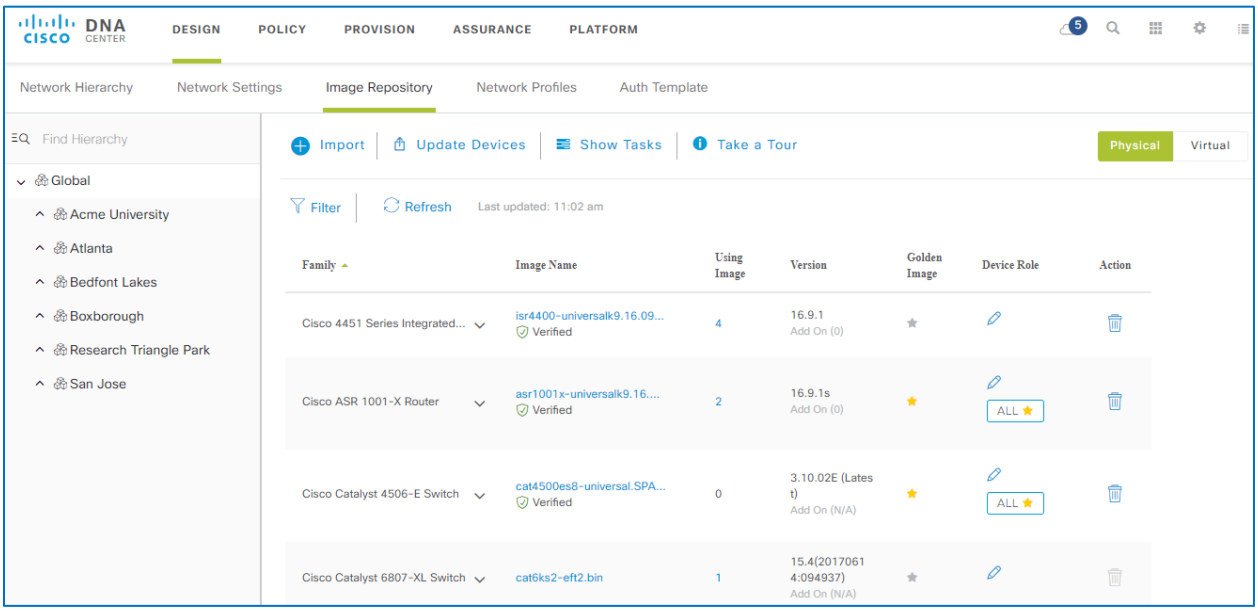
Tip: For optimal legibility, set the PDF zoom level to 100%.



What I Will See in the Image Repository

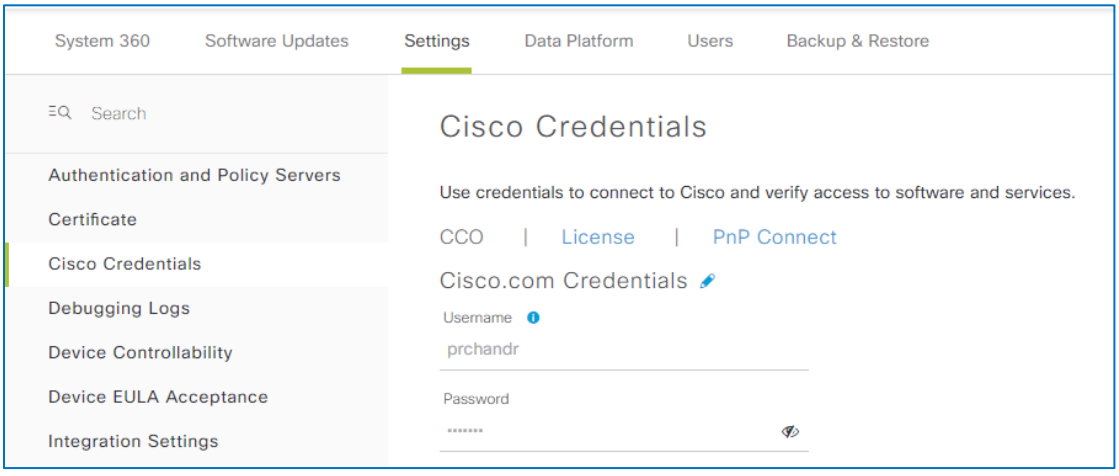
Physical, Virtual, and Add-On Images and Image Distribution

The **Image Repository** lists images and add-on packages based on its connectivity to Cisco.com.



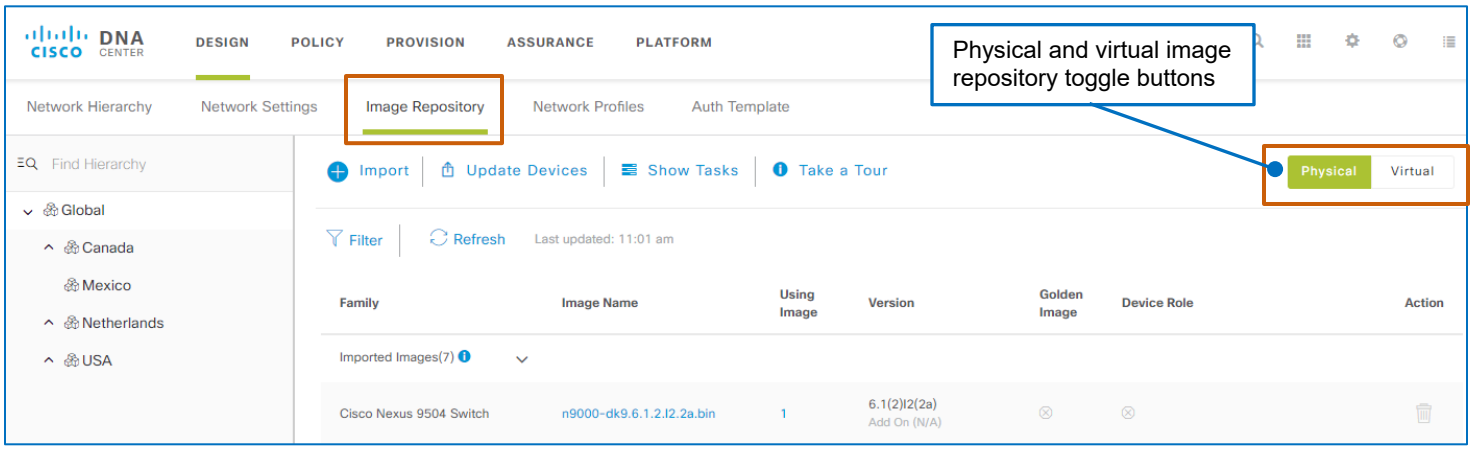
When Cisco DNA Center is online with Cisco.com, it organizes images in their applicable device families.

Note: To enable system connectivity, an administrator must configure Cisco.com credentials in the Cisco DNA Center system settings.

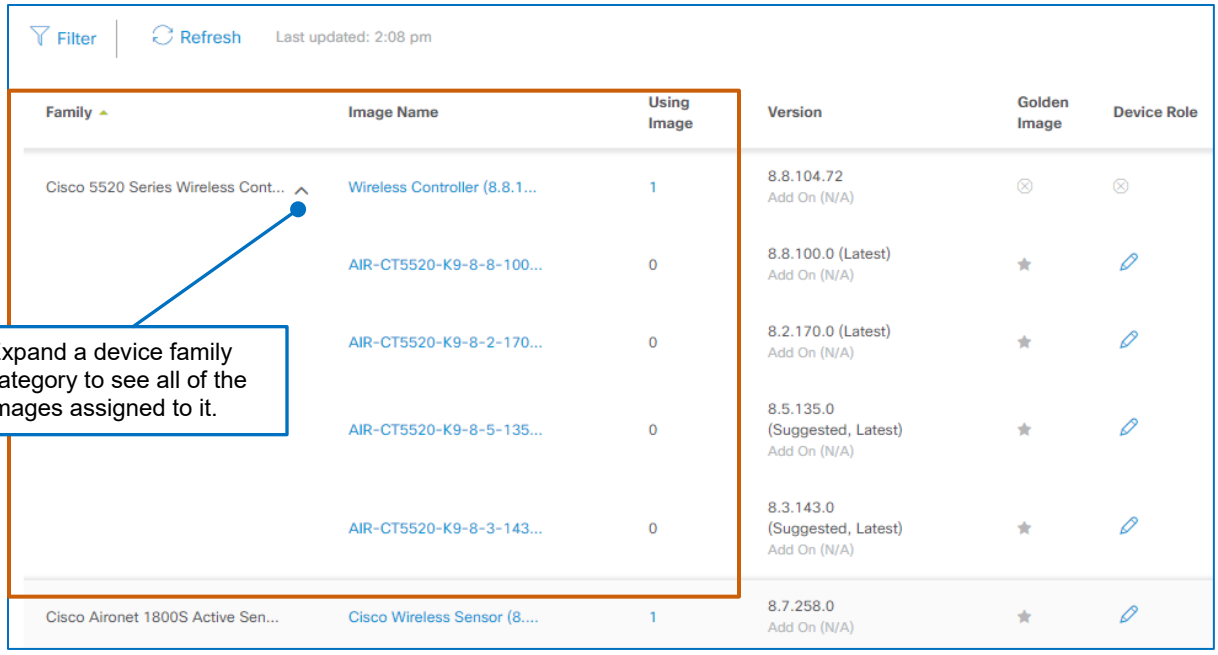


When Cisco DNA Center is not online and you import images, it lists all of the device families. In these cases, you must determine and assign images to their applicable devices family and models.

The page lists the images that are available for physical devices, by default, and provides access to images for virtual machines.



To see all of the images and add-ons assigned to a device family, you can expand the category.



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

Image Name	Using Image	Version
Wireless Controller (8.8.1...	1	8.8.104.72 Add On (N/A)
AIR-CT5520-K9-8-8-100...	0	8.8.100.0 (Latest) Add On (N/A)
AIR-CT5520-K9-8-2-170...	0	8.2.170.0 (Latest) Add On (N/A)
AIR-CT5520-K9-8-5-135...	0	8.5.135.0 (Suggested, Latest) Add On (N/A)

This way, you can determine whether the repository contains the image or add-on that a device requires. If the image or add-on 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 them with the image name of unknown.

Image names also can have indicators next to them to emphasize their statuses, as follows:

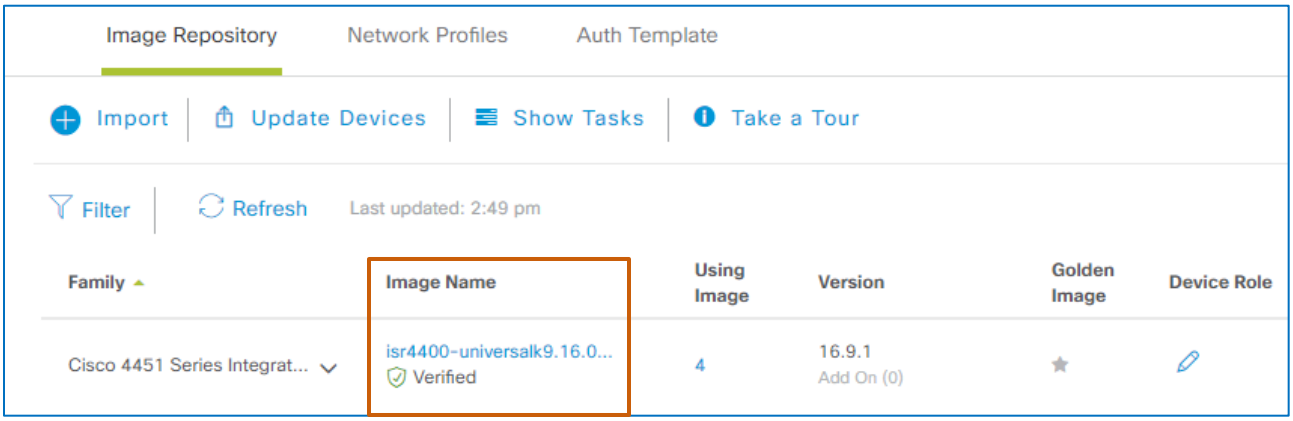
- **Suggested**
  Cisco recommends using the image or add-on for optimal results with demonstrated stability
- **Latest**
  The most recently released image or add-on
- **Suggested, Latest**

Cisco Aironet 1800S Activ...	Cisco Wireless Sensor (...	1	8.7.258.0 Add On (N/A)
Cisco ASR 1001-X Router	asr1001x-universalk9.16... Verified	0	16.6.4 (Suggested) Add On (0)
Cisco ASR 1002 Router	asr1000rp1-adventerpri...	1	03.17.04.S Add On (0)
Cisco ASR 1002-X Router	asr1002x-universalk9.03...	1	03.16.02.S Add On (0)
Cisco ASR 1004 Router	asr1000rp2-ipbasek9.03... Verified	0	3.02.01S (Latest) Add On (0)

Image Integrity Verification to Help Ensure Device Security

To support device security, Cisco DNA Center verifies that the software images in the image repository are authentic and valid when system users initially import images into Cisco DNA Center. When images meet Cisco-defined requirements, the **Image Repository** indicates a **Verified** status below the image names.

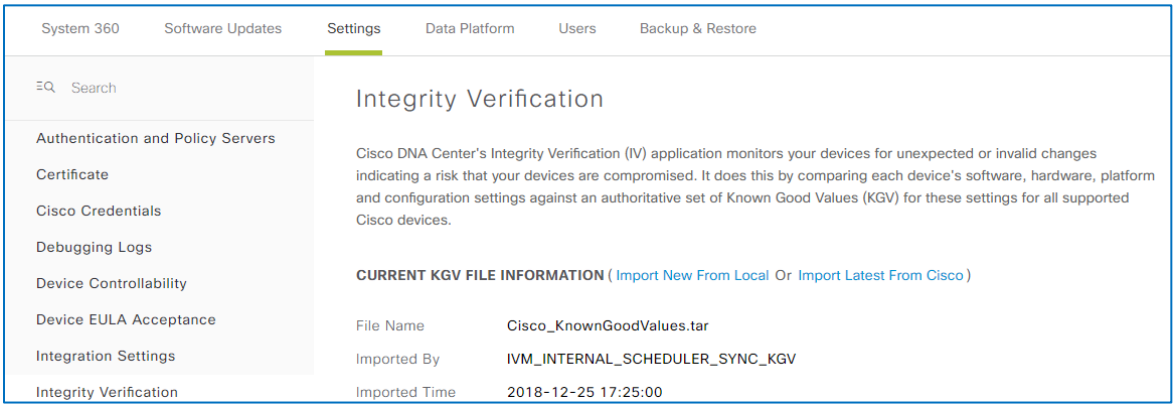
Note: The system does not validate the integrity of add-on packages.



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.

Note: A system administrator downloads the KGV file to Cisco DNA Center as an initial system configuration task.

After that, Cisco DNA Center downloads the file automatically every 7 days.

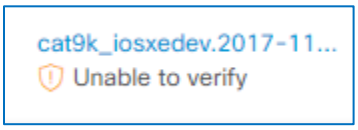


For more information, refer to the **Cisco Digital Network Architecture Center Administrator Guide**.

Important Note: Cisco DNA Center does not perform a subsequent image integrity validation when an updated KGV file uploads to the system.

To reverify integrity, you need to delete the image from the image repository and import it again.

When an image is not captured in the KGV file, the comparison result indicates a status of **Unable to verify**.



You can use images with an **Unable to verify** status.

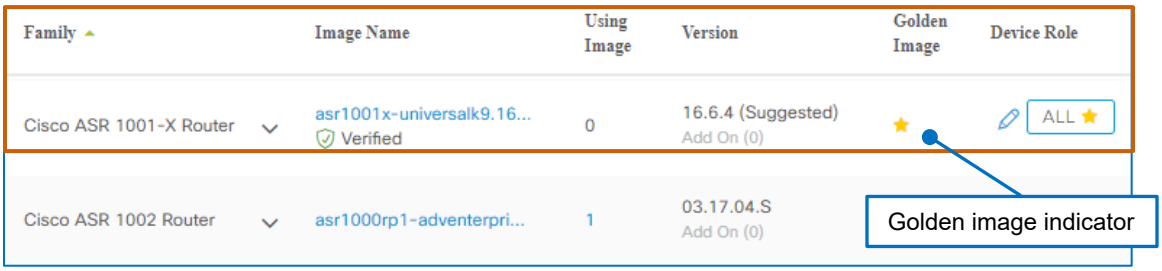
Caution: While the **Unable to verify** status does not necessarily indicate that there is an issue with the image, be aware that Cisco cannot ensure its integrity.

When the image checksum values do not match, file tampering or corruption has occurred, and the system deletes the image automatically on import.

Access to Importing Images

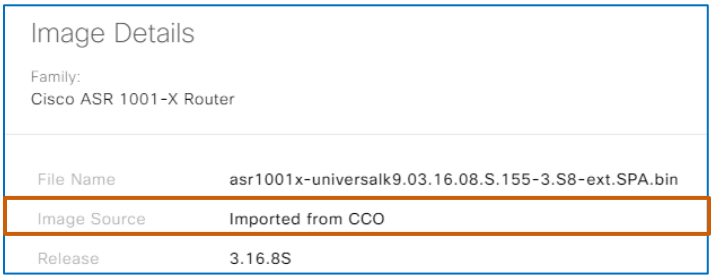
The Image Repository lists the device software images and add-ons that are available for download or already downloaded. To make images available for the device upgrade process, they must be imported into the repository, which can occur automatically or manually.

Designating an image or image and add-on combination as golden can start an automated import process from either a device or from Cisco.com.

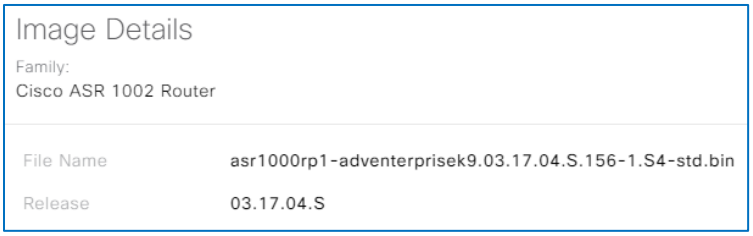


You can determine whether the system will download the image from a device or from Cisco.com by opening the detailed image information.

The **Image Source** field indicates from where the download will occur.

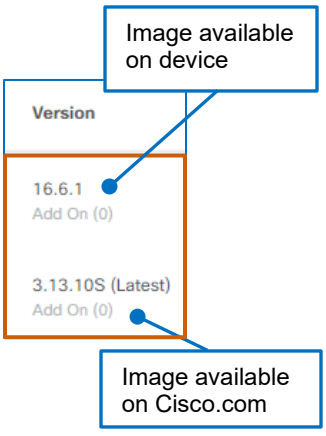


When downloading from a device, the panel does not indicate an image source.



Or, in the **Version** column, when the image version includes a description, such as **Suggested** or **Latest**, the system will download the image from Cisco.com.

When there is an image version with no description, the system will download the image from the device.

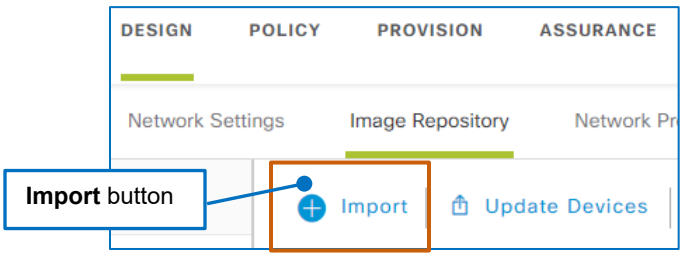


Note: The system cannot download image files from wireless LAN controllers (WLCs).

You must import WLC images manually.

You can import an image or add-on file manually from:

- Cisco.com
- A locally-stored file
- A supported file server.

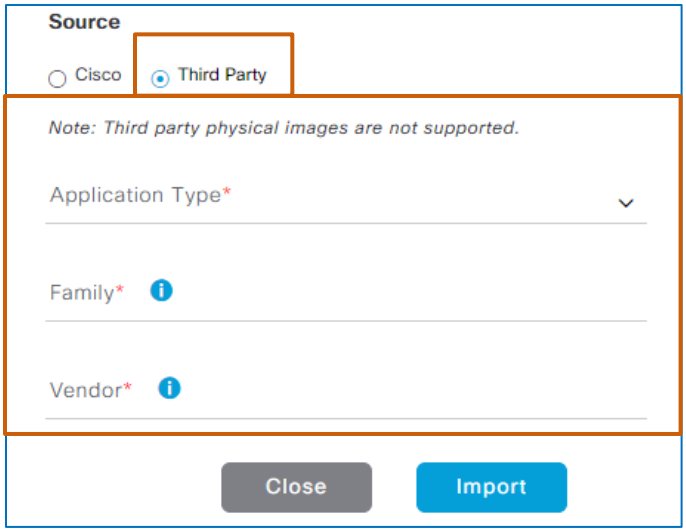


Note: You cannot import WLC or switch images manually when they are in install mode.

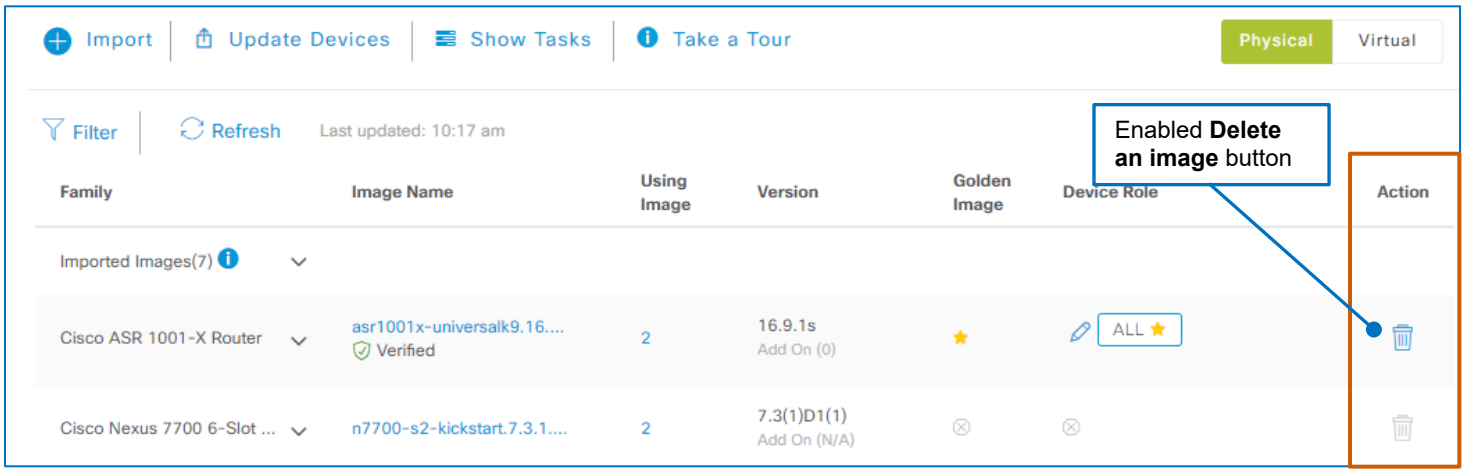
For virtual machines, you also can import third party vendors' software images manually when those images are compatible with Cisco Enterprise Network Function Virtualization Infrastructure Software (Cisco Enterprise NFVIS) for later provisioning on virtual machines.

Note: Cisco Enterprise NFVIS supports dynamically deploying virtualized network functions, such as a virtual routers, firewalls, and WAN acceleration, on supported Cisco devices.

For more information, refer to the current **Cisco Enterprise Network Function Virtualization Infrastructure Software Release Notes**.



When a software image is available for use by Cisco DNA Center, the **Delete an image** button is available as a link in the image's **Action** column.



The Standardized, Golden Image Characteristics and Process

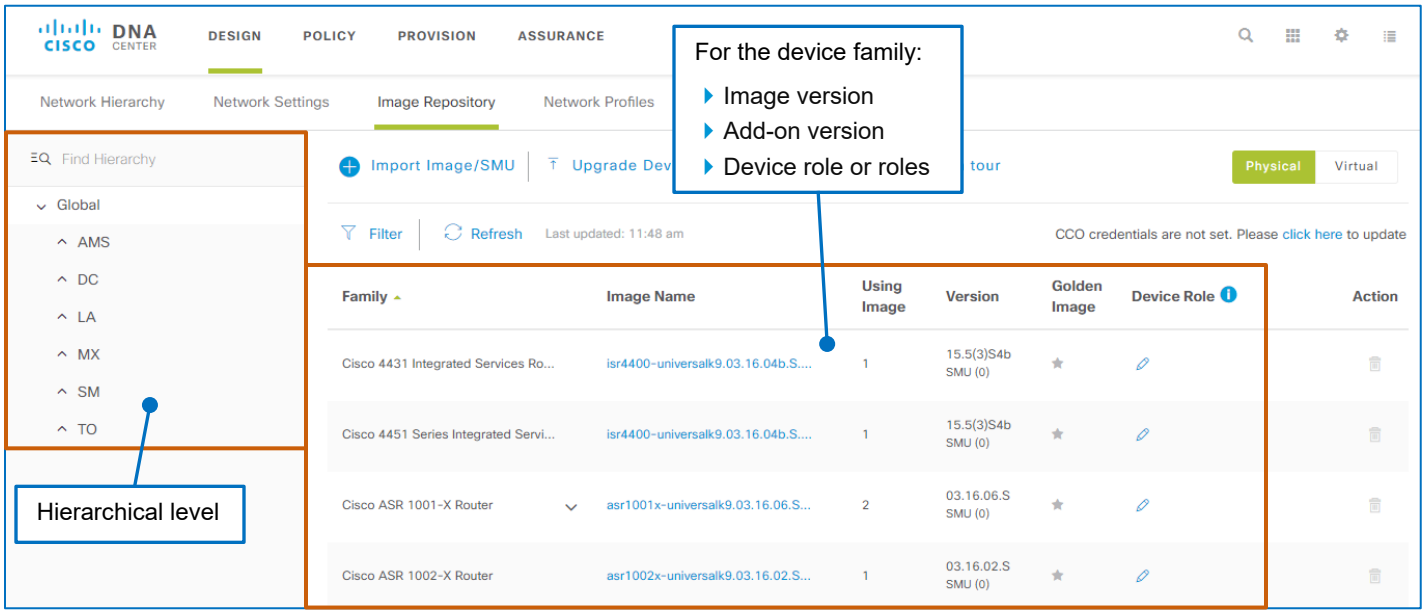
Determining the Business Intent and Designating Image Characteristics

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 add-on associated with the image that also needs to be distributed to ensure that the device has the features it needs and runs as expected?

You can indicate any combination of the following characteristics and designate, or mark, them as the standard, referred to as a golden image in Cisco DNA Center based on those characteristics:

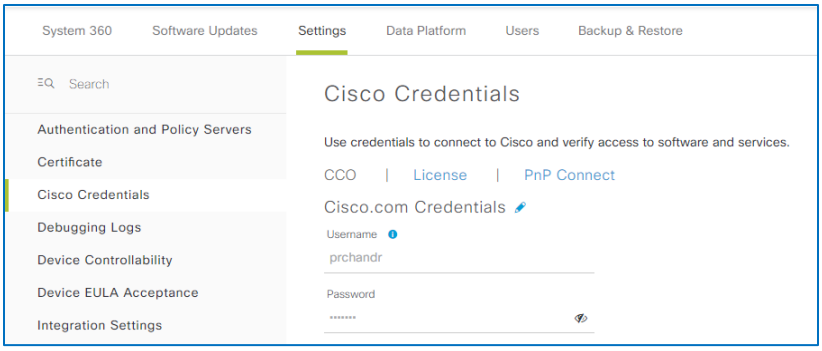
- Any level in the network hierarchy , including the overarching **Global** hierarchical level
- The device family
- The software image
- The applicable add-on that applies to the software image
- The role or roles of the devices on the network



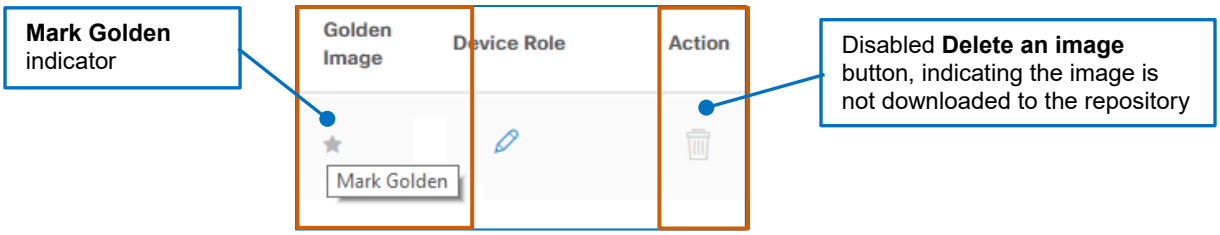
The Tagging Golden Action and the Import Process

When you indicate a standardized, golden image, and the image has not been imported previously, the action of clicking the **Mark Golden** indicator in the **Golden Image** column initiates the automated image import process from Cisco.com.

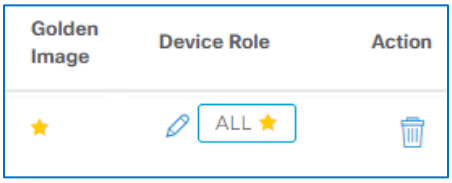
Note: To support automatic image imports, an administrator must configure Cisco.com credentials in the Cisco DNA Center system settings.



When an image is not in the repository, the **Delete an image** button in the **Action** column is unavailable.

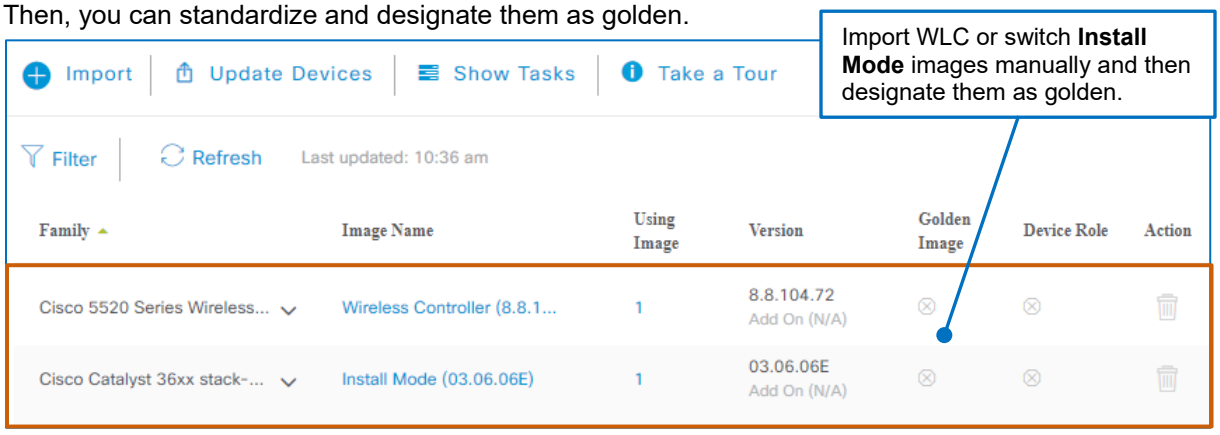


When the import is complete, the indicator displays yellow color-coding and the **Delete an image** button is available.



Note: You must import wireless LAN controller (WLC) or switch images with the **Install Mode** image name manually.

Then, you can standardize and designate them as golden.



The Golden Image Requirement for Device Image Auditing and Compliance

The system references the golden image designations in its automated image auditing and compliance process, allowing it to identify, and notify you of, devices matching the golden images characteristics that do not comply.

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

Important Note: Only image or image combinations that are designated golden are available to apply in the upgrade process, even when the image is available in the **Image Repository**.

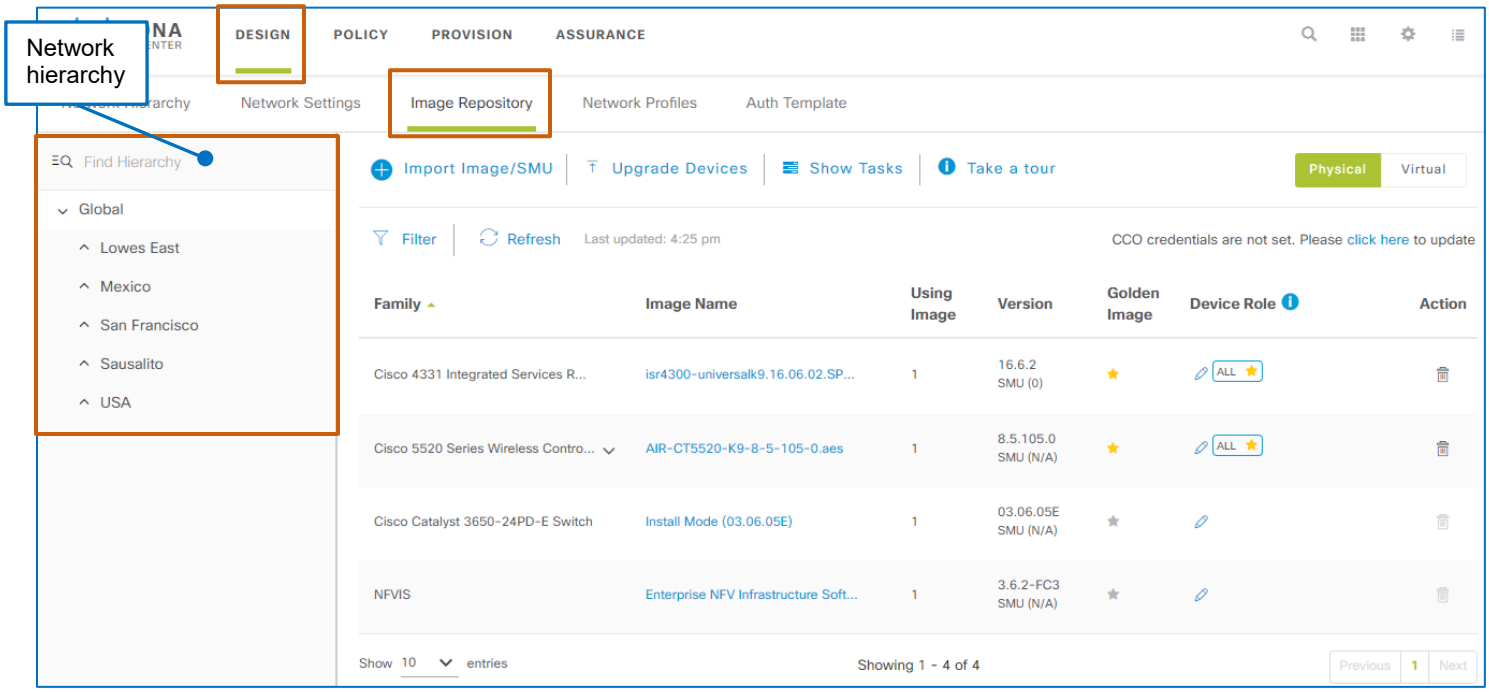
As device images, versions, and add-ons change, you can redefine image standards, as needed.

The Way That the Network Hierarchy Affects Image Upgrades

Inheritance Applies Standardized Images to Devices on Dependent Levels

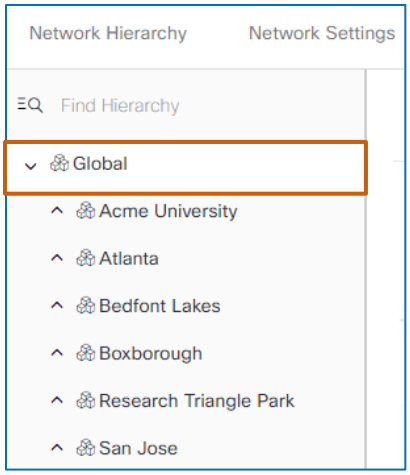
During network design, system users configure a network hierarchy, which arranges network devices by their geographical or organizational relationships and dependencies.

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

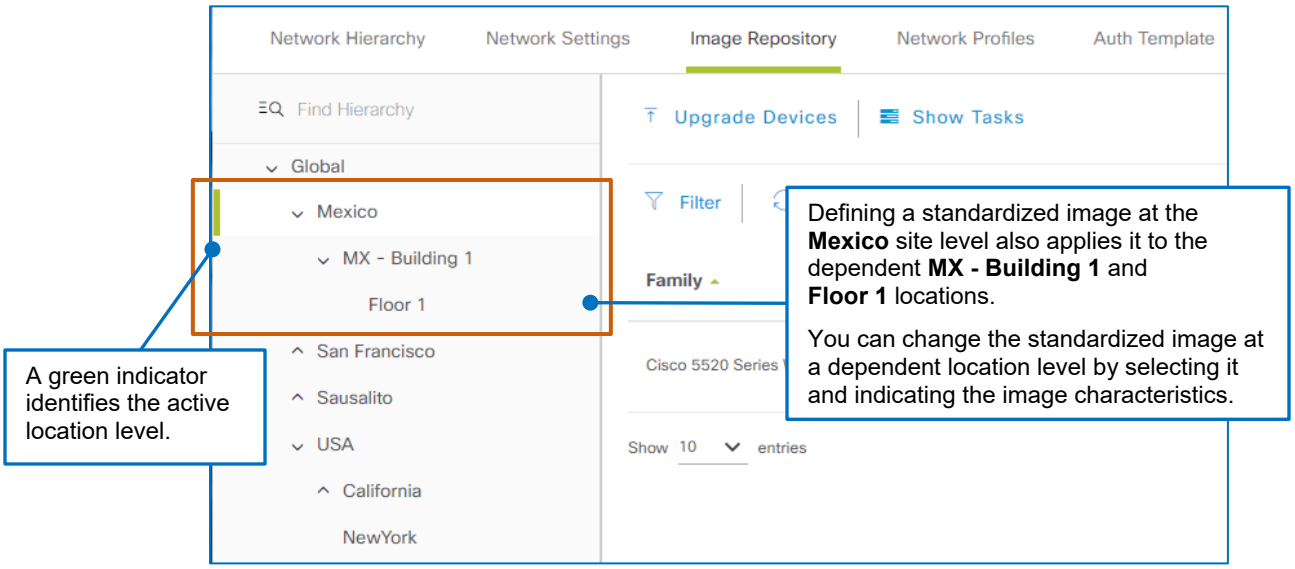


The system applies standardized images to the active location level that you select in the hierarchy, and to all of the dependent locations organized, in a parent/child relationship as long as that relationship is not broken.

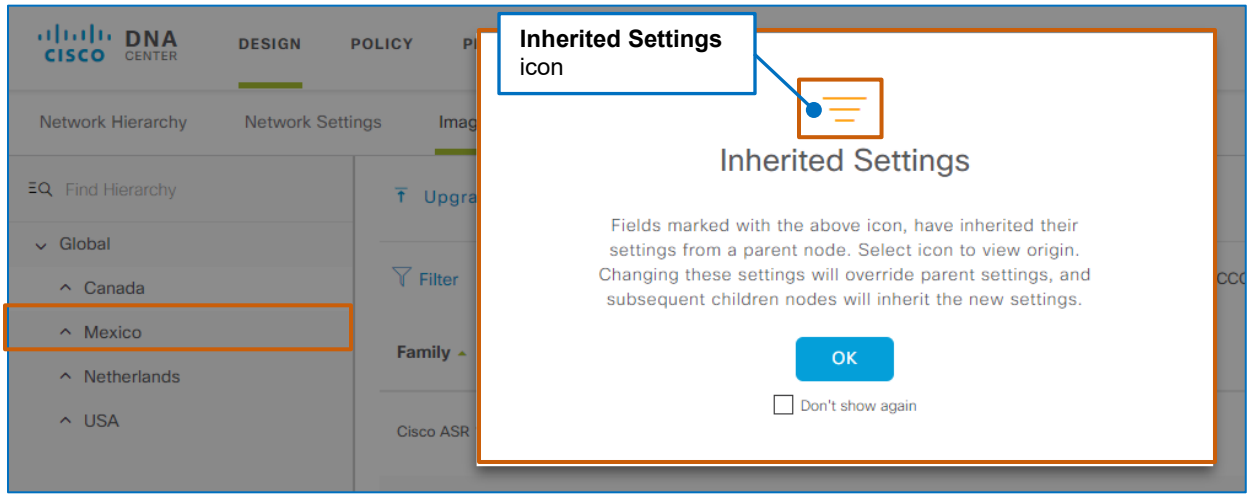
When you open the **Image Repository**, the system selects the **Global** level in the hierarchy by default. When system users organize other sites below the **Global** level, they initially have a child relationship and inherit the **Global** level characteristics.



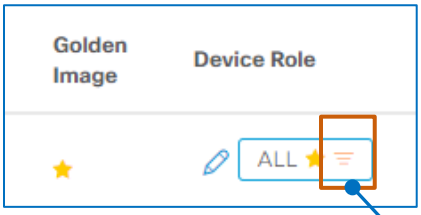
Then, you can define standardized images with varying characteristics and apply them at any level in the hierarchy based on operational requirements for the devices at that location.



When you click a dependent location that has inherited standards from a parent level, a system message opens indicating the inherited state.



As a visual indicator, the icon above the **Inherited Settings** heading also appears beside the device role indicator with settings inherited from a parent location.



Caution: When child sites have inherited hierarchical settings and a system user changes those standards at a higher level in the hierarchy, the system applies those changes to all of the dependent child sites.

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

If you need to change a standard, take note of any inherited standards at the child levels in case you need to reapply them because when you break a hierarchical relationship, you cannot reassociate that relationship subsequently.

The Way That Cisco DNA Center Determines Image Compliance with Standards

By Running an Automated Audit Process

When system users define standardized, golden images and add-ons, the system automatically audits all of the applicable devices for compliance with the standard.

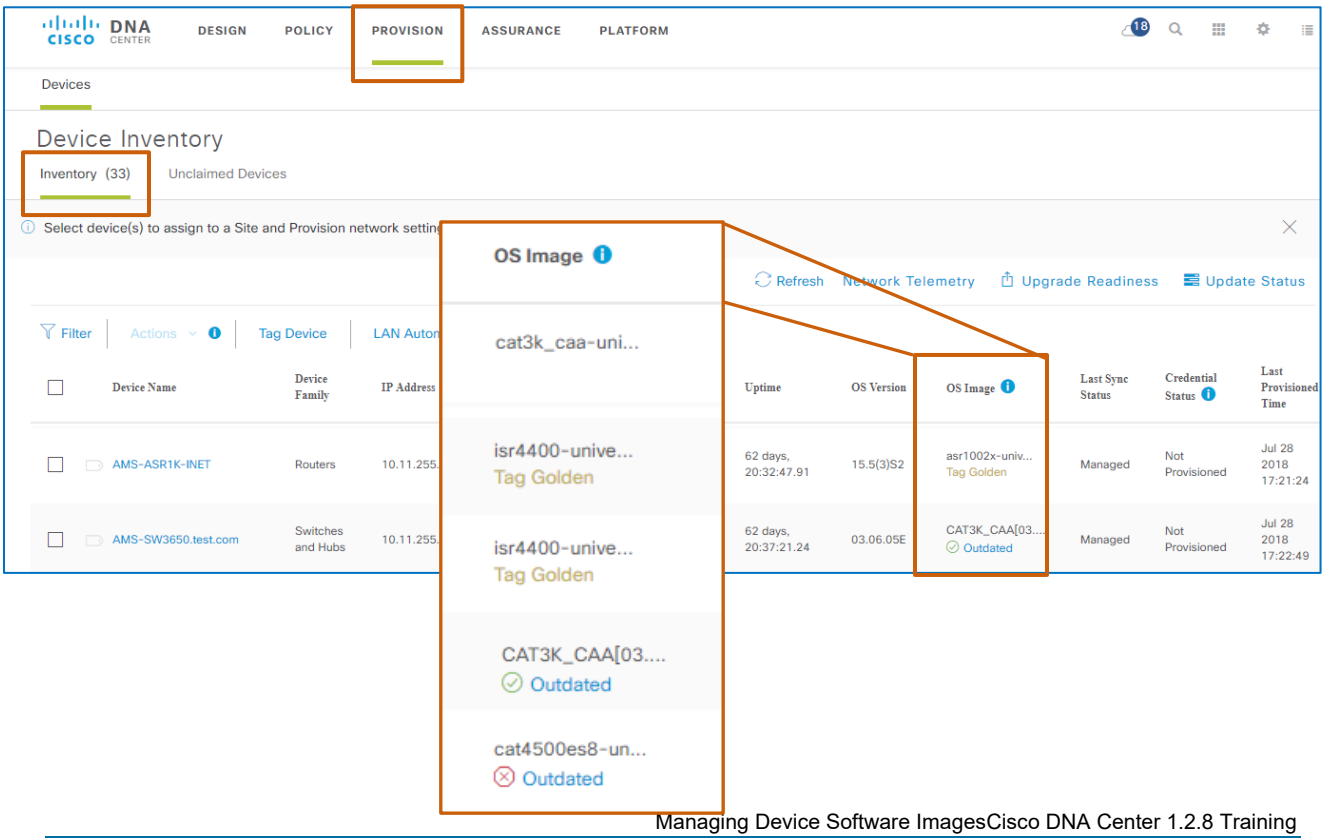
When the tagging golden action occurs in the **Image Repository**, the automated process compares the device's current running software image, which it captures during inventory collection, with the image and characteristics identified in the standardized, golden image and determines compliance.

Audits also occur automatically when the system begins managing new devices and indicates whether those devices are compliant or require a system user to designate a golden image that addresses device attributes.

Note: The system runs audits on only those device families for which system users have designated golden image standards.

When standardization is not configured, a **Tag Golden** indicator appears below the image name.

Audit and upgrade readiness results are available in **Provision**, on the **Inventory** tab, in the **OS Image** name column, under each image name.

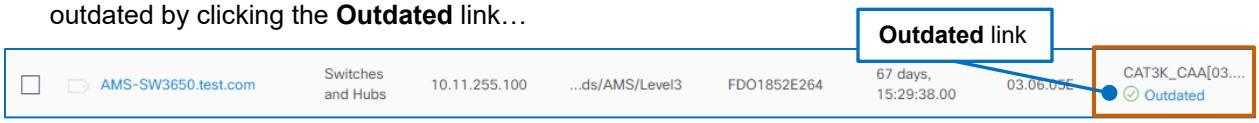


That Cisco DNA Center Evaluates Device Upgrade Readiness

By Evaluating Key Device Attributes Automatically and Presenting Results

Cisco DNA Center automatically determines and presents the status of various device attributes, which helps to ensure that distribution or activation can occur successfully.

In **Provision**, you can review readiness results for any device indicating that its running image is outdated by clicking the **Outdated** link…

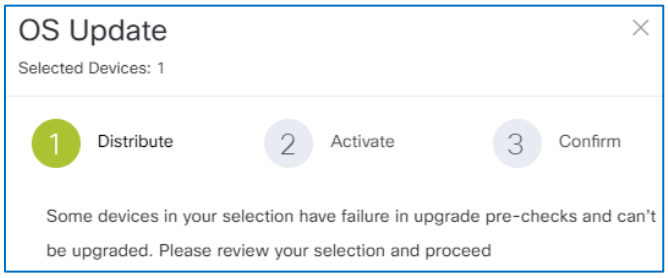


…and opening the **Image Upgrade Readiness Check** panel.

Upgrade readiness status indicators can include:

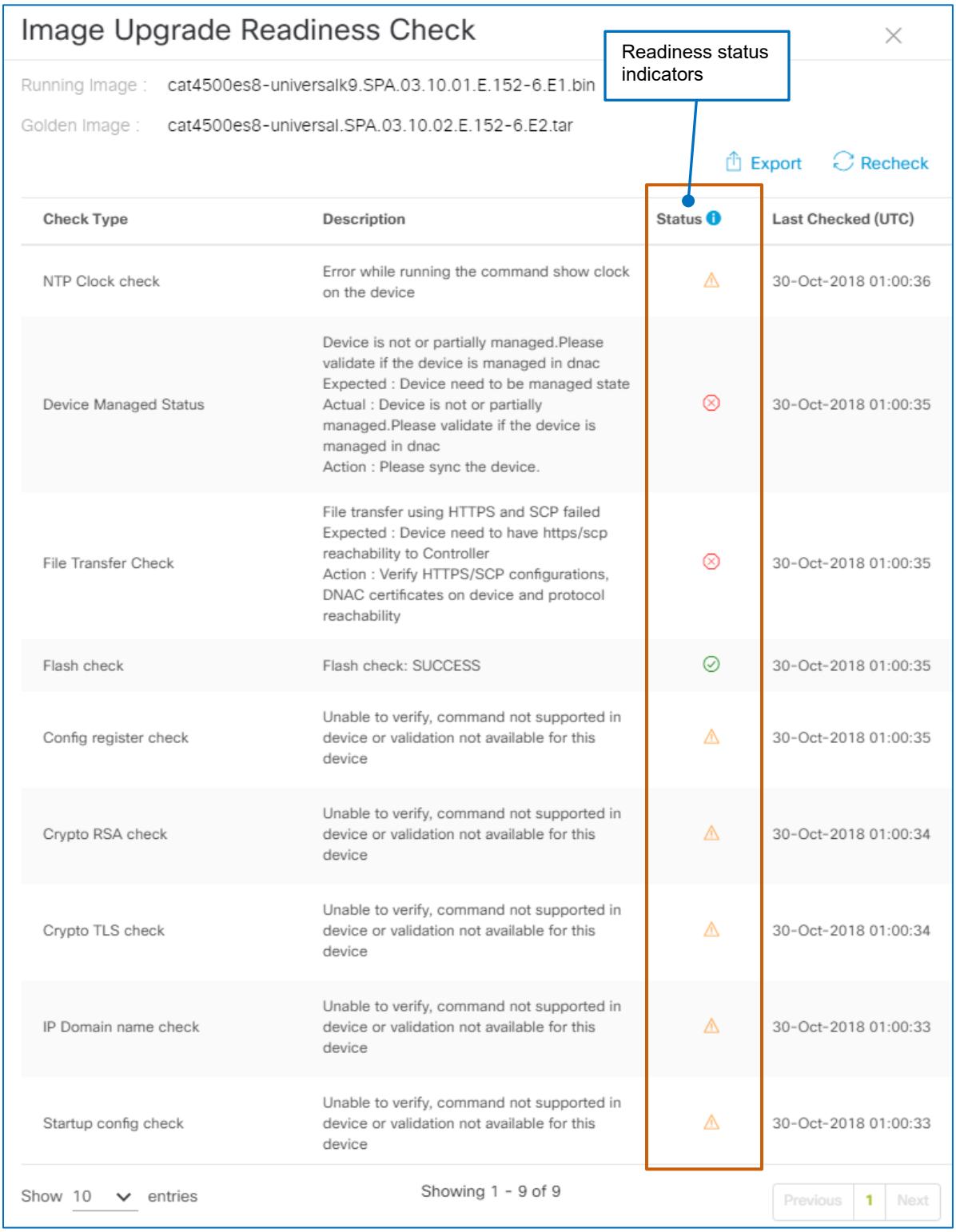
- Success
- Warning
- Failed

Important Note: When one or more of the validation tests returns a failure, you cannot upgrade the device.



The screenshot on the following page illustrates readiness check results.

The top of the panel indicates the current running image name and, when available, the standardized, golden image file name.



The device attributes that Cisco DNA Center evaluates to determine device readiness are:

- **NTP Clock Check**
  Synchronization of the device time and the Cisco DNA Center server time

  Time synchronization of the device and the server is required so that Cisco DNA Center can install its certificate on the device, which then enables its communication with that device. If either the device time or Cisco DNA Center server time is not synchronized, the test will fail.

  You must correct the synchronization issue before you can configure an upgrade.

- **Device Managed Status**
  Cisco DNA Center's active management of the device.

  Cisco DNA Center must be managing the device before you can configure an upgrade.

- **File Transfer Check**
  Device reachability by SCP or HTTPS, which Cisco DNA Center uses to distribute the image file to the device. When this test fails, you cannot continue with the distribution task.

- **Flash Check**
  Whether enough flash memory size is available for the device to accept the image file during distribution. When there is not enough memory available:

  - For devices that that support the ability for Cisco DNA Center to remove extraneous files, the evaluation presents a warning. If you continue with the upgrade, Cisco DNA Center will remove the extraneous files in an attempt to distribute the image.

    Tip: Cisco DNA Center records the files that it removes in the system audit logs.

  - For devices that do not support the ability to remove files, the evaluation presents a failure. You can remove extraneous file manually, and then return to the process.

- **Config Register Check**
  On devices with IOS or IOS-XE operating system, whether the configuration register value is set to support booting the image that you are activating

  The configuration register value controls the way in which the device boots. When set incorrectly, the device will not boot the image that you are activating.

  Caution: Although you can continue configuring an upgrade when this test indicates a warning, the device will not boot the image that you are activating, resulting in an upgrade failure.

  The device might still be running after the upgrade, but not with the image that you distributed and activated.

  For more information about how to identify and correct a configuration register value, refer to the **Use of the Configuration Register on All Cisco Routers Troubleshooting TechNote**.

  Note: A device's flash memory can contain more than one image.

- **Crypto RSA Check**
  Whether the device has the RSA configuration enabled, so that Cisco DNA Center can establish secure communication by using its RSA certificate

When RSA is not enabled on the device, the test presents a warning.

When an image that you need to activate is already available on the device, the device does not need the RSA configuration enabled. In this case, even though the test returns a warning, you can configure and run an activation only task.

Important Note: When you are configuring a distribution or combined upgrade task, the device must have the RSA configuration enabled and pass this test before you can continue.

- **Crypto TLS Check**
  Determines whether support for TLS (transport layer security) protocol version 1.2 on the device

  To establish an https tunnel between the system and the device and support its traffic, the device must be able to support TLS 1.2.

  When you have devices that cannot support TLS, the system reverts to SCP protocol to establish communication.

Note: Cisco DNA Center does not support TLS 1.1.

- **IP Domain Name Check**
  Whether the IP domain name is included in the RSA certificate key

  When generating RSA certificates, it is an industry best practice to include the IP domain name at the end of the key so that the system can validate its communication over that domain.

  When the domain name is not present, you can continue. In those cases, Cisco DNA Center will apply a self-generated certificate for communication.

- **Startup Config Check**
  Determines whether the device has a startup configuration

  When the device does not have a startup configuration, you need to take action to ensure that the device does have a startup configuration before you can continue. This requirement avoids upgrade failures or the necessity to start a device manually after an attempted upgrade.

You Manage Virtual Software Images by Following the Same Tasks

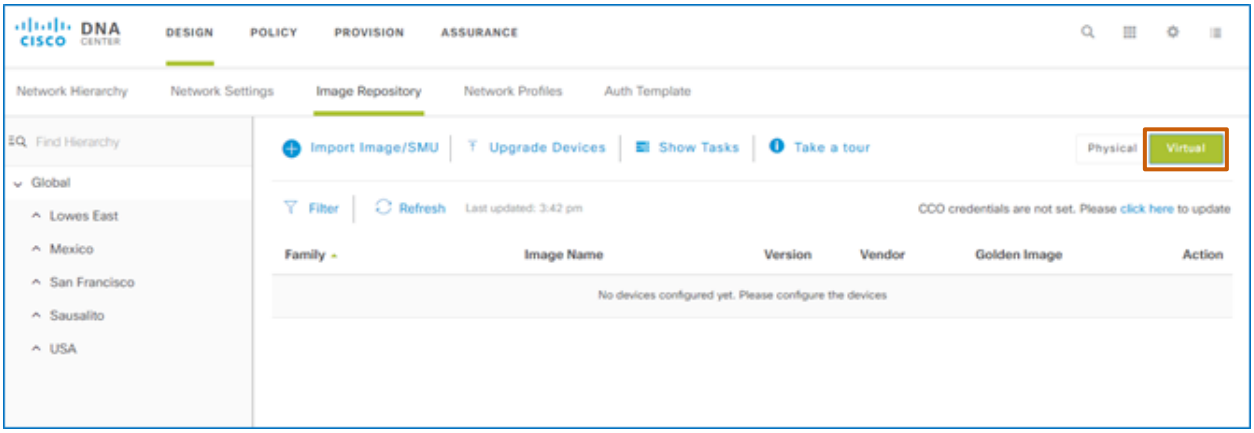
You also can import and standardize virtual software images to support, for example, virtual branch deployments.

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

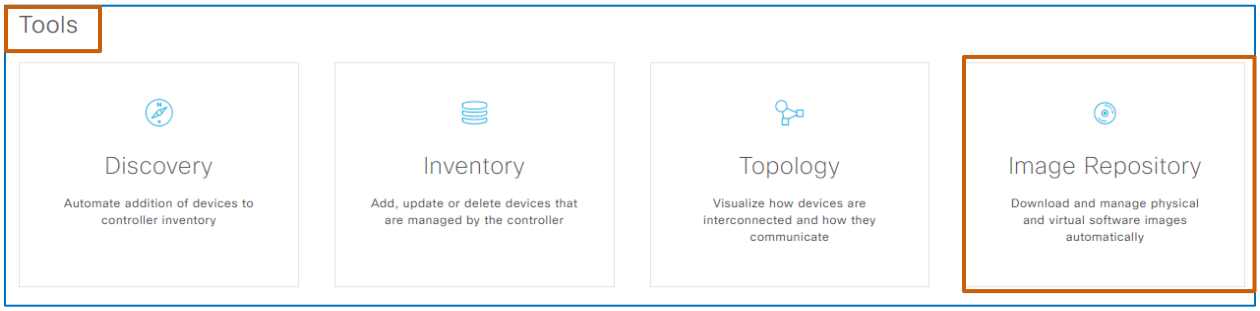
An Alternate Image Repository Page for Global Management

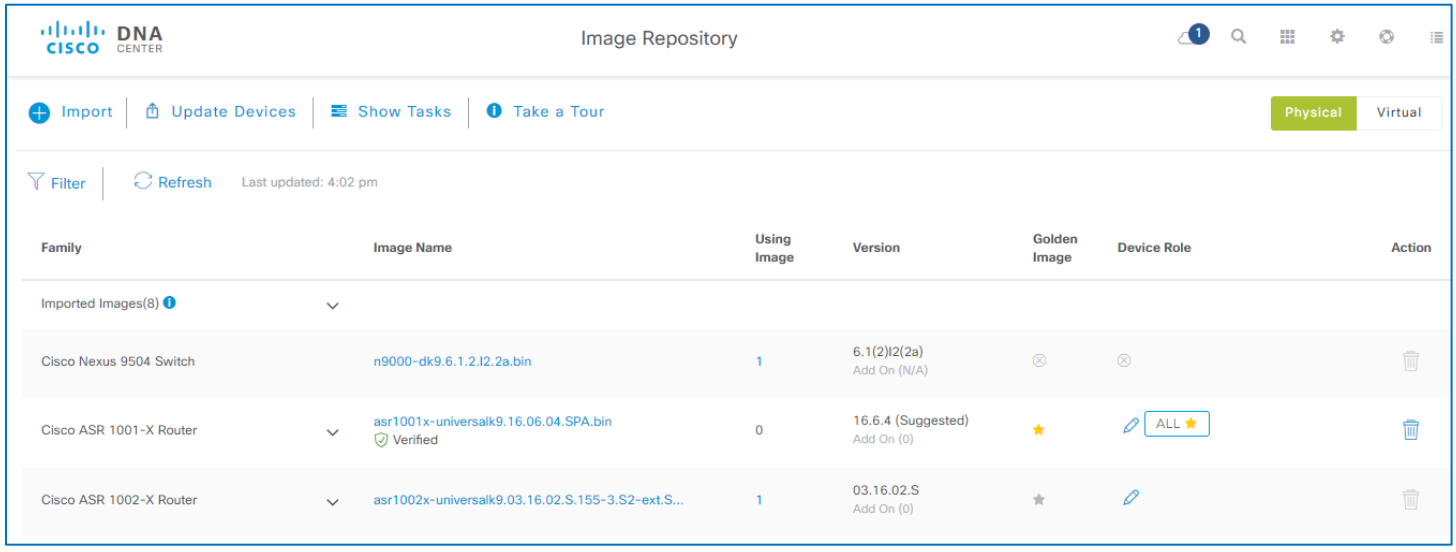
Cisco DNA Center also provides an **Image Repository** page, which you can access on the home page using the **Image Repository** link under **Tools**.

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 as golden on the **Image Repository** page, the system will apply the standard at the global level and present the automated audit results based at that hierarchical level.

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





The Skills That I Need

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

Key Terms

Add-On Packages (Add-Ons)

An add-on that contains specific corrections for an existing base image.

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

Device Family

A category of devices of a common type, such as routers, switches and hubs, or wireless controllers

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

Device Series

Within a device family, such as switches and hubs, the number that identifies the specific device model, for example, Cisco Catalyst 4500 Series switches.

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

Upgrade and Update

The GUI uses the terms upgrade and update interchangeably. This document uses the term upgrade except when naming GUI elements.

Upload and Download

The GUI and documentation use the term upload and download interchangeably. This document uses the term download except when naming GUI elements.

How Do I Prepare to Manage Device Software Images?

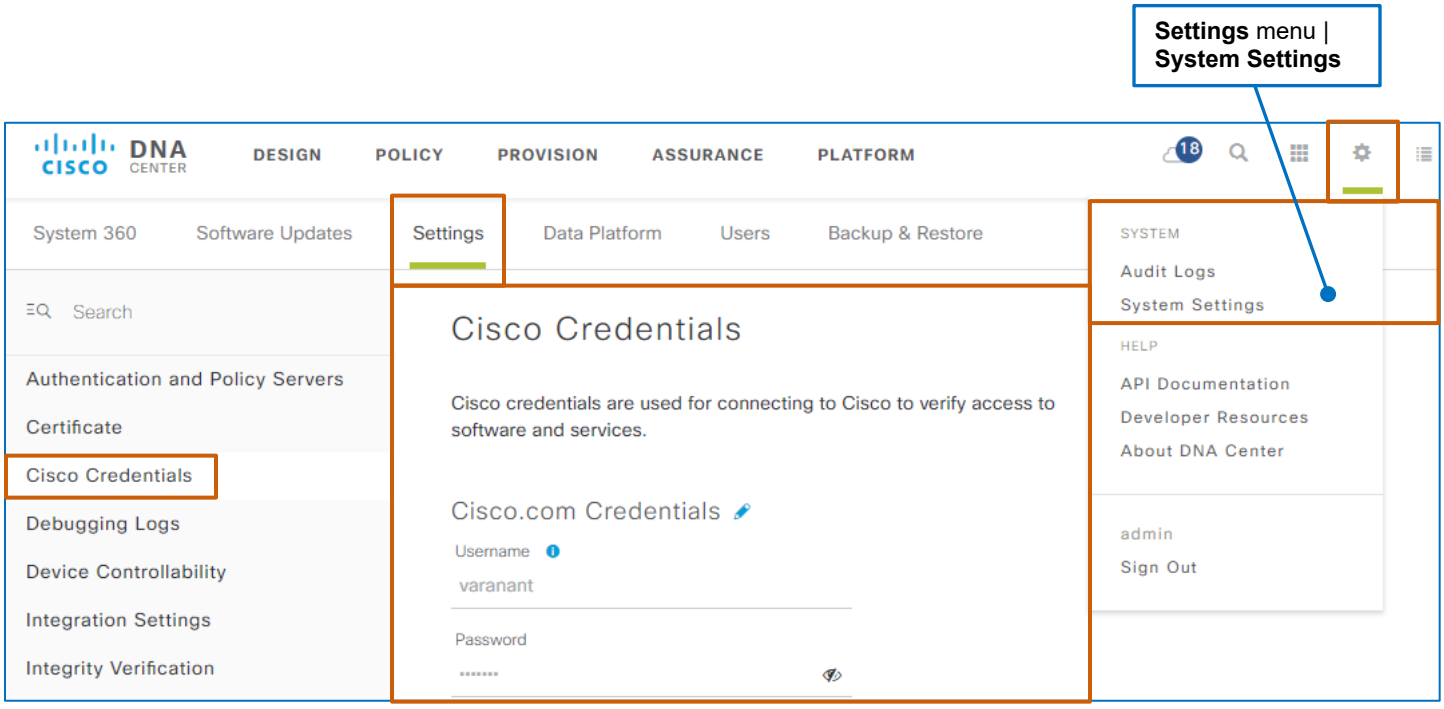
In Cisco DNA Center…

…For Access to Images and the Integrity Verification Tool Online, Configure Cisco.com Access Credentials

New software images and add-ons are available on Cisco.com for download to registered users, including Cisco DNA Center.

Cisco.com also houses the Known Good Values (KGV) tool that Cisco DNA Center references when auditing devices for compliance with image standards.

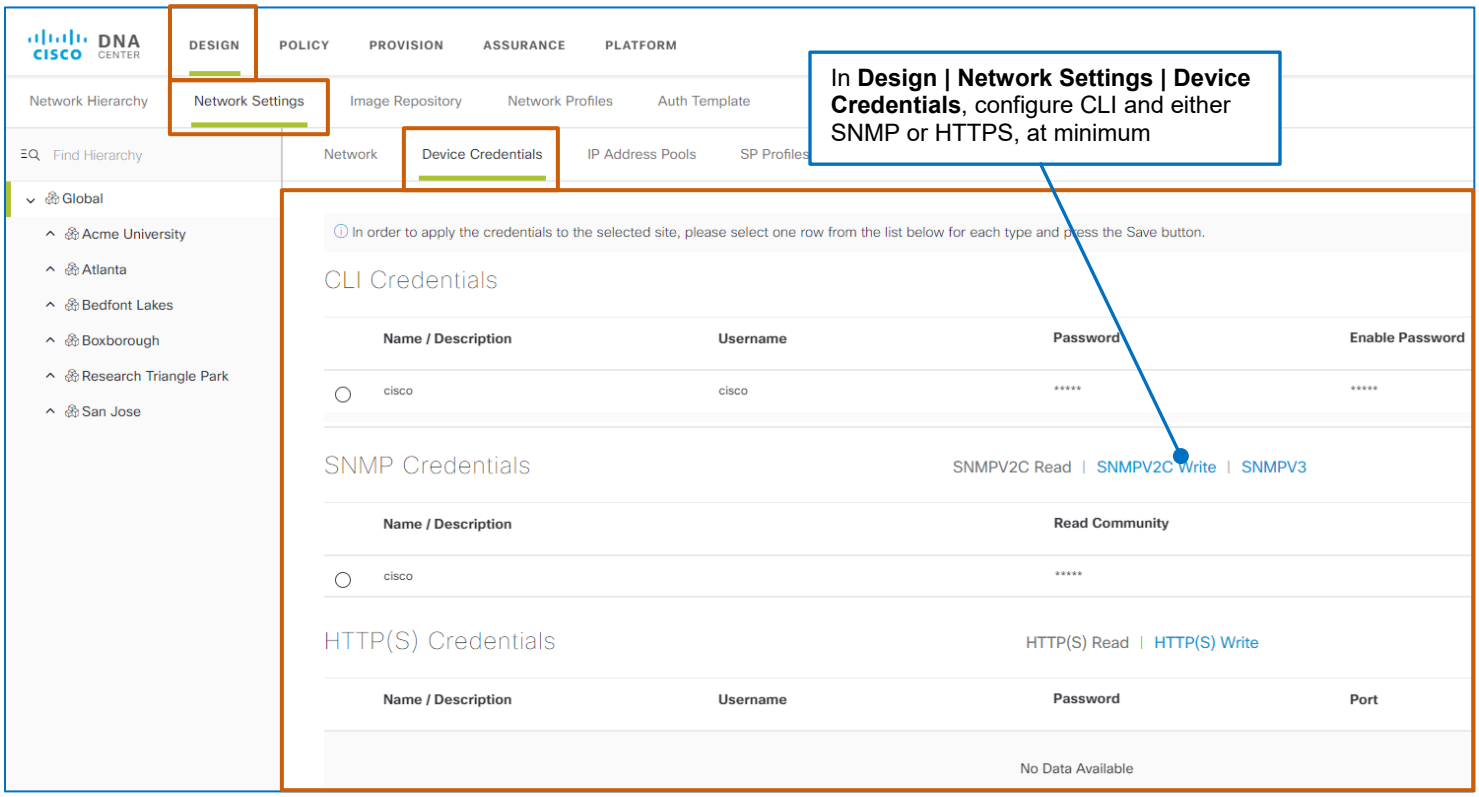
An administrator configures Cisco.com credentials in Cisco DNA Center in **System Settings**.



…For Cisco DNA Center Access to Device Images, Configure Device Credentials and Protocols for Communication

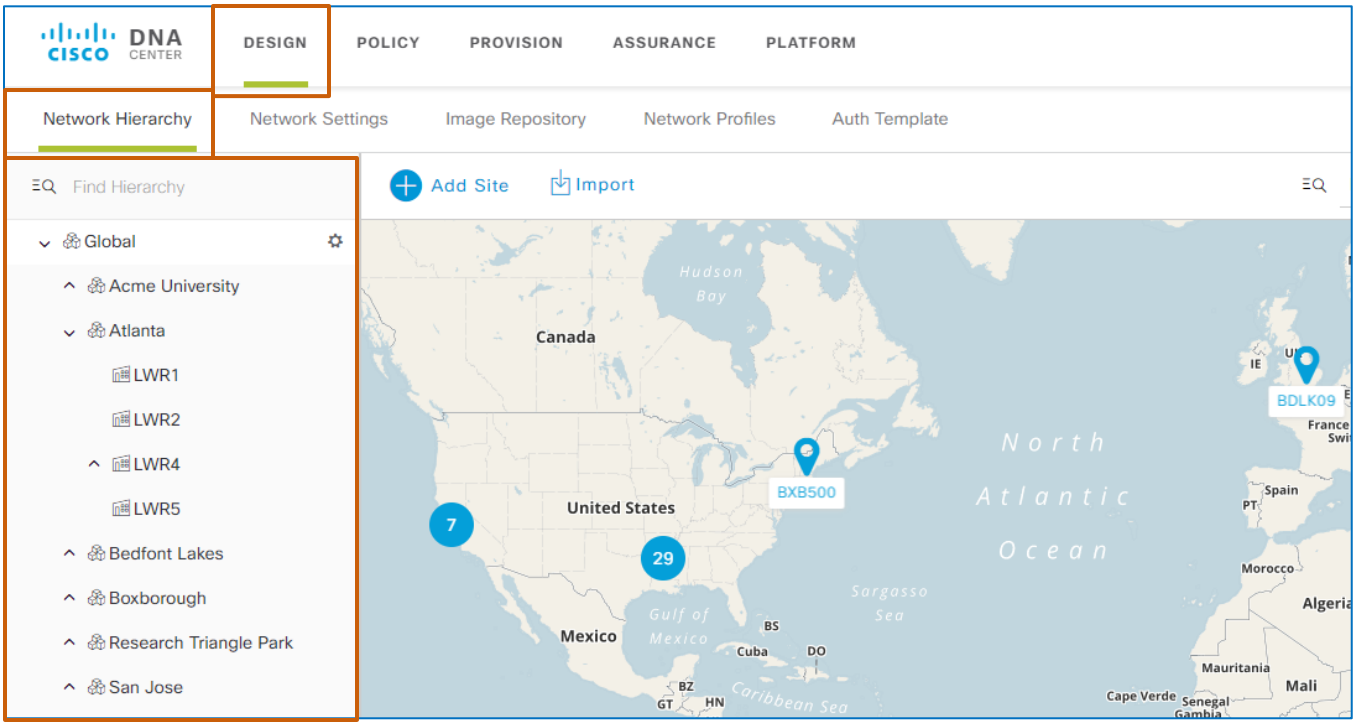
To support communication among network devices and Cisco DNA Center, the devices need to have the following access credentials configured in **Design | Network Settings | Device Credentials** at minimum:

- The CLI credentials that devices are using
- The SNMP read and write credentials that devices are using
- When you need to communicate with Cisco Enterprise Network Compute System (ENCS) devices, you also need to configure HTTPS credentials.

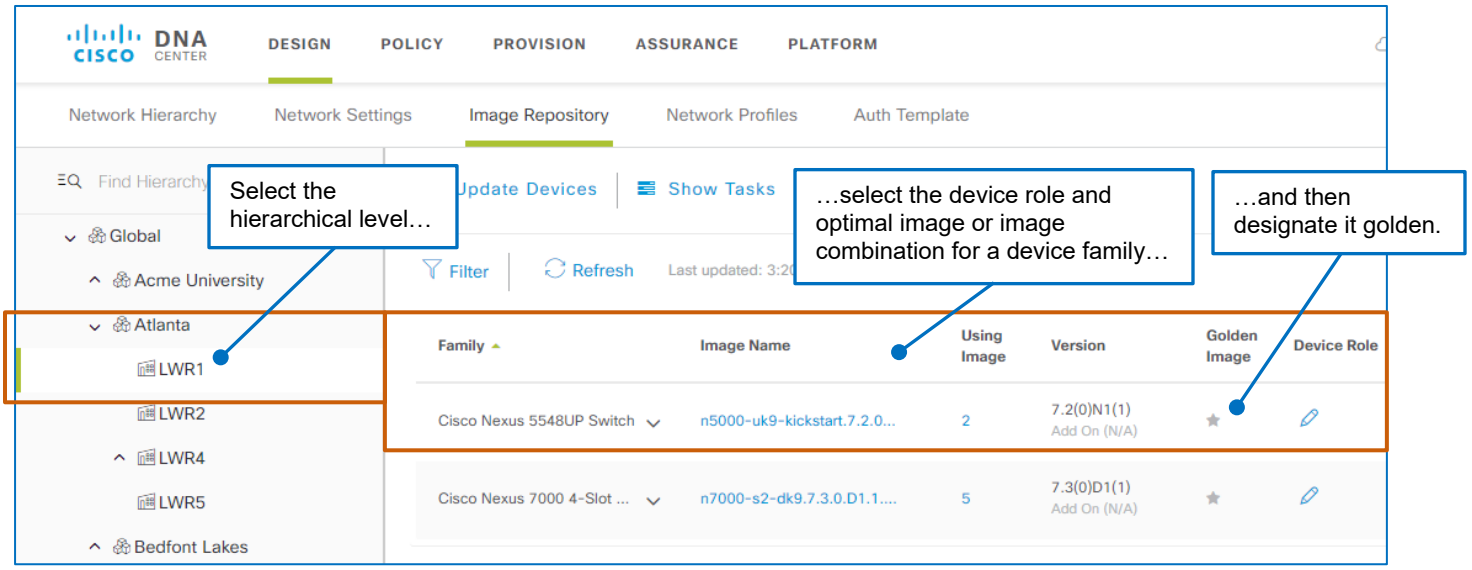


…For Image Standardization and Upgrades, Configure the Network Hierarchy

The network hierarchy defines the geographical or organizational relationships and dependencies of enterprise devices. System users configure the network hierarchy in **Design**, which most often occurs as an initial task after installing Cisco DNA Center.



Then, in the **Image Repository**, you can define varying image standards and apply them at any level in the hierarchy, which supports device configuration consistency and granular control of upgrades to help ensure devices are consistent and have the expected device features and technologies.

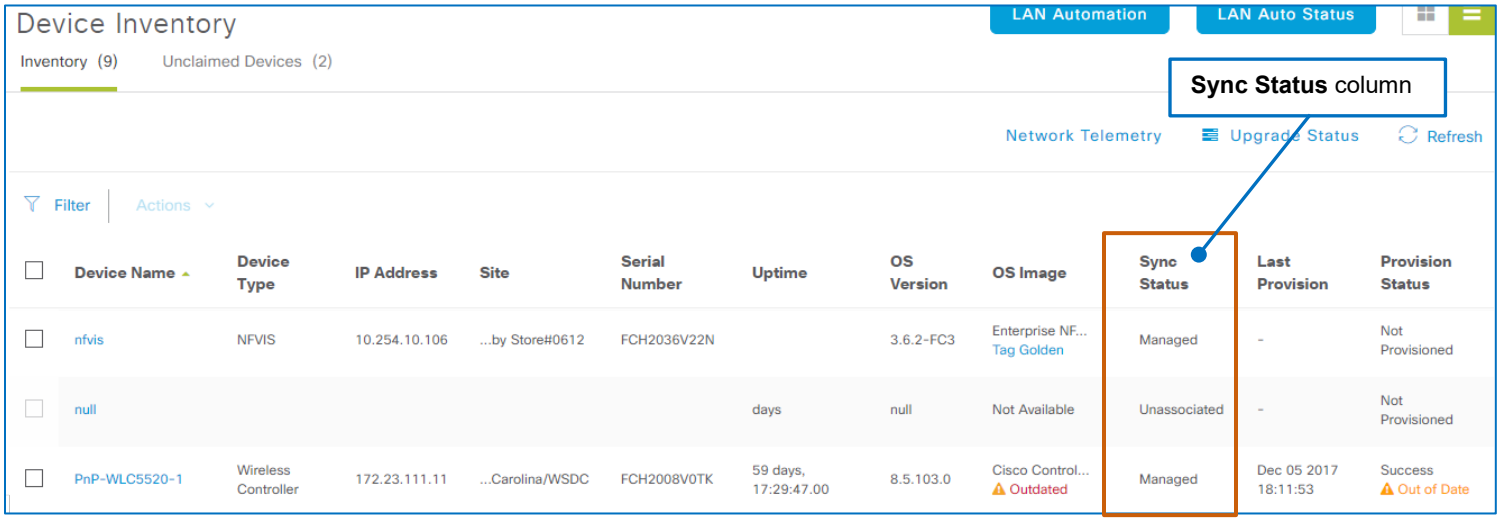


…For Image Upgrades, Ensure That Cisco DNA Center is Managing Devices

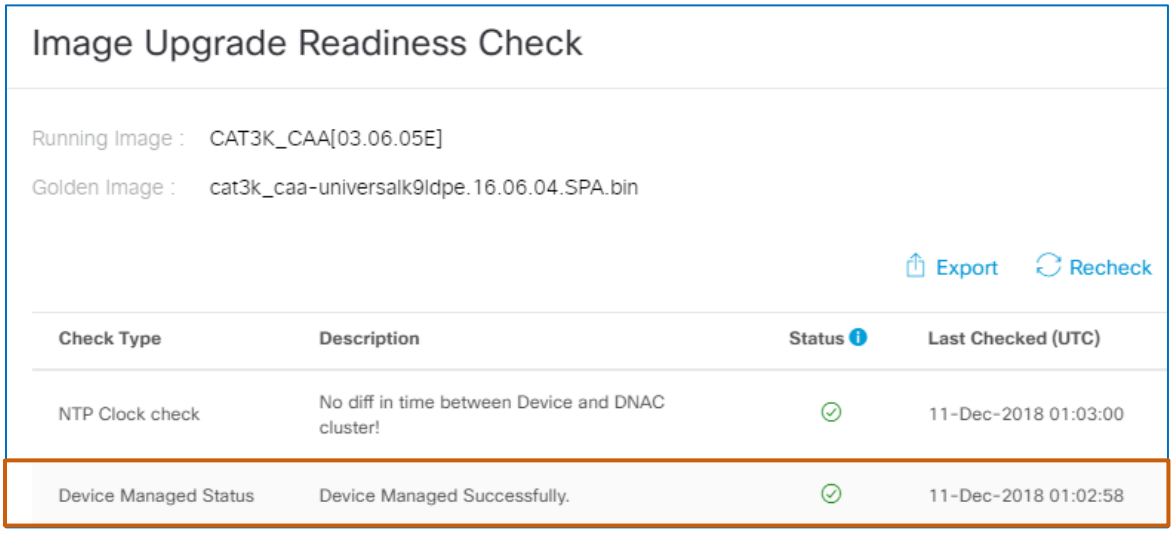
To accept upgrades, devices need to be in a managed state.

To determine a device's management state:

- On the **Inventory** tab, refer to the **Sync Status** column.



- For a device with an **Outdated** status, click **Outdated**, and then, in the **Image Upgrade Readiness Check** panel, review the **Device Managed Status** readiness check result.



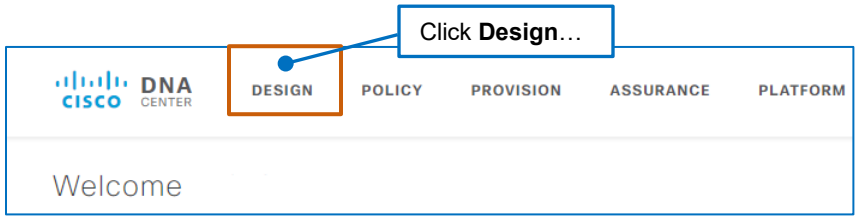
- For all devices with **Outdated** status, download the **Upgrade Readiness Export** .CSV file, and then review the **Device Managed Status** readiness check results.

What Are the Steps That I Take To…

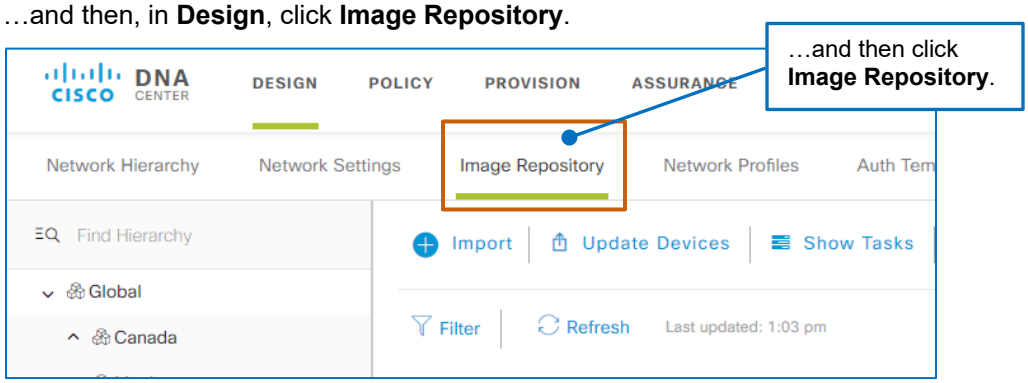
…Navigate to the Image Repository?

To navigate to the Image Repository, on the Cisco DNA Center **home page:**

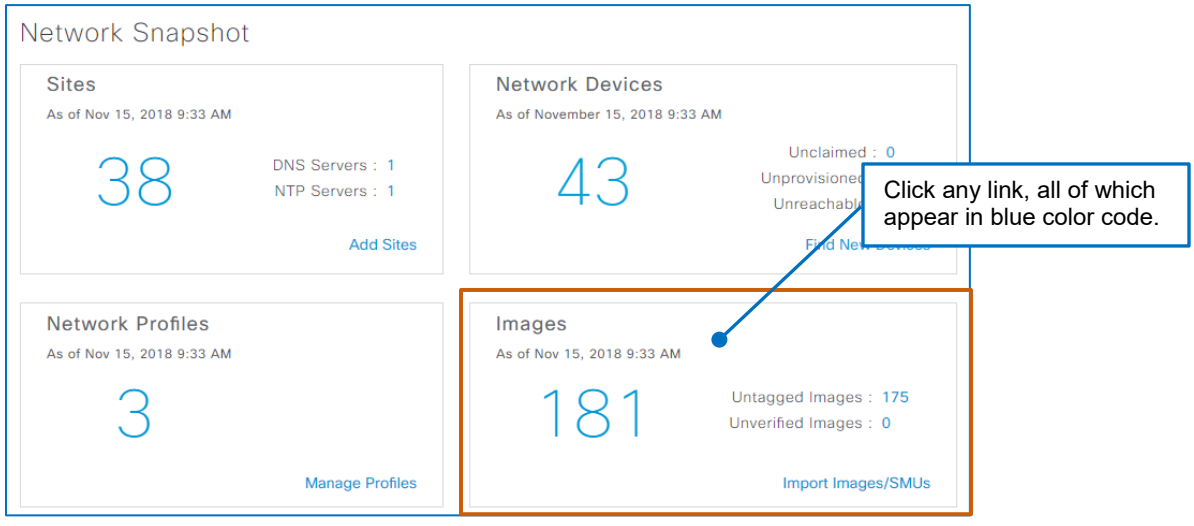
- On the application toolbar, click **Design**…



…and then, in **Design**, click **Image Repository**.



- Under **Network Snapshot**, in **Images**, click any link, each of which appears in blue-color code.



- Under **Design**, click **Designate golden images for device families**.

The system navigates to the **Design | Image Repository** page.

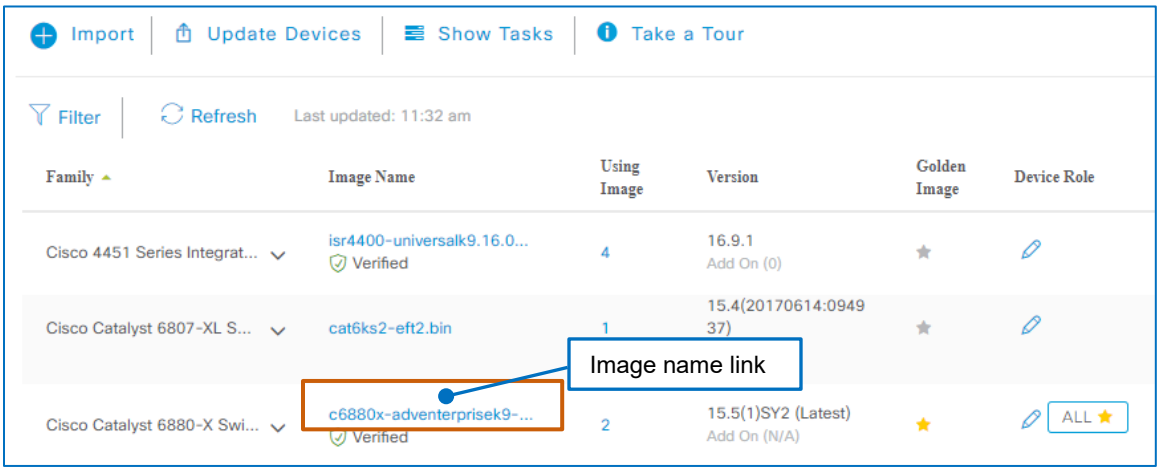
> **Note:** To review the page layout and contents, refer to the **What Will I See in the Image Repository?** topic.

…Review Image or Add-On Attributes, such as File Sizes?

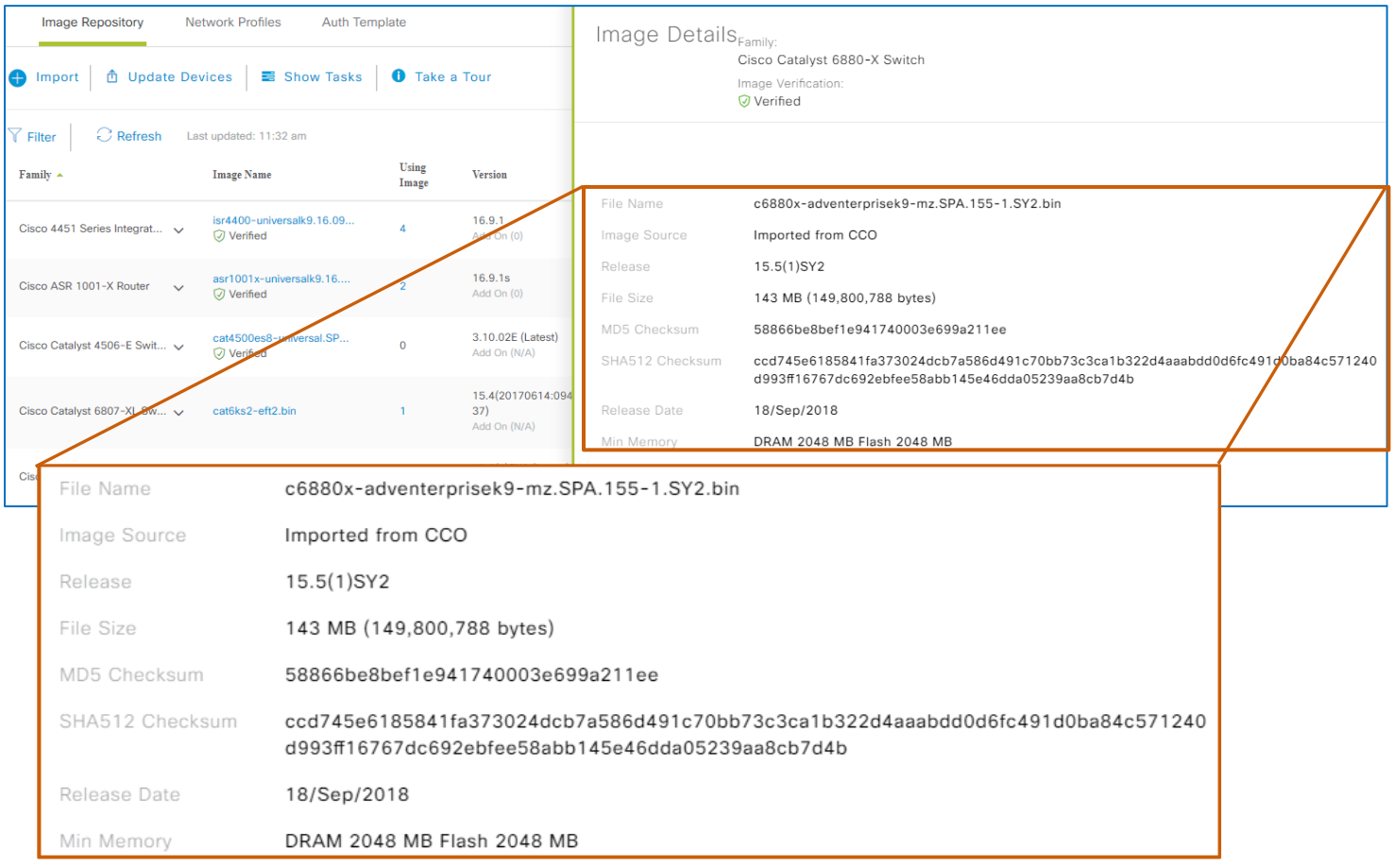
Each image and add-on name in the Image Repository provides a link to detailed attributes.

To open attributes details for an image or add-on:

- Click the image name link.



A panel opens and presents the attributes that are available.



…Import Device Software Images or Add-Ons?

Cisco DNA Center imports images to the **Image Repository** automatically when a system user designates images or add-ons that Cisco DNA Center is managing as golden based on image type, as follows:

- By importing images from Cisco.com, when an administrator configures Cisco.com credentials in Cisco DNA Center.
- By importing images from devices when a system user configures the device credentials.

Important Note: The system can import images from devices only when they are in bundle mode.

It cannot import images automatically from WLC devices.

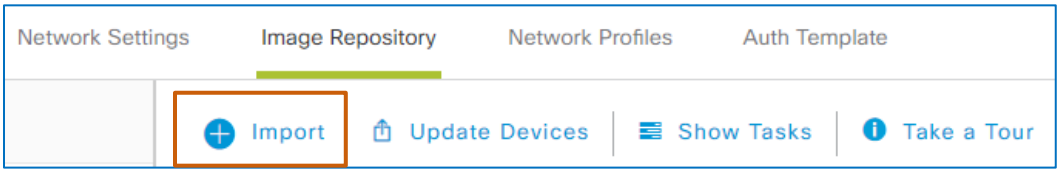
When you need to import an image manually, you can follow this process to download it to the **Image Repository**.

Note: You take the same steps to import virtual images.

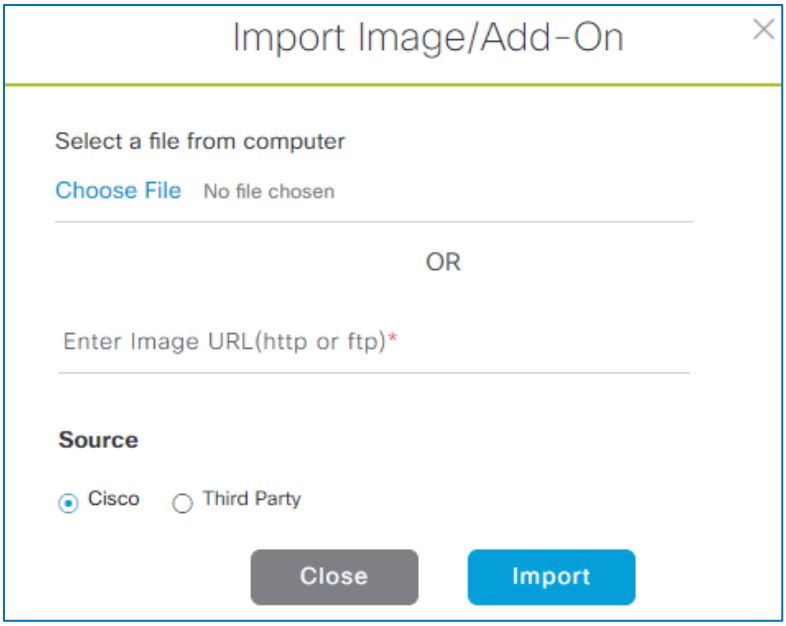
For more information importing images, refer to the **What Will I See in the Image Repository?** topic.

To import a software image or add-on:

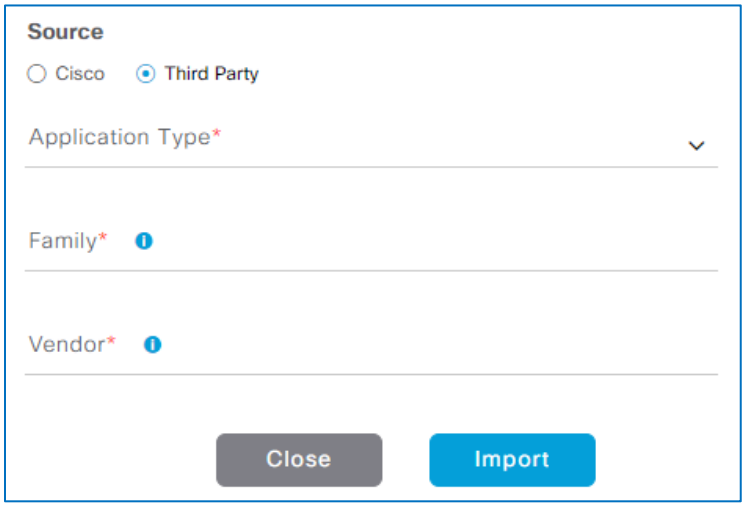
1. On the toolbar, click **Import**.



The **Import Image/Add-On** dialog box opens.



2. In the **Import Image/Add-On** dialog box:
   - 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 an NFVIS-compatible 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:
     a. Under **Source**, select **Third Party**. The section expands to display required import information fields.



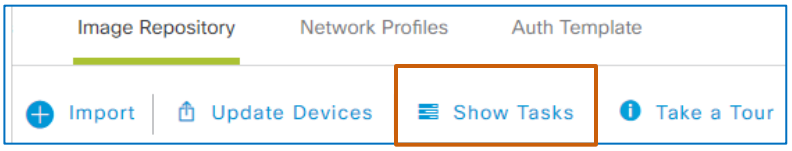
     b. To select the application that is running the image that you need, in the **Application Type** drop-down list, select the application type.
     c. To identify the image family, such as Windows or Linux, in the **Family** field, type the family name.
     d. To identify the company that produces the 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.

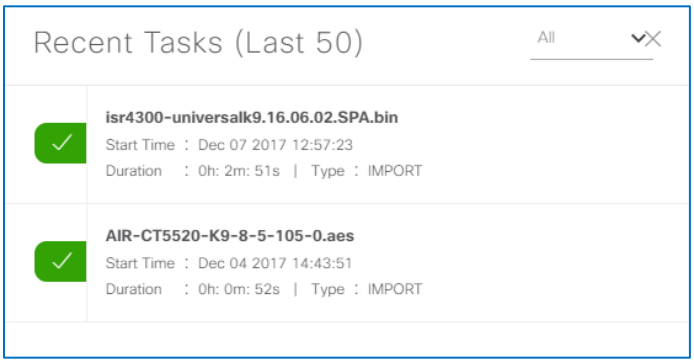
3. Click **Import**.

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

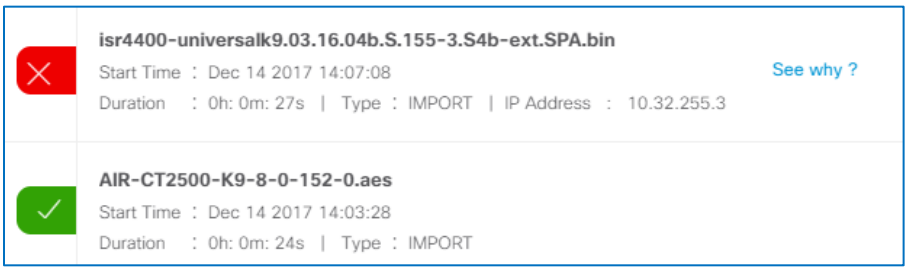
4. To monitor the progress and results of the import task, on the toolbar, click **Show Tasks**.



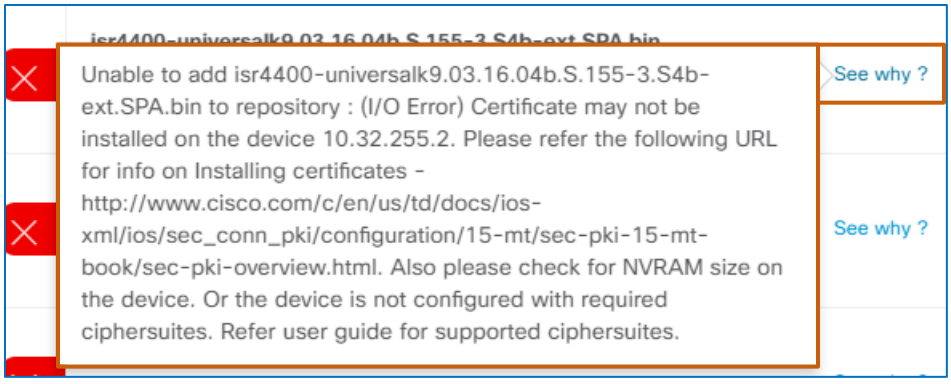
The **Recent Tasks** panel opens and lists the ongoing task.



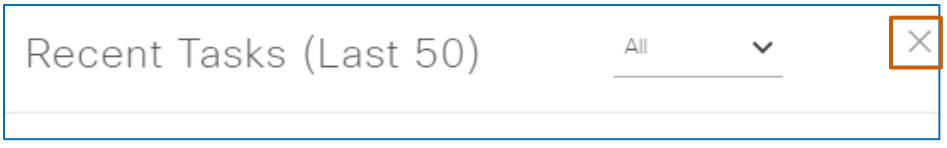
When the import is complete, the panel indicates success with a green indicator or failure with a red indicator.



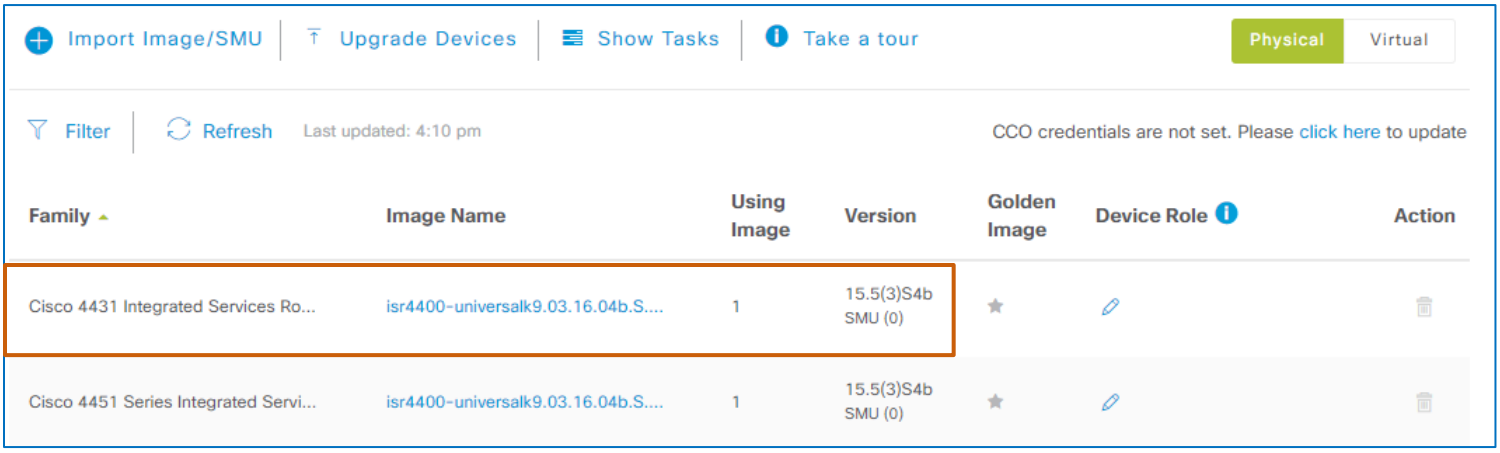
Tip: If an import fails, you can click **See why?** to open a tooltip that describes the problem and suggests ways to correct it.



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



Beside the applicable device family, the repository lists the image or add-on that you imported.



After importing an image or add-on:

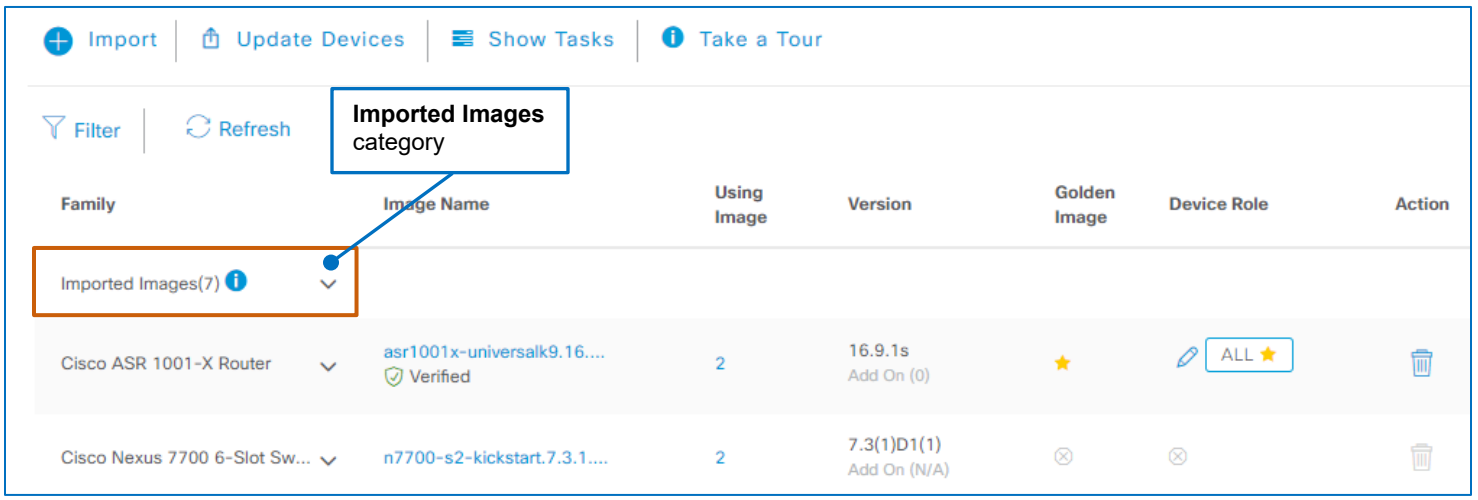
- To prepare for Plug and Play device provisioning, associate the image to a device family.
- To prepare for auditing compliance of existing devices and managing software upgrades, standardize the image and designate it as golden.

…Associate Images to Device Series or Families to Support PnP Provisioning?

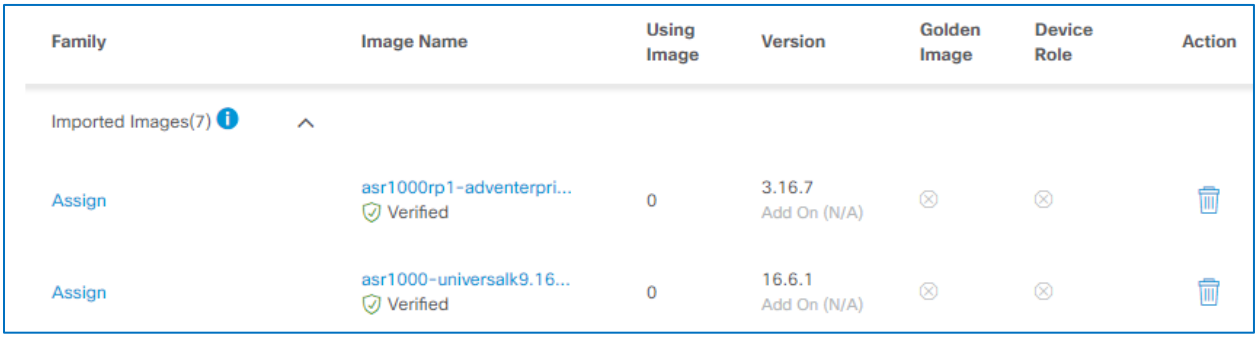
Cisco DNA Center provides the Plug and Play provisioning process, which supports automatically and remotely onboarding and provisioning new network devices. Inherently, these new devices are not yet captured in the Cisco DNA Center inventory. If this is the first time that you are provisioning devices in a device family by using Plug and Play, you need to assign the image that you imported to that family.

You can use the **Imported Images** category to assign images to their device families or the specific device models in those families in preparation for Plug and Play device onboarding and provisioning of new devices. Then, after onboarding, the system will indicate audit results based on the image that the device is running and the golden image that has been designated for its related family.

If you also designate the assigned image as golden before onboarding, the device can obtain the golden image during the onboarding process based on the Plug and Play configuration and begin running it when it boots.



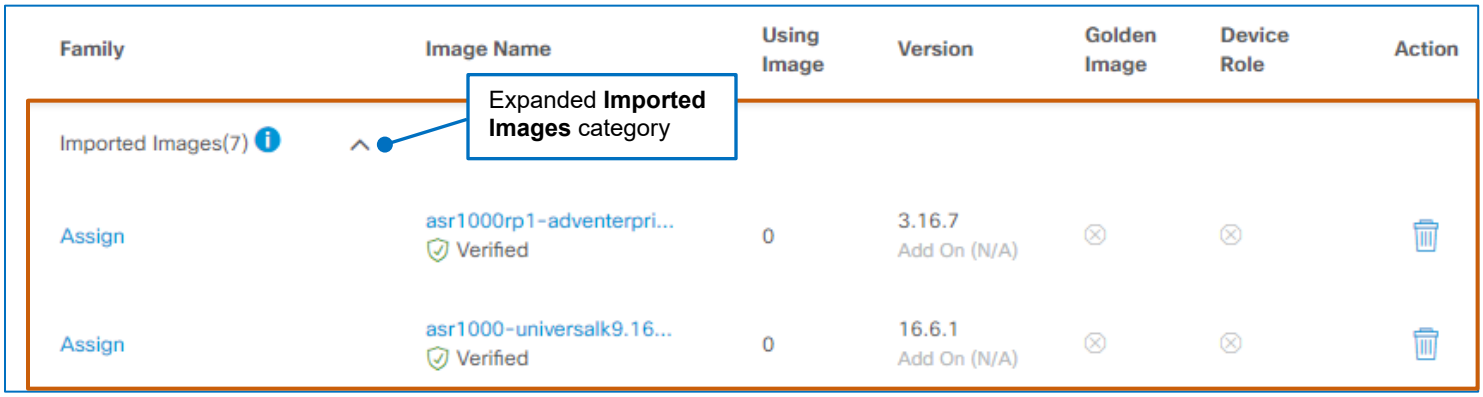
When you import images, they are added to the **Imported Images** category automatically. When images apply to device families that are present in the list, the repository also includes them with [their applicable device families](#).



To associate images to device families or series:

1. Expand the **Imported Images** row.

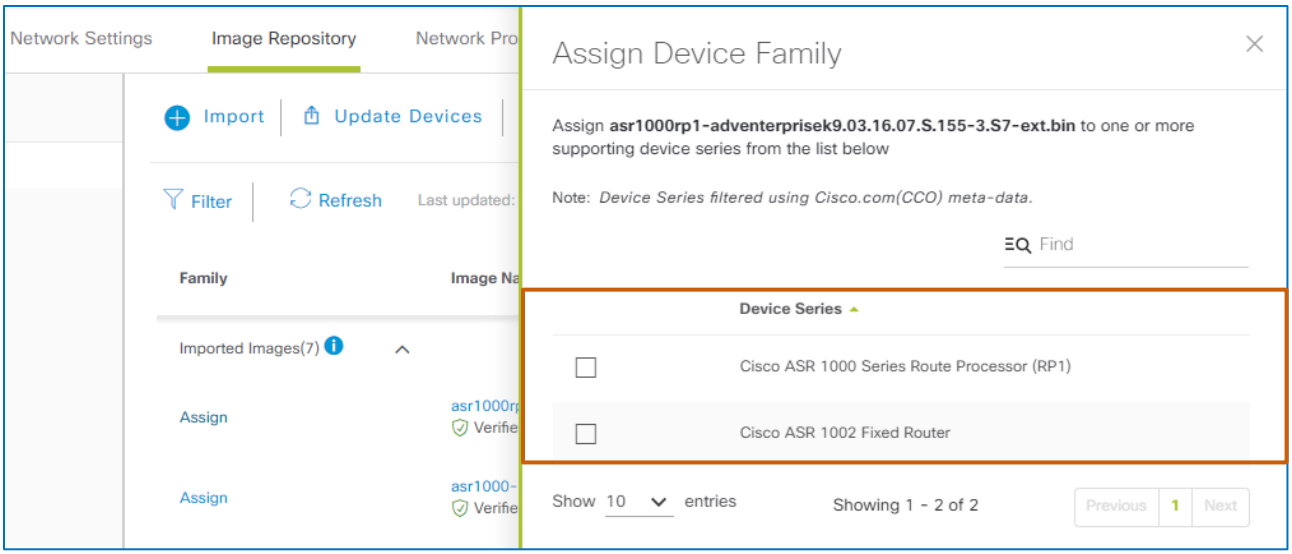
   The category opens and lists every image that system users have imported or that have been imported in the automated tag golden process.



2. Beside the applicable image, click **Assign**.

   The **Assign Device Family** panel opens and overlays the page.

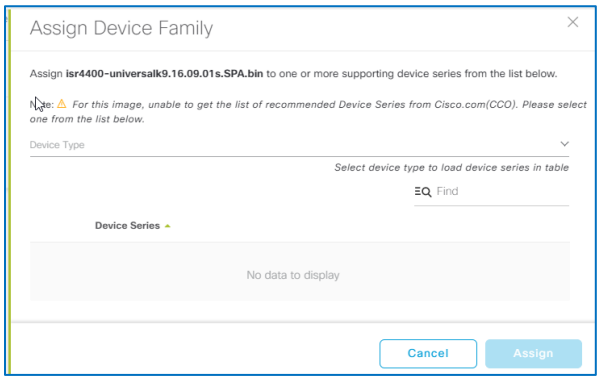
   Under **Device Series**, when Cisco DNA Center is online with Cisco.com, a list can populate automatically with the applicable models in the device family by referring to image metadata.



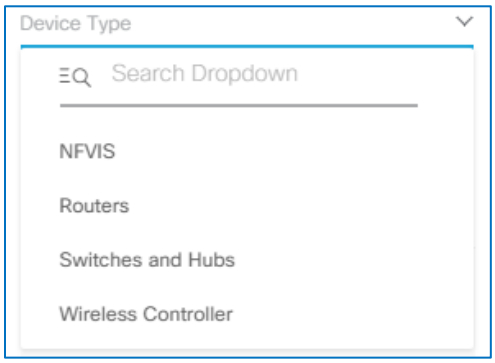
When not on online with Cisco.com, Cisco DNA Center cannot access image metadata, so it cannot reconcile the image with its applicable device family or series.

Or, in some cases, users can change the image name from its default.

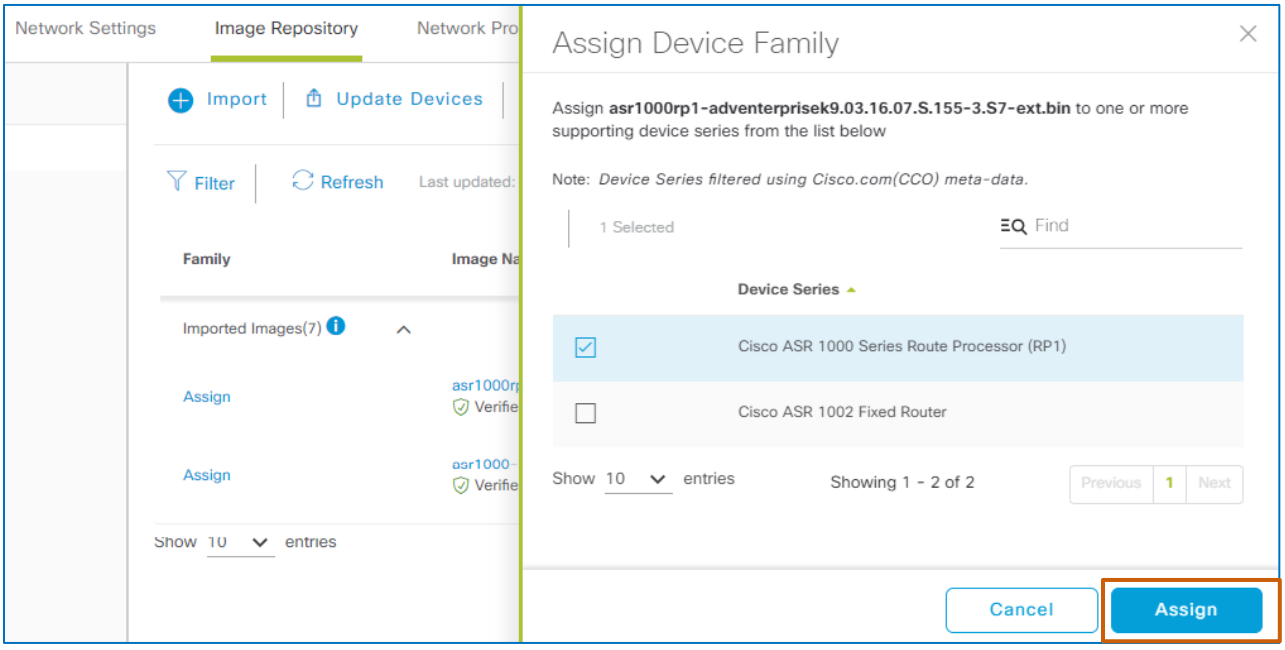
In those cases, the list appears blank.



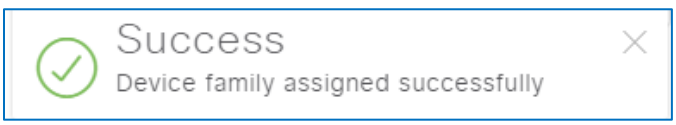
3. Under **Device Series**, determine whether the panel lists device models in the family of devices that apply to the image.
   - When device models are available, go to step 4.
   - When nothing appears in the list, in the **Device Type** drop-down list, select the category of the device or devices to which you need to assign the image, which populates the list automatically, and then go step 4.



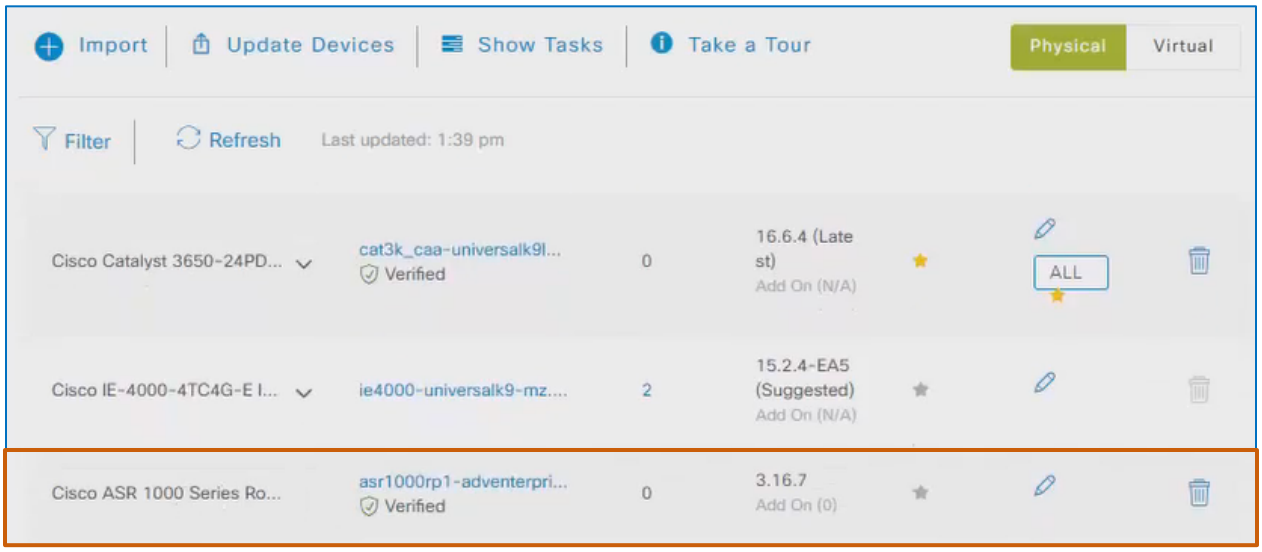
4. In the list, to assign the image:
   - To the device family, beside every device model included in the list, select the check box, and then click **Assign**.
   - To a specific device model or models, beside each model that you want to include, select the check box, and then click **Assign**.



The panel closes, and a system message opens at the bottom of the page, indicating the action.



The image now appears in the list in the **Image Repository** and is available for standardizing and designating as golden.



…Standardize Software Images or Add-Ons and Tag Golden?

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

In the standardization process, you designate a combination of characteristics as golden, including the software image.

Important Note: This action makes the image or image combination available for device upgrades.

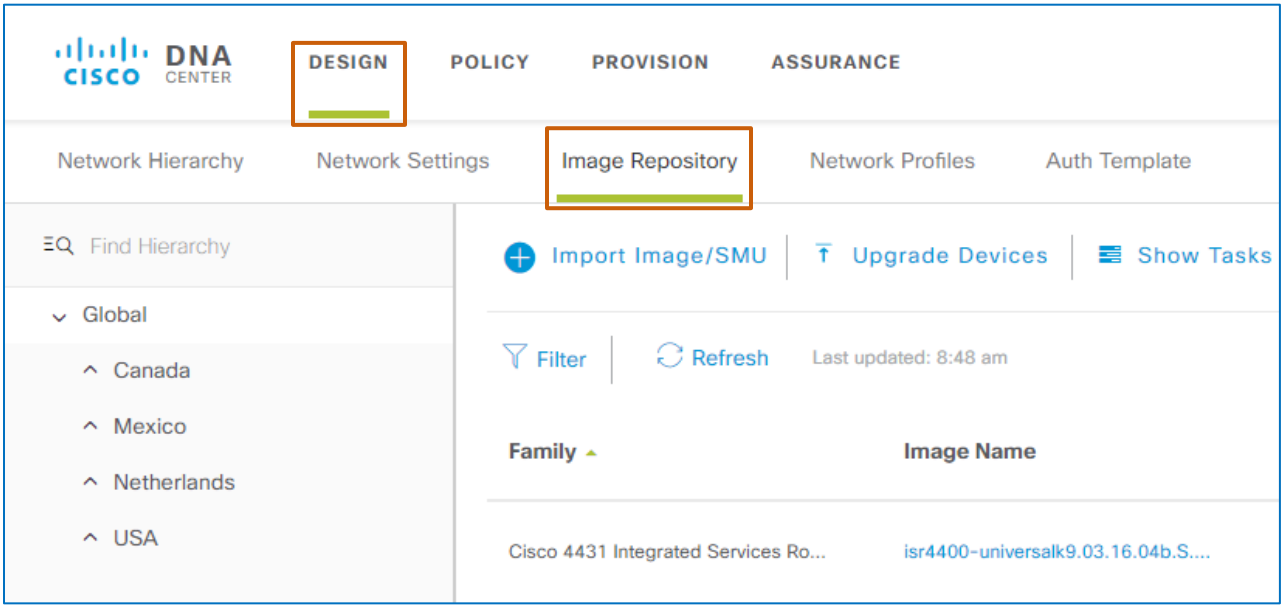
When they are available, Cisco DNA Center associates an add-on to the base image that it updates automatically. When you standardize an add-on by designating it golden, you first must designate its associated base image as golden.

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

Important Note: Only one add-on can be designated as golden for a base image.

When you standardize an image and its optimal add-on, the system provisions both the image and add-on when upgrading devices.

When a device is running the base golden image but is not running the associated golden add-on, the system upgrades the add-on only.



Cisco Best Practice: 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.

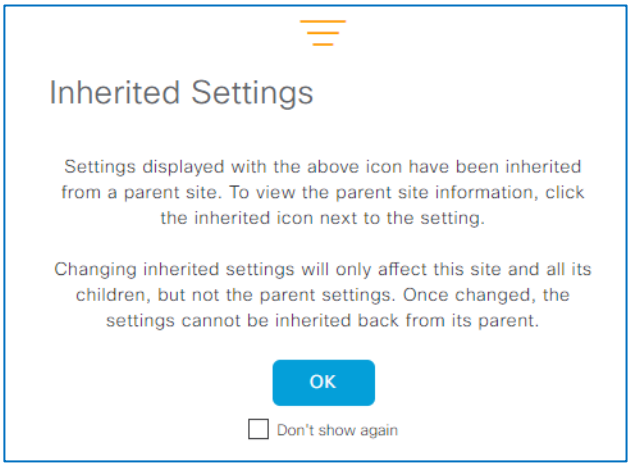
For more information, refer to **The Alternate Image Repository Page for Reviewing** topic.

To standardize a device image or add-on:

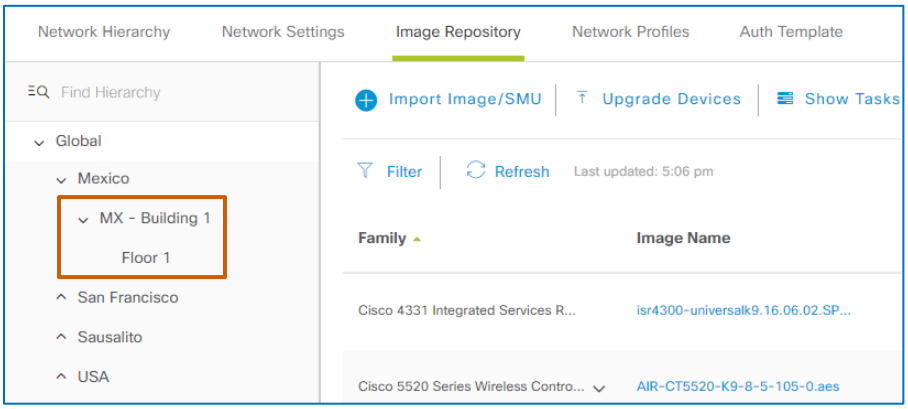
1. Follow the steps to navigate to the **Image Repository**.
2. Determine whether the image is available in the **Image Repository**.
   - If the image is in the repository, indicated by an enabled **Delete an image** button, go to step 3.
   - If the image is not in the repository, indicated by a disabled **Delete an image** button, and can be imported in the tag golden process, go to step 3.
   - If you are working with a WLC image or an image with the **Install Mode** image name and it is not in the repository, import the image manually, and then go to step 3.
3. To select the hierarchical level for which you need to standardize image characteristics, in the **Design | Image Repository** tab, in the network hierarchy list, select the level.

Important Note: Dependent levels in the hierarchy inherit the attributes that you apply at a parent location level when the inheritance relationship has not been broken.

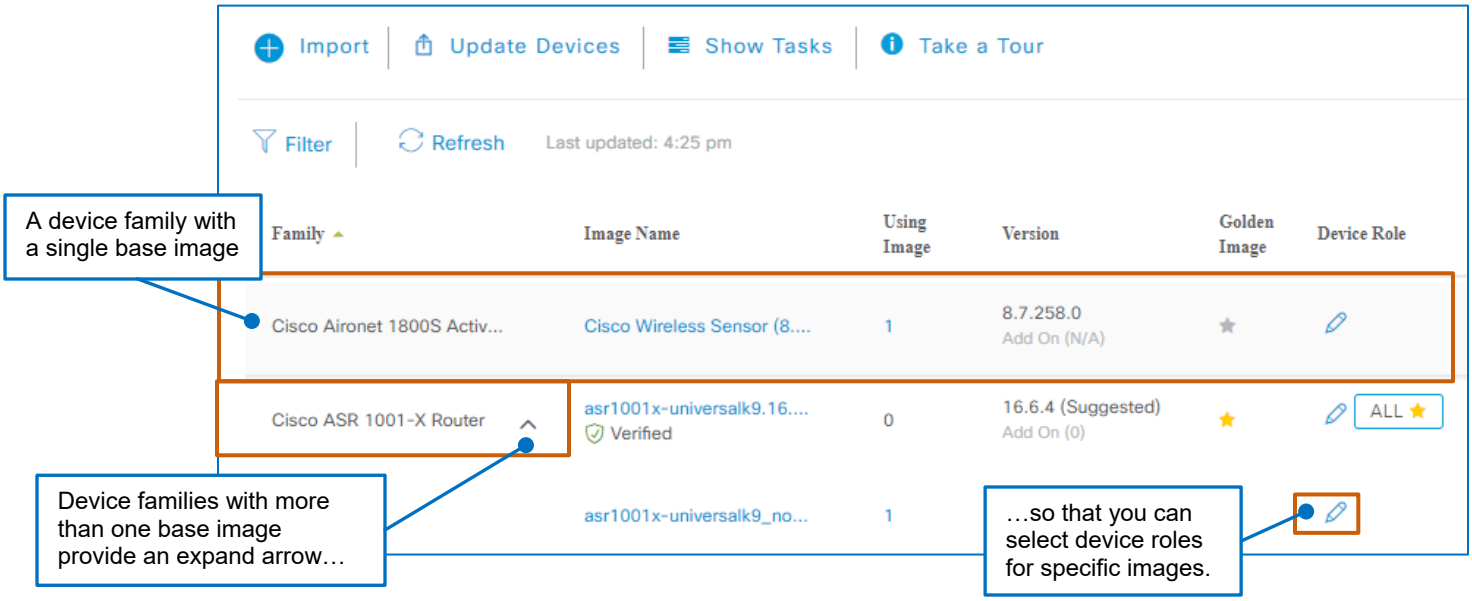
When you select a hierarchical level with inheritance intact, a system message opens, alerting you to the relationship.



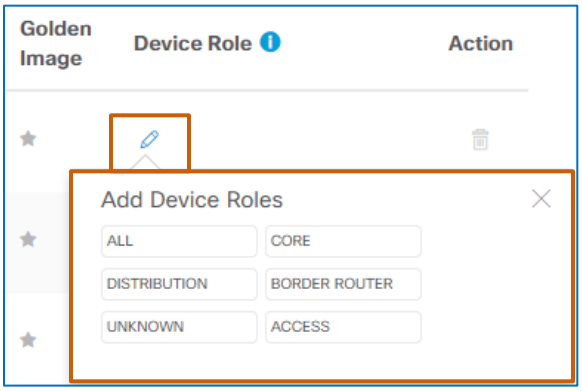
For more information, refer to the **Inheritance Applies Standardized Images to Devices on Dependent Levels** topic.



4. To define the device's role in the network topology at the location level that you selected in step 1, which provides further differentiation among devices in the same family:
   - 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 4a.
   - When the role applies to a specific base image and add-on combination running on specific devices in the device family, expand the device's **Family** row, beside the applicable combination, in the **Device Role** field, click the pencil icon , and then go to step 4a.



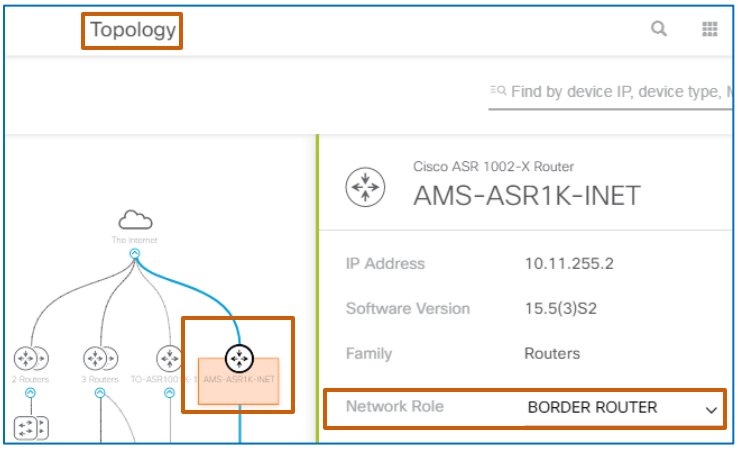
The **Add Device Roles** pop-up window opens.



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

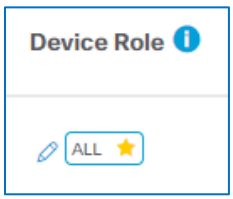
Important Note: During device discovery, the system automatically assigns a network role to the device, which indicates the device's function, and indicates it in the topology.

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.



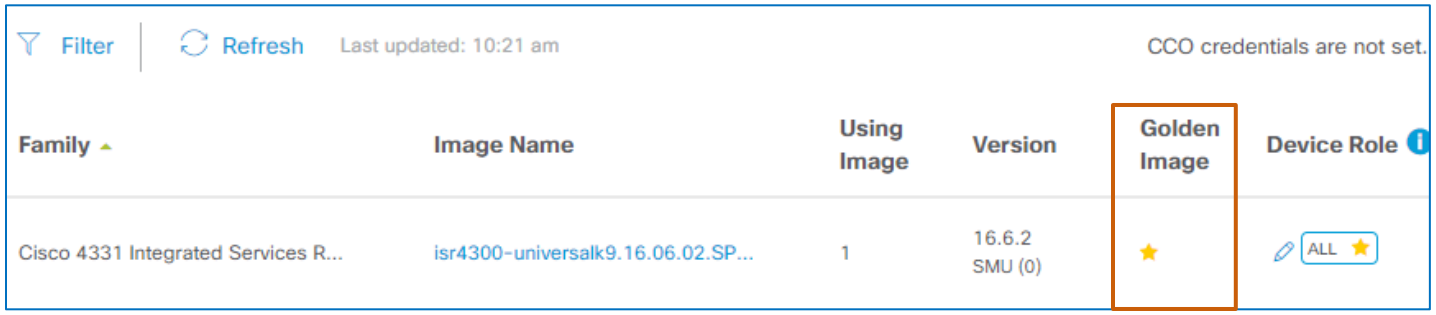
b. Close the pop-up window.

The role that you assigned appears beside the pencil icon.



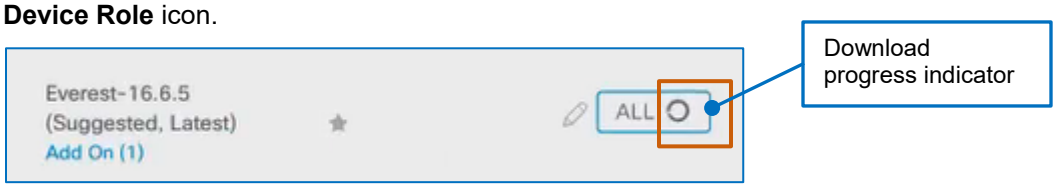
5. To designate the optimal base software image that should run on devices at the location and with the role that you selected, in the applicable row, in the **Golden Image** field, click the star-shaped **Mark Golden** icon.

   When the image is not already in the repository and can be imported automatically from a device or from Cisco.com, the system initiates downloading the image to the repository.



Important Note: Depending on the image size and connectivity, the image download process can take time to complete. The icon turns yellow when the download has completed.

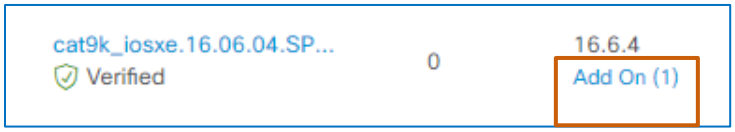
When a download is in progress, the system displays a download indicator beside the **Device Role** icon.



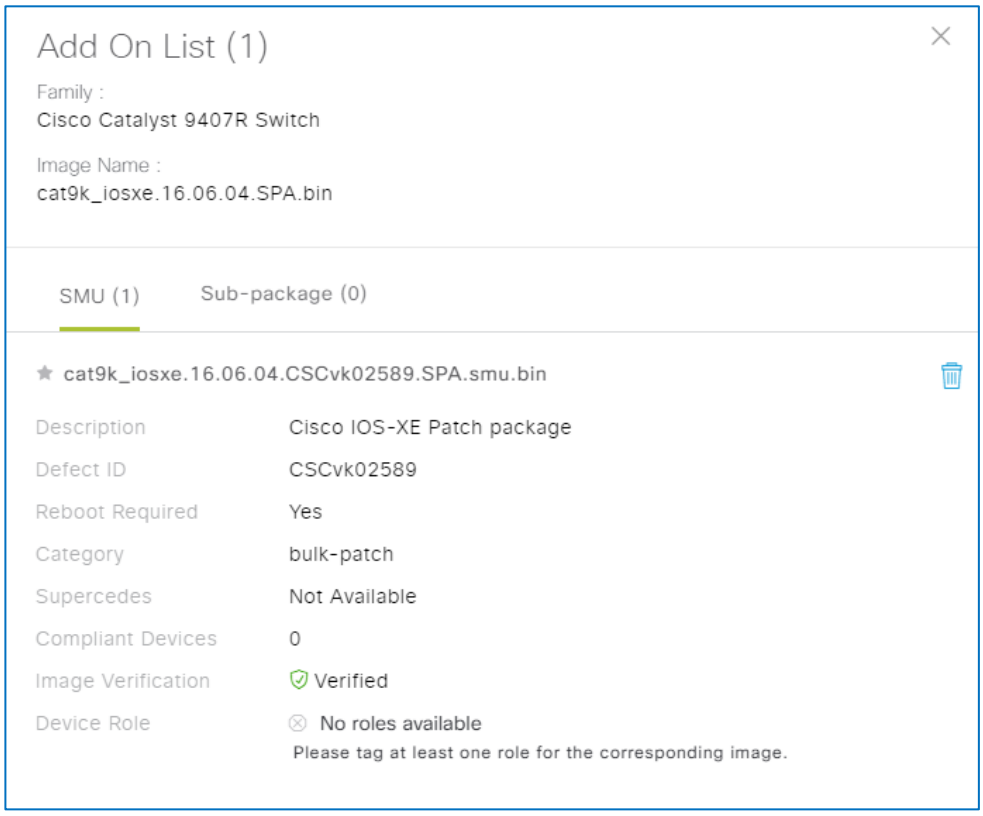
When the download is complete, the start icon displays yellow color-coding to indicate that download and tagging are complete.

6. When applicable, to designate an image add-on as optimal:

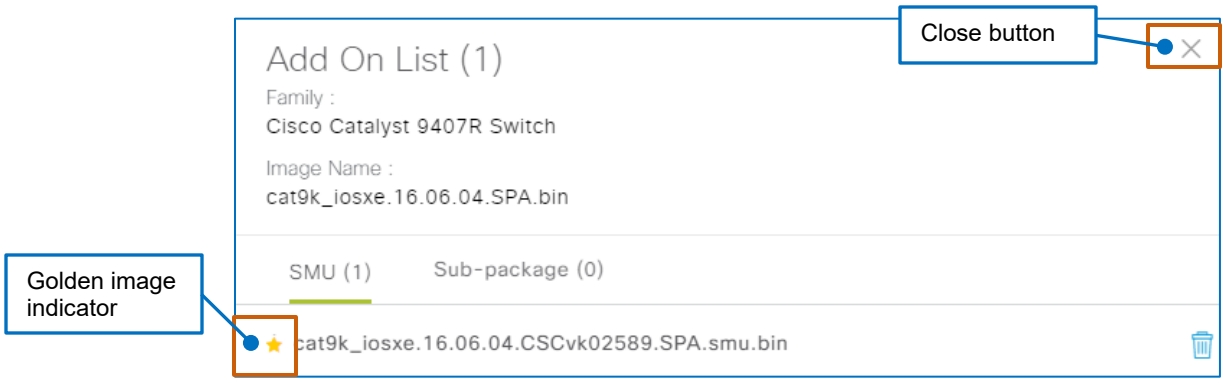
   a. Under **Version**, below the version number, click the **Add On (#)** link.



The **Add On List** panel opens and lists all of the add-ons that are available in the system for the software image.



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



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

7. To standardize another image, return to step 1, and when you have standardized all of the images that you need, you have completed the standardization process.

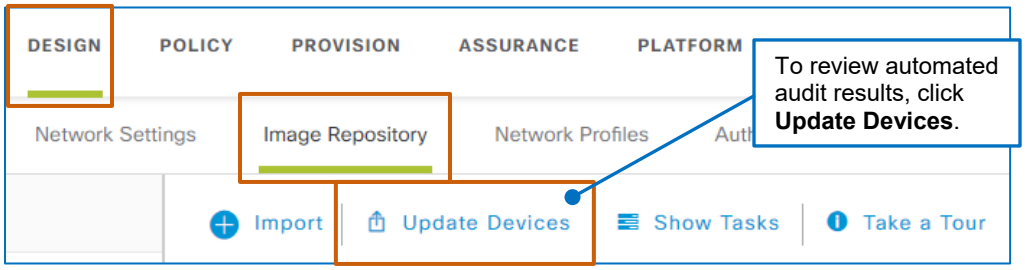
To evaluate state of device images based on the standards that you defined, you can evaluate the automated image audit results.

…Evaluate Automated Audit Results?

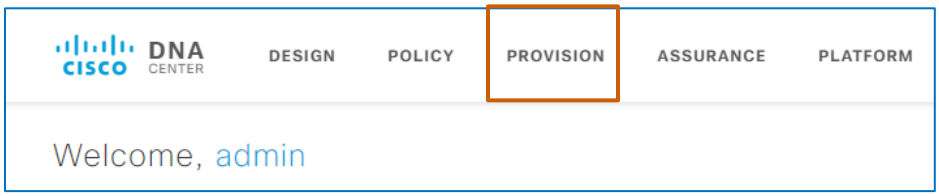
To evaluate automated audit results:

1. To navigate to the results:

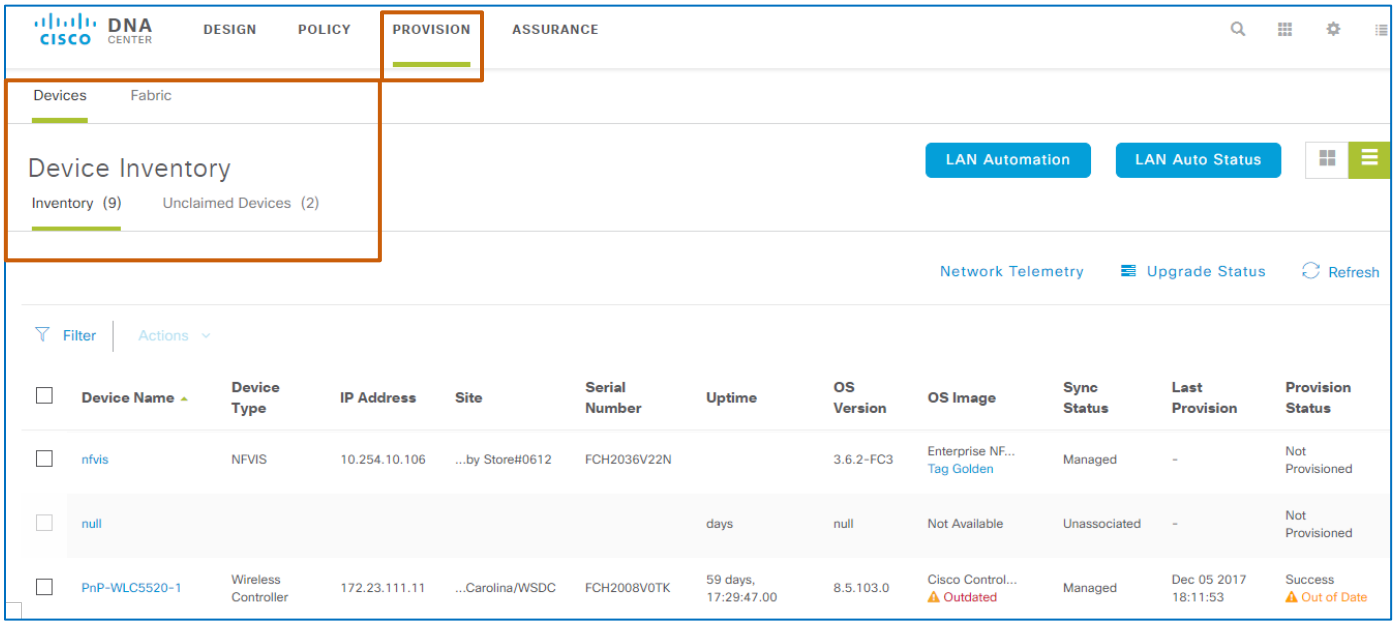
   - In **Design**, on the **Image Repository** tab, on the toolbar, click **Update Devices**.



   - On any page in Cisco DNA Center, click **Provision**.

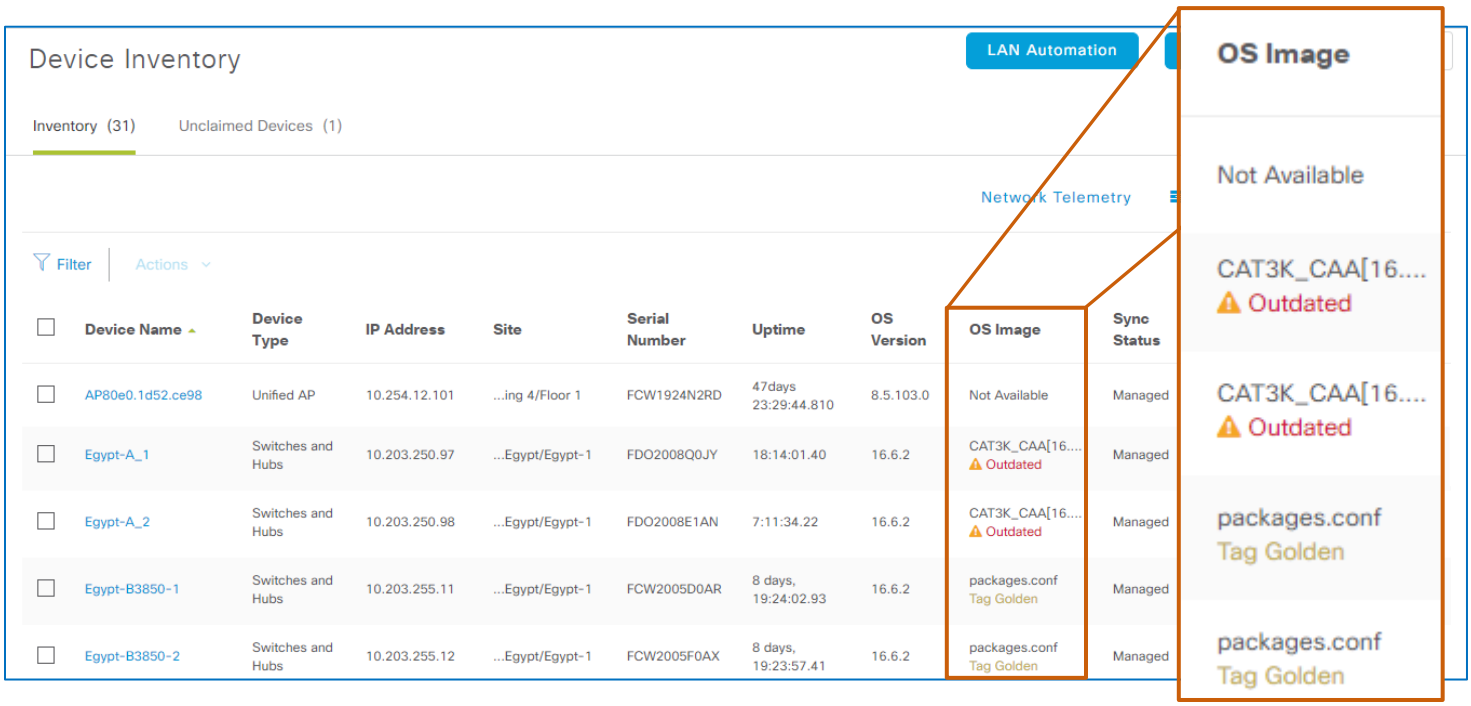


   The system navigates to **Provision**, and the **Devices** tab, **Device Inventory | Inventory** subtab is active by default.



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

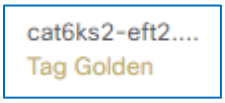
Note: Because the system does not manage access point images, it cannot import them into the repository. For this reason, under **OS Image**, access point devices indicate that an image is **Not Available**.



Audit results include:

- **Tag Golden**
  Indicates that a standardized image has not been defined for the device.

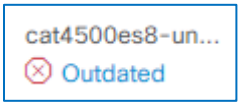
  A device cannot receive an upgrade in this state.



- **Outdated**
  Indicates that there is a standardized image available for the device and that the device is not running the standardized image and provides a link to review upgrade readiness results.

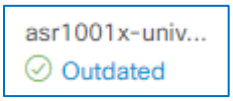
  - **Red Icon**
    Indicates that the device is failing one or more of the automated device readiness tests.

    In this case, you must correct issues causing all of the failing test statuses before you can continue.



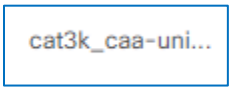
  - **Green Icon**
    Indicates that the device is passing the automated readiness checks.

    The device can receive an image upgrade in this state.



- **Compliance (without indicator)**
  Indicates that the device is using the applicable standardized image.

  The device does not need an image upgrade in this state.



…Address Audit Results?

For Devices with Tag Golden Statuses, Standardize an Image

To address devices with Tag Golden audit statuses:

- Perform the steps to standardize an image for the device family, and then evaluate the audit results.

For Individual Devices with Outdated Statuses, Review Upgrade Readiness

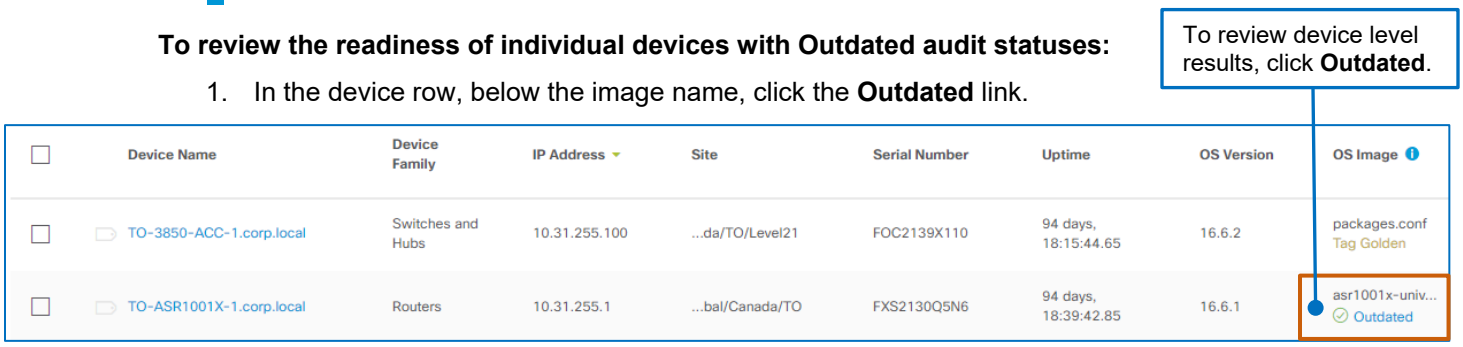
Important Note: Follow the steps in this topic to review readiness results for a single device.

Clicking **Upgrade Readiness** on the toolbar provides the readiness results for all of the devices with **Outdated** statuses, even when you select a single device in the list.

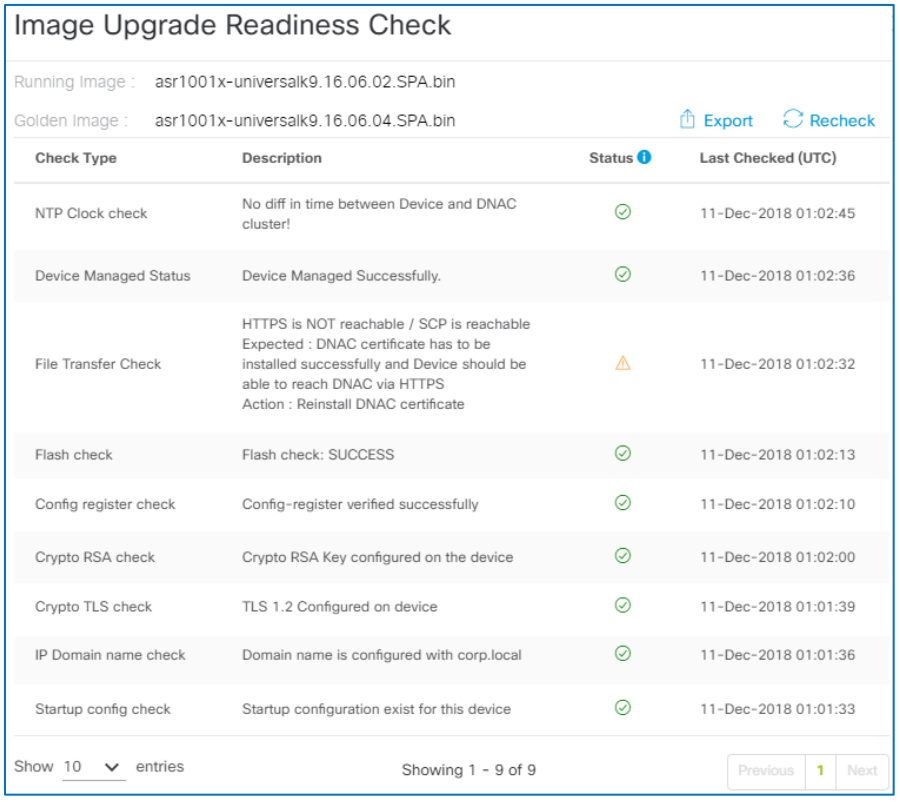
To review the readiness of individual devices with Outdated audit statuses:

1. In the device row, below the image name, click the **Outdated** link.

To review device level results, click **Outdated**.



The **Image Upgrade Readiness Check** panel opens and overlays the page, listing the readiness results for the device.

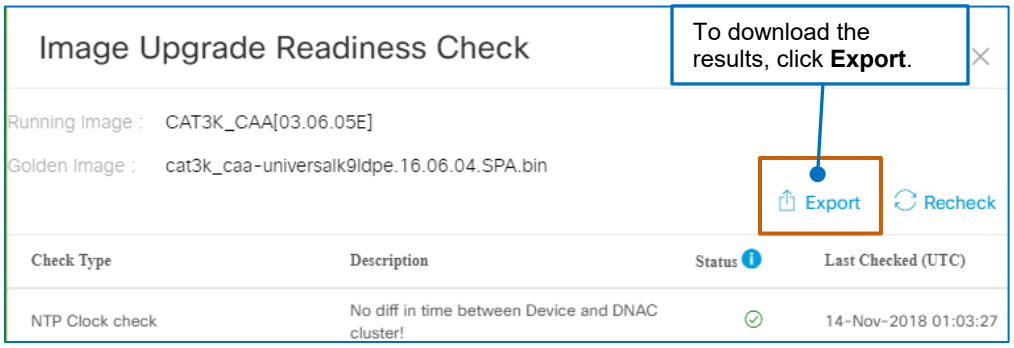


2. Based on the results:
   - If the results are successful, you can upgrade the device image.
   - If the results include failures or warnings:
     a. Take the actions that will allow the device upgrade to proceed.

Tip: You can export a .CSV file that lists the readiness results. You can use the file as a checklist to take the actions that you need.

To download the results in a .CSV file, in the **Image Upgrade Readiness Check** panel:

- Click **Export**.



     b. When any corrections that you make affect devices or their configurations, in the Inventory tool, resynchronize those devices with Cisco DNA Center, which helps ensure that the system has current data.

Note: For instructions on resynchronizing devices, refer to the **Cisco Digital Network Architecture User Guide**.

     c. When these actions are complete, in **Provision**, in the device row, click the **Outdated** link.
     d. In the **Image Upgrade Readiness Check** panel, click **Recheck**, and then review the current results.

        When the results are successful or allow you to continue, you can upgrade the device image.

When you determine that devices require an upgrade, perform the upgrade task.

For All of the Devices with Outdated Statuses, Review Upgrade Readiness

You can review the upgrade readiness results for all of the devices in the inventory that indicate **Outdated** statuses in a .CSV file. This information can be helpful for preparing devices ahead of time to help ensure that upgrades are successful.

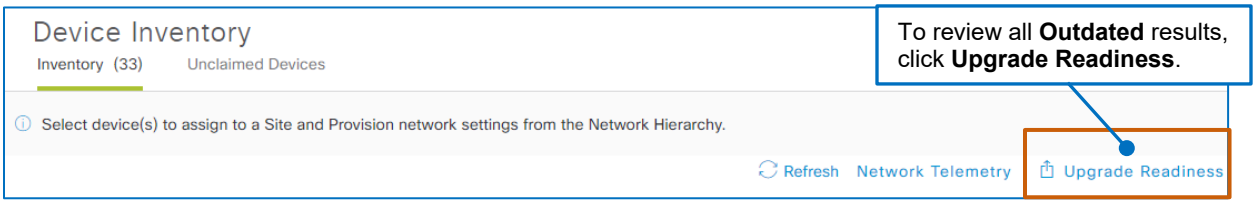
	A	B	C	D	E	F	G	H	I	J	K
1	Device IP	Device Name	DeviceType	Target Image	Target Version	Image Type	Reboot	Check Type	Description	PreCheck Status	LastChecked
2	10.0.255.42	ASR1K-CORE1	Routers	asr1000rp2-ipba	3.02.01S	SYSTEM_SW	Yes	Startup config check	Startup config check: SUCCESS : Startup configuration exist for this device	SUCCESS	12/11/2018 1:01
3	10.0.255.42	ASR1K-CORE1	Routers	asr1000rp2-ipba	3.02.01S	SYSTEM_SW	Yes	Device Managed Status	Device Managed Successfully. : Device Managed Successfully.	SUCCESS	12/11/2018 1:02
4	10.0.255.42	ASR1K-CORE1	Routers	asr1000rp2-ipba	3.02.01S	SYSTEM_SW	Yes	Config register check	Config register check: SUCCESS : Config-register verified successfully	SUCCESS	12/11/2018 1:02
5	10.0.255.42	ASR1K-CORE1	Routers	asr1000rp2-ipba	3.02.01S	SYSTEM_SW	Yes	File Transfer Check	File Transfer Check: WARNING : HTTPS is NOT reachable / SCP is reachable	WARNING	12/11/2018 1:02
6	10.0.255.42	ASR1K-CORE1	Routers	asr1000rp2-ipba	3.02.01S	SYSTEM_SW	Yes	Crypto RSA check	Crypto RSA check: FAILED : Crypto RSA Key not configured on the device	FAILED	12/11/2018 1:02
7	10.0.255.42	ASR1K-CORE1	Routers	asr1000rp2-ipba	3.02.01S	SYSTEM_SW	Yes	Flash check	Flash check: WARNING : Image Size is larger than free space	WARNING	12/11/2018 1:02
8	10.0.255.42	ASR1K-CORE1	Routers	asr1000rp2-ipba	3.02.01S	SYSTEM_SW	Yes	IP Domain name check	IP Domain name check: WARNING : Domain name is not configured for this de	WARNING	12/11/2018 1:01
9	10.0.255.42	ASR1K-CORE1	Routers	asr1000rp2-ipba	3.02.01S	SYSTEM_SW	Yes	NTP Clock check	NTP Clock check: SUCCESS : No diff in time between Device and DNAC cluster!	SUCCESS	12/11/2018 1:02
10	10.0.255.42	ASR1K-CORE1	Routers	asr1000rp2-ipba	3.02.01S	SYSTEM_SW	Yes	Crypto TLS check	Crypto TLS check: WARNING : Not enough data to check TLS1.2 support on this	WARNING	12/11/2018 1:01
11	10.30.255.1	LA1-ASR1001X-1	Routers	asr1001x-univers	16.6.4	SYSTEM_SW	Yes	Crypto RSA check	Crypto RSA check: SUCCESS : Crypto RSA Key configured on the device	SUCCESS	12/11/2018 1:01
12	10.30.255.1	LA1-ASR1001X-1	Routers	asr1001x-univers	16.6.4	SYSTEM_SW	Yes	Crypto TLS check	Crypto TLS check: SUCCESS : TLS 1.2 Configured on device	SUCCESS	12/11/2018 1:01
13	10.30.255.1	LA1-ASR1001X-1	Routers	asr1001x-univers	16.6.4	SYSTEM_SW	Yes	Startup config check	Startup config check: SUCCESS : Startup configuration exist for this device	SUCCESS	12/11/2018 1:01
14	10.30.255.1	LA1-ASR1001X-1	Routers	asr1001x-univers	16.6.4	SYSTEM_SW	Yes	Config register check	Config register check: SUCCESS : Config-register verified successfully	SUCCESS	12/11/2018 1:02
15	10.30.255.1	LA1-ASR1001X-1	Routers	asr1001x-univers	16.6.4	SYSTEM_SW	Yes	Device Managed Status	Device Managed Successfully. : Device Managed Successfully.	SUCCESS	12/11/2018 1:02
16	10.30.255.1	LA1-ASR1001X-1	Routers	asr1001x-univers	16.6.4	SYSTEM_SW	Yes	IP Domain name check	IP Domain name check: SUCCESS : Domain name is configured with corp.local	SUCCESS	12/11/2018 1:01
17	10.30.255.1	LA1-ASR1001X-1	Routers	asr1001x-univers	16.6.4	SYSTEM_SW	Yes	Flash check	Flash check: SUCCESS :	SUCCESS	12/11/2018 1:02
18	10.30.255.1	LA1-ASR1001X-1	Routers	asr1001x-univers	16.6.4	SYSTEM_SW	Yes	File Transfer Check	File Transfer Check: WARNING : HTTPS is NOT reachable / SCP is reachable	WARNING	12/11/2018 1:02
19	10.30.255.1	LA1-ASR1001X-1	Routers	asr1001x-univers	16.6.4	SYSTEM_SW	Yes	NTP Clock check	NTP Clock check: SUCCESS : No diff in time between Device and DNAC cluster!	SUCCESS	12/11/2018 1:02

The spreadsheet also indicates whether devices will reboot automatically after image activation, which can help in determining the schedule that you want to apply to activation tasks.

	A	B	C	D	E	F	G
1	Device IP	Device Name	DeviceType	Target Image	Target Version	Image Type	Reboot
2	10.0.255.42	ASR1K-CORE1	Routers	asr1000rp2-ipba	3.02.01S	SYSTEM_SW	Yes

To review the readiness of all of the devices with Outdated audit statuses:

- In **Provision**, on the **Inventory** tab, on the toolbar, click **Upgrade Readiness**, and then browse to and save the file to the local device.



The spreadsheet lists each readiness test result for each device on a separate row.

	A	B	C	D	E	F	G	H	I	J	K
1	Device IP	Device Name	DeviceType	Target Image	Target Version	Image Type	Reboot	Check Type	Description	PreCheck Status	LastChecked
2	10.0.255.42	ASR1K-CORE1	Routers	asr1000rp2-ipba	3.02.01S	SYSTEM_SW	Yes	Startup config check	Startup config check: SUCCESS : Startup configuration exist for this device	SUCCESS	12/11/2018 1:01
3	10.0.255.42	ASR1K-CORE1	Routers	asr1000rp2-ipba	3.02.01S	SYSTEM_SW	Yes	Device Managed Status	Device Managed Successfully. : Device Managed Successfully.	SUCCESS	12/11/2018 1:02
4	10.0.255.42	ASR1K-CORE1	Routers	asr1000rp2-ipba	3.02.01S	SYSTEM_SW	Yes	Config register check	Config register check: SUCCESS : Config-register verified successfully	SUCCESS	12/11/2018 1:02
5	10.0.255.42	ASR1K-CORE1	Routers	asr1000rp2-ipba	3.02.01S	SYSTEM_SW	Yes	File Transfer Check	File Transfer Check: WARNING : HTTPS is NOT reachable / SCP is reachable	WARNING	12/11/2018 1:02
6	10.0.255.42	ASR1K-CORE1	Routers	asr1000rp2-ipba	3.02.01S	SYSTEM_SW	Yes	Crypto RSA check	Crypto RSA check: FAILED : Crypto RSA Key not configured on the device	FAILED	12/11/2018 1:02
7	10.0.255.42	ASR1K-CORE1	Routers	asr1000rp2-ipba	3.02.01S	SYSTEM_SW	Yes	Flash check	Flash check: WARNING : Image Size is larger than free space	WARNING	12/11/2018 1:02
8	10.0.255.42	ASR1K-CORE1	Routers	asr1000rp2-ipba	3.02.01S	SYSTEM_SW	Yes	IP Domain name check	IP Domain name check: WARNING : Domain name is not configured for this de	WARNING	12/11/2018 1:01
9	10.0.255.42	ASR1K-CORE1	Routers	asr1000rp2-ipba	3.02.01S	SYSTEM_SW	Yes	NTP Clock check	NTP Clock check: SUCCESS : No diff in time between Device and DNAC cluster!	SUCCESS	12/11/2018 1:02
10	10.0.255.42	ASR1K-CORE1	Routers	asr1000rp2-ipba	3.02.01S	SYSTEM_SW	Yes	Crypto TLS check	Crypto TLS check: WARNING : Not enough data to check TLS1.2 support on this	WARNING	12/11/2018 1:01

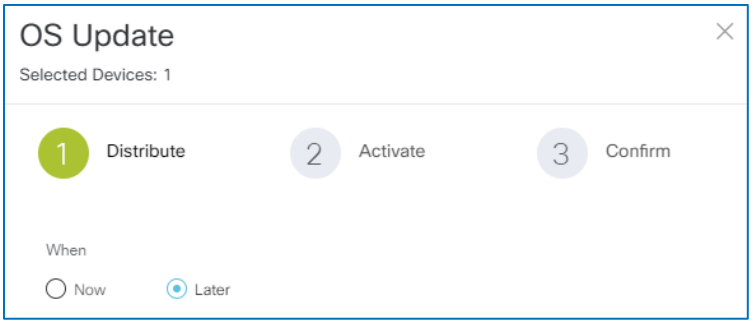
Under **Target Image** and **Target Version**, it also indicates the standardized, golden image and version for each device.

	A	B	C	D	E
1	Device IP	Device Name	DeviceType	Target Image	Target Version
2	10.0.255.42	ASR1K-CORE1	Routers	asr1000rp2-ipbasek9.03.02.01.S.151-1.S1.bin	3.02.01S

When you determine that devices require an upgrade, perform the upgrade task.

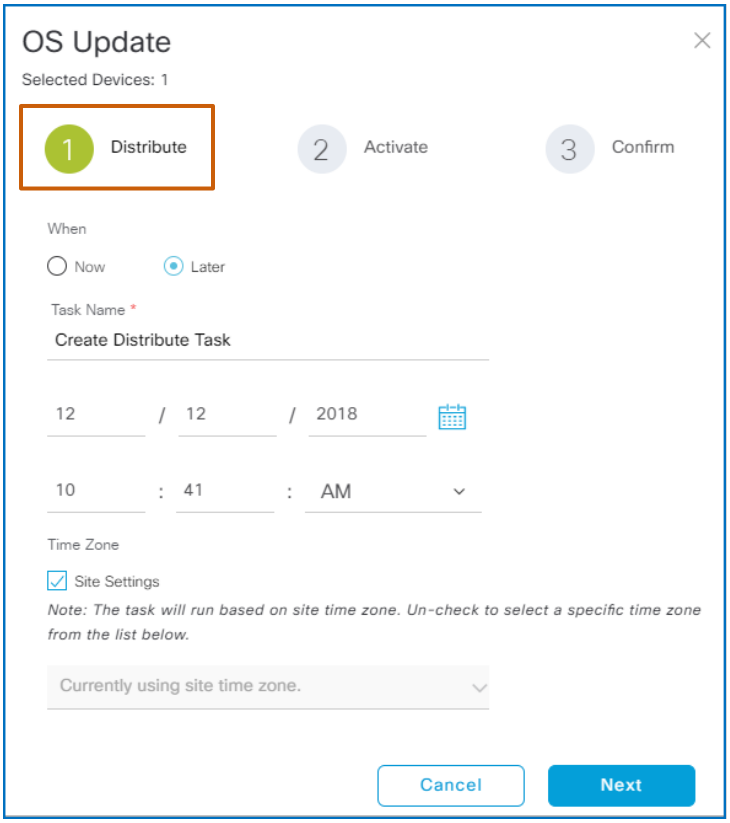
…Upgrade Devices?

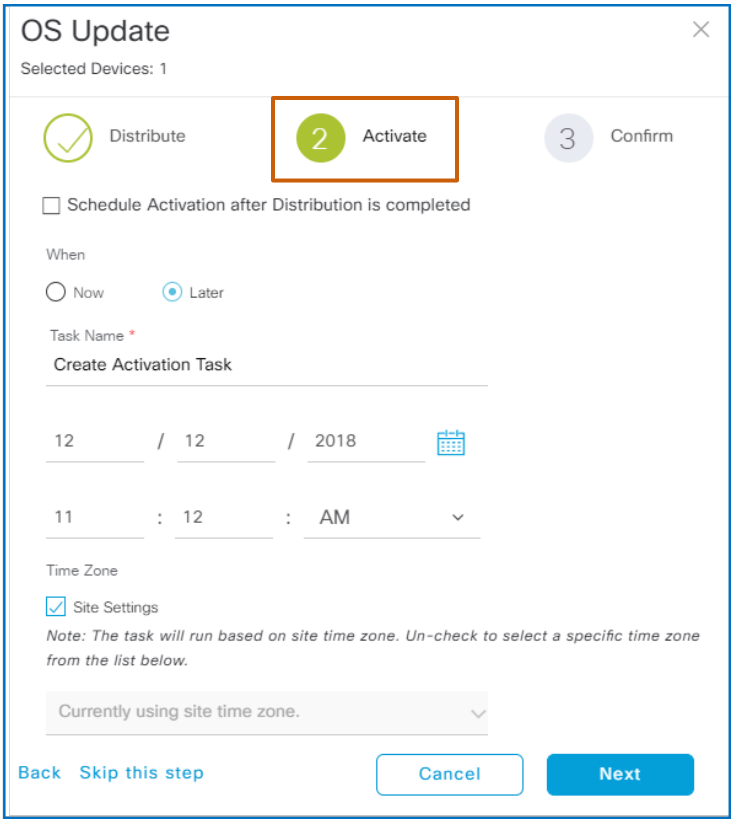
You can configure and schedule distribution and activation tasks so that they run sequentially or occur following a schedule by using the **OS Update** wizard. Scheduling the tasks separately is helpful, for example, when the enterprise wants to distribute images during business hours, and schedule activation during a maintenance window.



You also can configure distribution and activation tasks as separate activities, for example, when you are distributing images in preparation for an activation that needs to occur at an undetermined time.

The steps that you take to configure the distribution and activation tasks are similar.





Task 1A: Select Devices and Open the OS Update Panel

Notes: When establishing device connectivity to support image distribution, Cisco DNA Center first uses the HTTPS protocol.

In case of failure, for routers and switches, it attempts to establish communication by using the SCP protocol,

For WLCs, it attempts to establish communication by using the SFTP protocol.

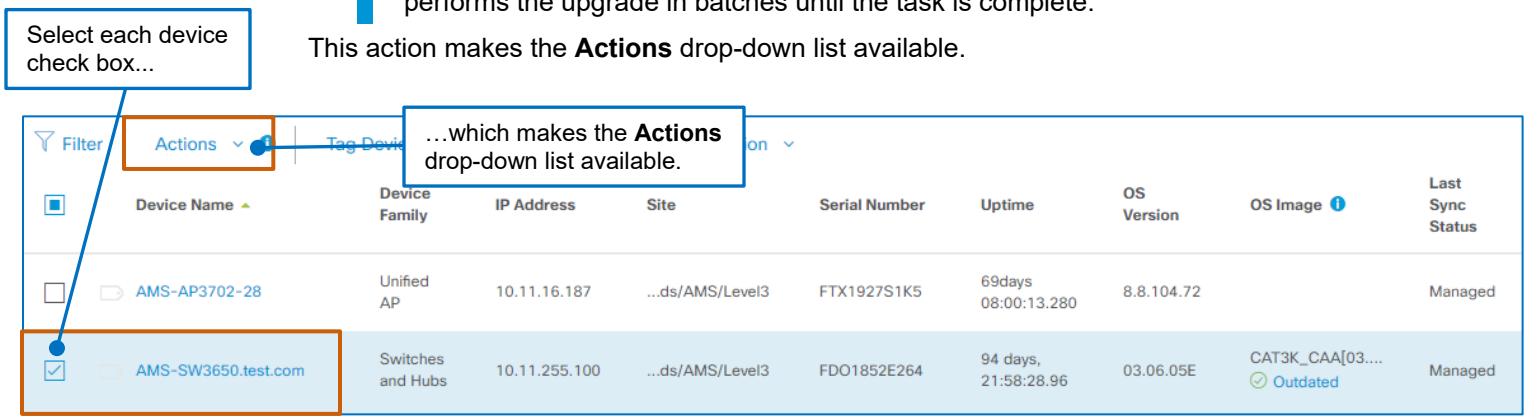
When you are distributing or activating images on more than 25 devices, Cisco DNA Center performs the task in batches of 25 devices in parallel.

To configure the distribution task devices:

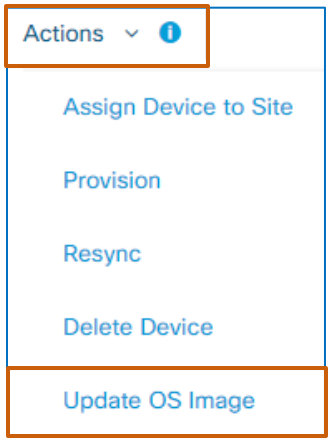
1. In the list, beside the **Device Name** field of each non-compliant device, select the check box.

   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.



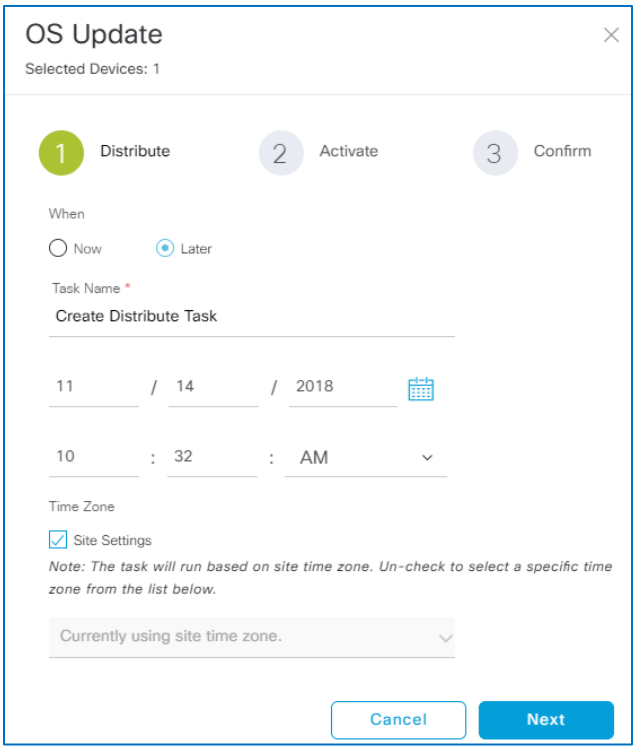
2. In the **Actions** drop-down list, select **Update OS Image**.



The **OS Update** panel opens and provides a wizard to step you through the process. You can distribute and activate images separately and can schedule each action based on operational requirements.

Note: When you need to upgrade a group of devices, and some of those devices have the image file because it was distributed in a previous task, while others do not yet have the image file, the **OS Update** panel opens the **Distribute** task and indicates that there are devices that require image distribution.

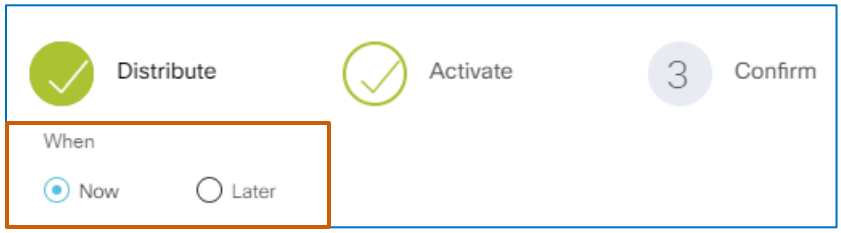
You need to configure the distribution task for those images, and then you can configure the activation task for all of the devices in the same upgrade task or in a separate activation task.



Task 1B: Configure the Distribution Task

To configure the distribution task:

1. To indicate when you want the task to run, below **When**:

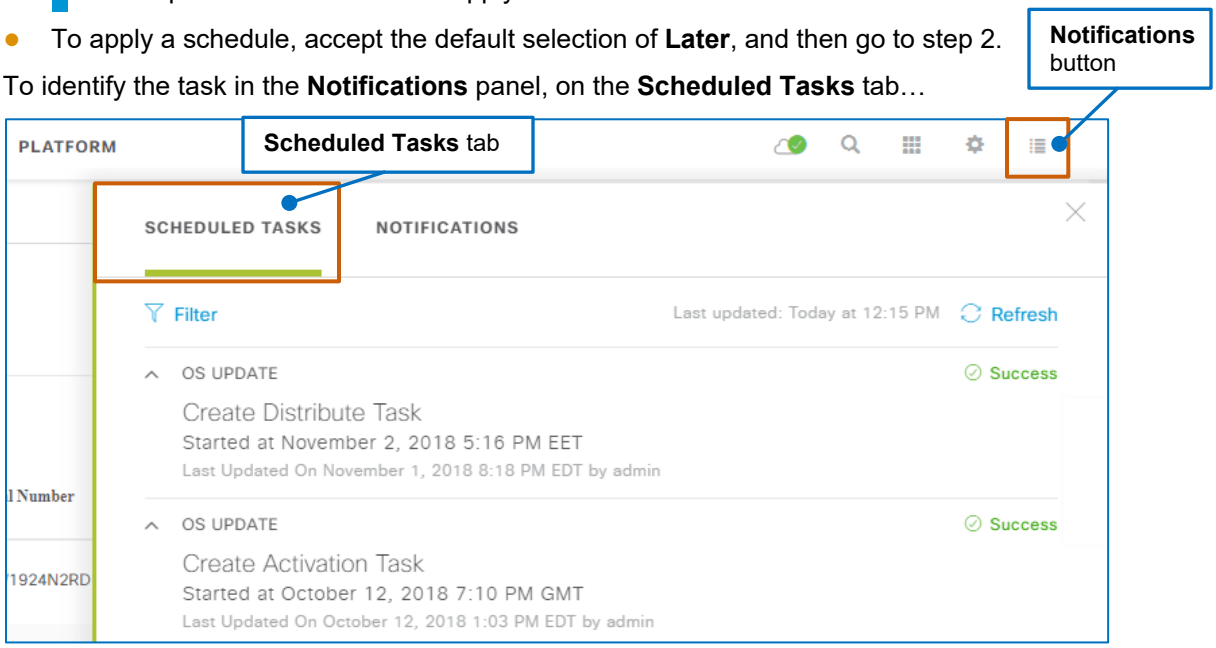


- To run it immediately, click **Now**. Go to step 5.

Note: This action collapses the task naming and scheduling options, and Cisco DNA Center applies the task name **Create [Distribution/Activation] Task** automatically.
A unique task name does not apply.

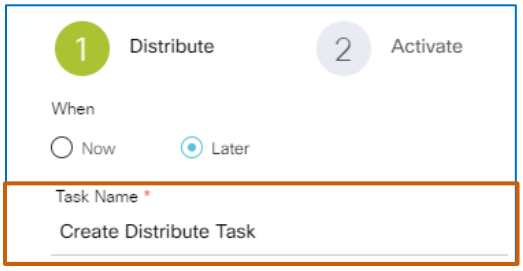
- To apply a schedule, accept the default selection of **Later**, and then go to step 2.

2. To identify the task in the **Notifications** panel, on the **Scheduled Tasks** tab…

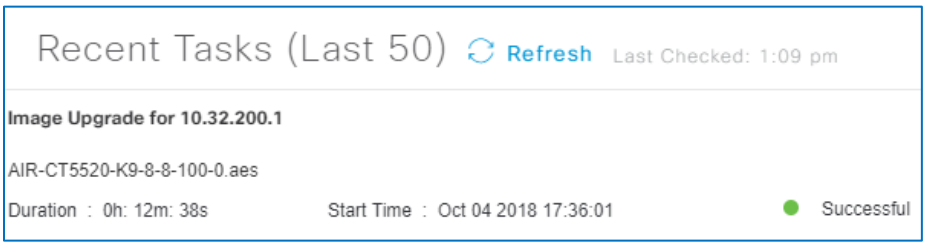


…in the **Task Name** field:

- Accept the default task name
- Type a meaningful name for the task.

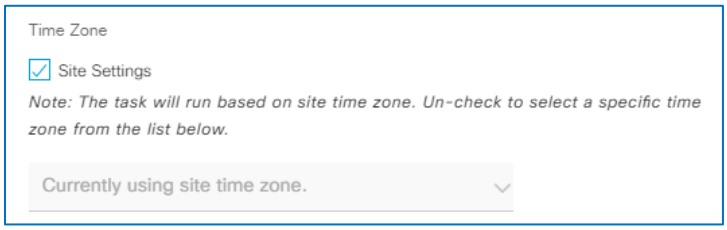


Note: This name does not appear in the **Recent Tasks** panel that opens when you click **Update Status**.



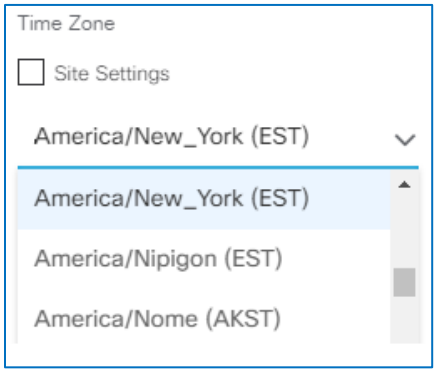
3. Below the task name, select the date and time that you want distribution to occur.
4. To indicate the time zone on which to base the date and time schedule and in which the task will occur:

- To have the task occur in the device's local time zone, which can result in the tasks occurring on varying schedules based on device location, accept the default selection of **Site Settings**.



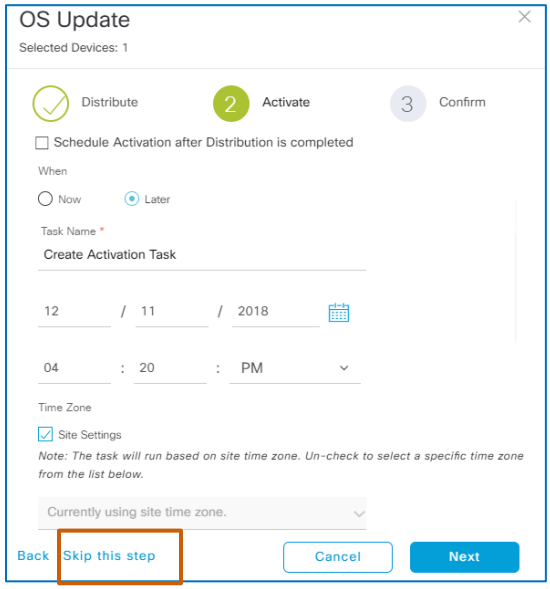
- To select a different time zone that will apply to the schedule for all of the devices included in the task, clear the **Site Settings** check box, and then, in the drop-down list, select the time zone.

Note: When you apply a specific time zone, the system distributes the image to, or activates the image on, all of the devices that you include in the task based on the time that you indicated in step 3 and in the time zone that you select here.

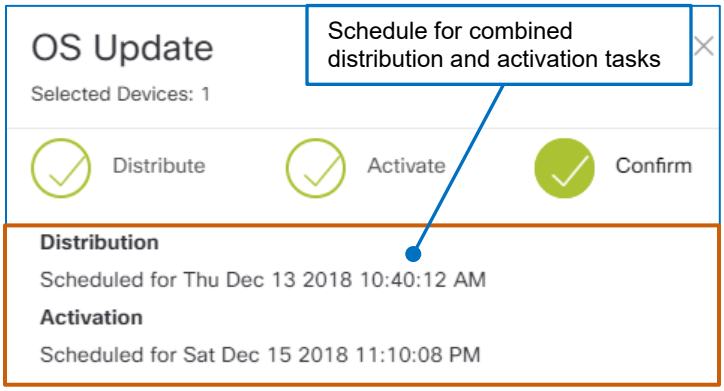


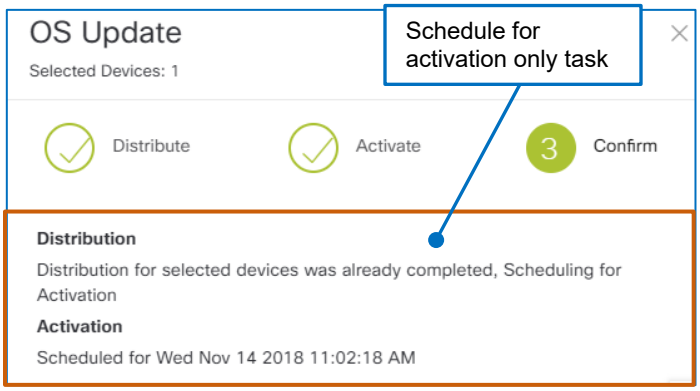
5. To continue, click **Next**, and then:
   - To distribute the image only, go to step 6.
   - To configure the activation task, go to task 1C, and then go to step 7.
   - To continue the process after configuring the activation task, go to step 7.

6. On the **Activate** page, click **Skip This Step**.



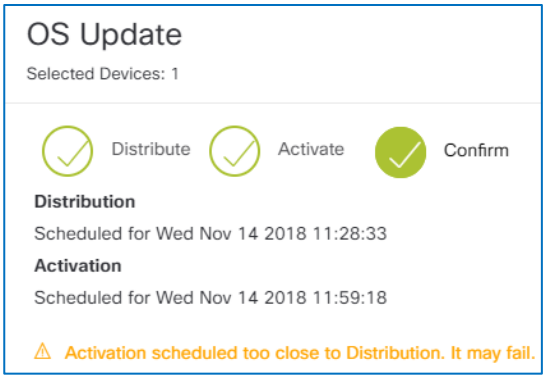
7. To continue, on the **Confirm** page, review the scheduling information.





Note: On the **Confirm** page, Cisco DNA Center can present generic courtesy messages that indicate possible task outcomes based on general factors.

For example, the message below indicates a possible outcome based on the schedules of combined distribution and activation tasks. It is based on schedule timing only; no pre-testing occurred to determine the possible outcome that the message indicates.



8. After you review the scheduling information:

   - To schedule or start the task based on your settings, click **Confirm**.

     When you are starting tasks immediately, you can review the tasks statuses and results.

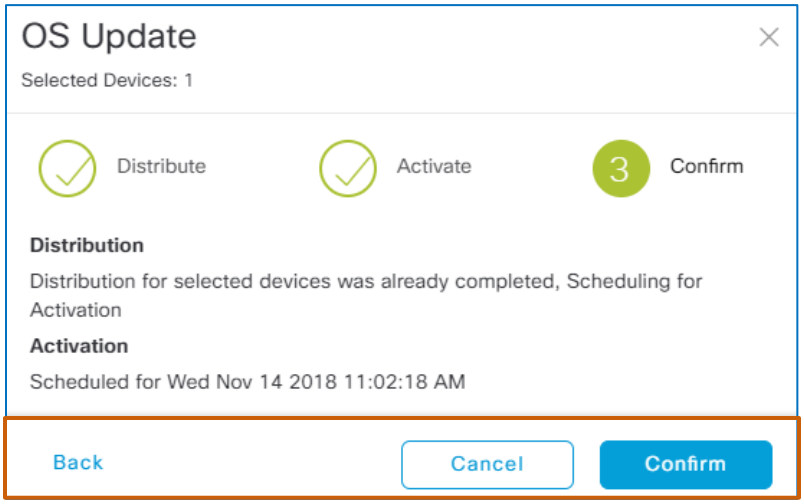
     When you are scheduling tasks to run later, you can review the pending tasks.

   - To adjust the task or schedule, click **Back**.

     The wizard returns to the **Activate** page.

   - To cancel the task, click **Cancel**.

     The panel closes automatically, and Cisco DNA Center discards the task configuration.



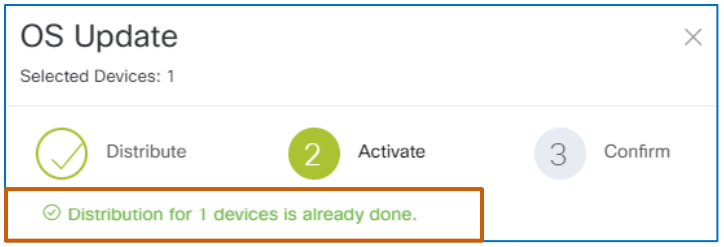
When you need to configure an activation task, go to task 1C.

When you have finished configuration, you can review pending, ongoing, or completed tasks and task results.

Task 1C: Configure the Activation Task

When you configure activation tasks, the process addresses previously distributed or undistributed images based on the devices that you select.

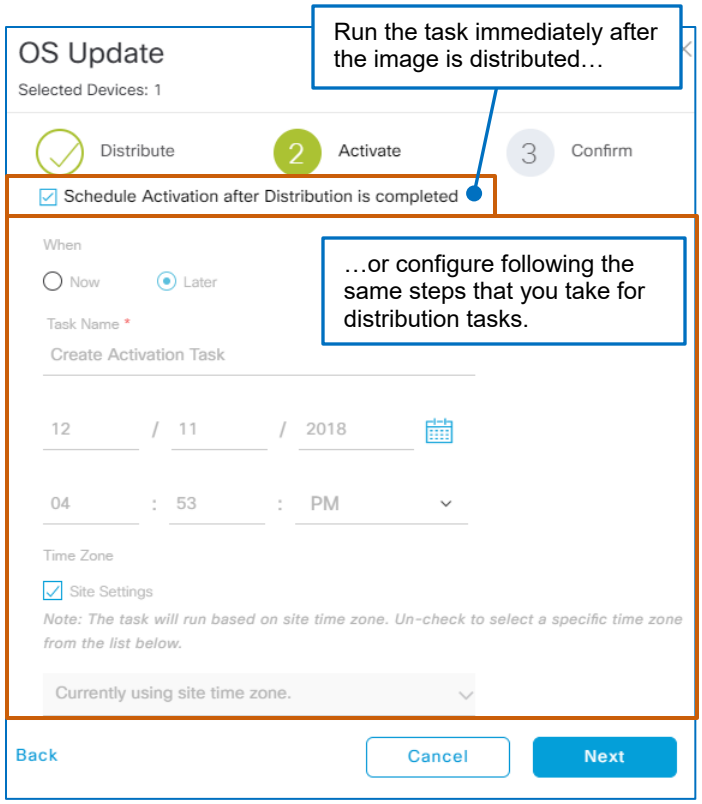
When the image that you need to activate was distributed previously to the devices that you select, the wizard indicates the completed distribution task and opens the **Activate** step in the wizard automatically.



When you select a group of devices in which some contain the image that you need to activate and other do not, the process automatically attempts to distribute the image to those devices without the image in the activation process.

To configure an activation task:

1. Determine whether the image was distributed previously in a separate task.
   - If the image was distributed in a separate task, follow the steps to select the device or devices with the images that you need to activate and open the OS Update panel, and then go to step 2.
   - If you are configuring the distribution and activation tasks at the same time, go to step 2.
2. In the **OS Update** panel, on the **Activate** page:
   - To run the task immediately after the image is distributed, select the **Schedule Activation after Distribution is completed** check box, and then, follow the steps to validate what you configured.
   - To configure the task to run immediately or following a schedule, follow the steps to configure and validate the task.



…Review Pending, Ongoing, or Completed Tasks and Task Results

You can review information about pending or ongoing distribution, activation, or upgrade tasks.

Note: Upgrades refer to combined distribution and activation tasks that a system user configured at the same time in the **OS Update** wizard.

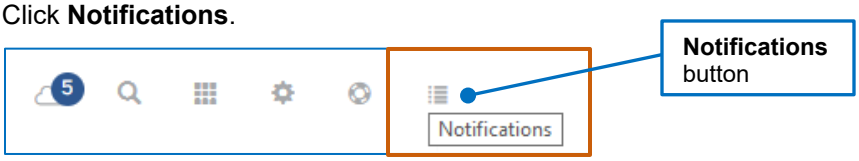
On task completion, you can review the results to determine whether the task was successful, completed with issues, or failed.

This chapter addresses various actions that you can take to find the information that you need.

Review the List of Pending, or Scheduled, Tasks

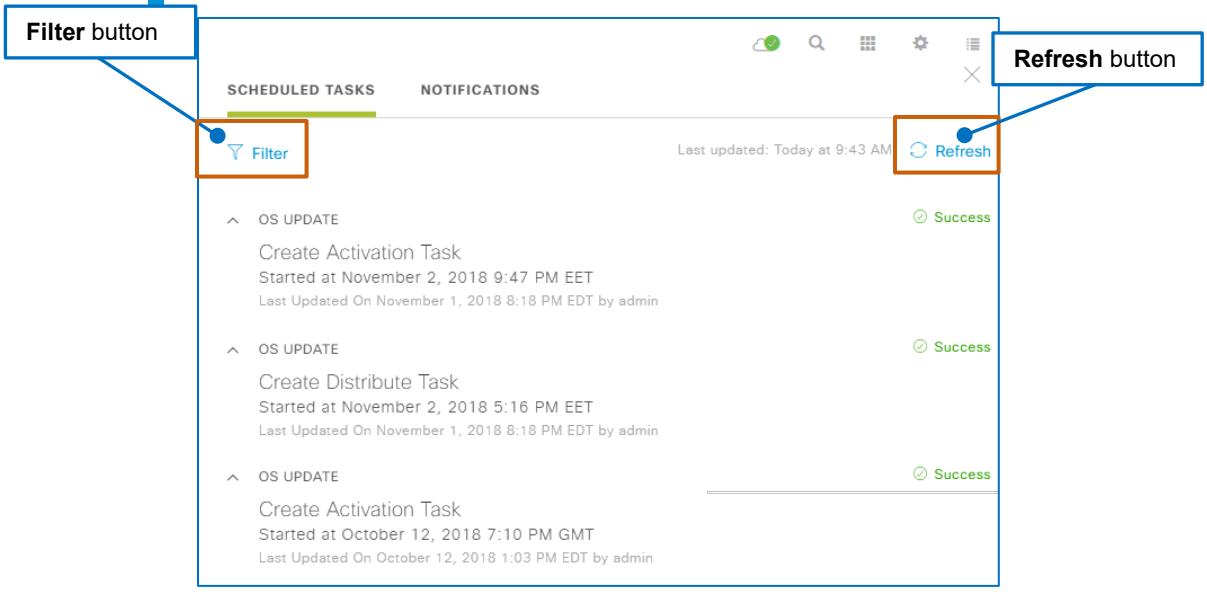
To see a list of tasks that are scheduled, on the application toolbar:

1. Click **Notifications**.

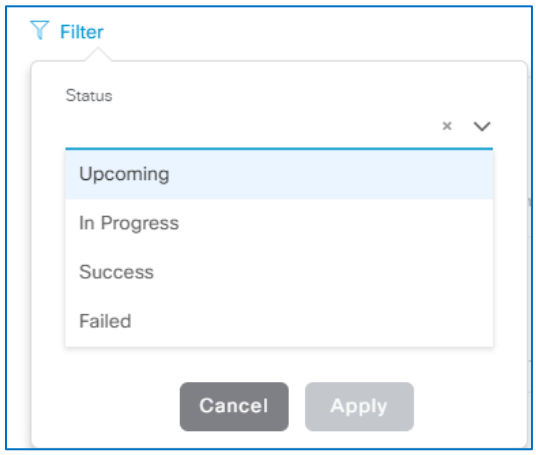


A panel opens and overlays that page. The **Scheduled Tasks** tab lists all of the image-related tasks, including those tasks that have completed based on a schedule.

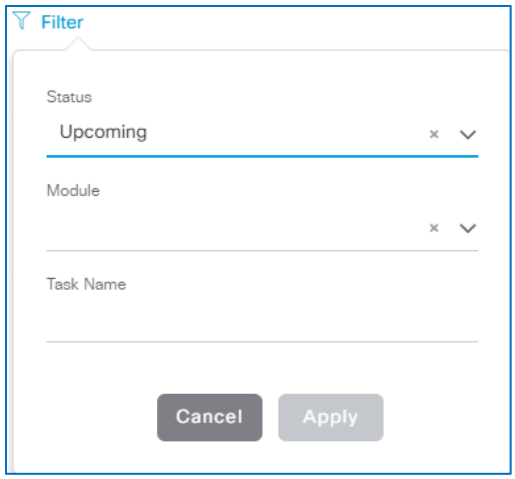
Note: The panel lists the 25 most recently run image management tasks. You can refresh the list to ensure that you are seeing current information. You also can apply filters to find a specific task more efficiently.



2. On the **Scheduled Tasks** tab, click **Filter**, and then, in the **Status** drop-down list, select **Upcoming**.



3. Click **Apply**.



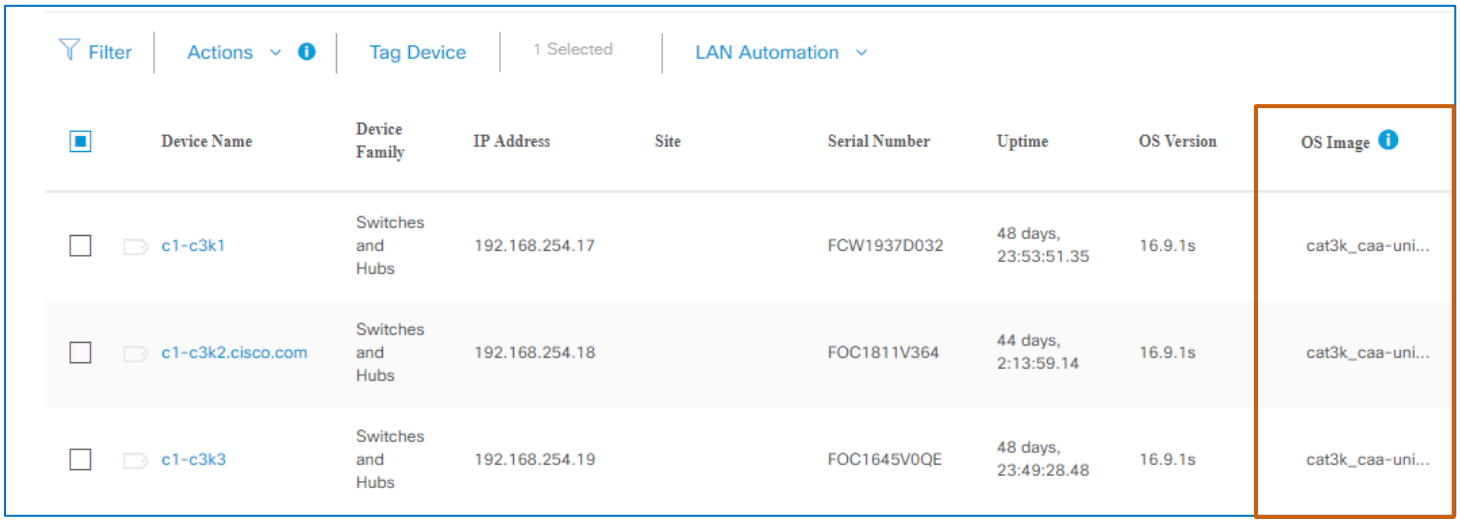
The filter closes and the list updates automatically to display only those tasks with the **Upcoming** status.

Determining Success of Activation or Upgrade Tasks

To determine whether an activation task was successful, on the Inventory tab:

- In the device list, for each device of interest, review the **OS Image** column.

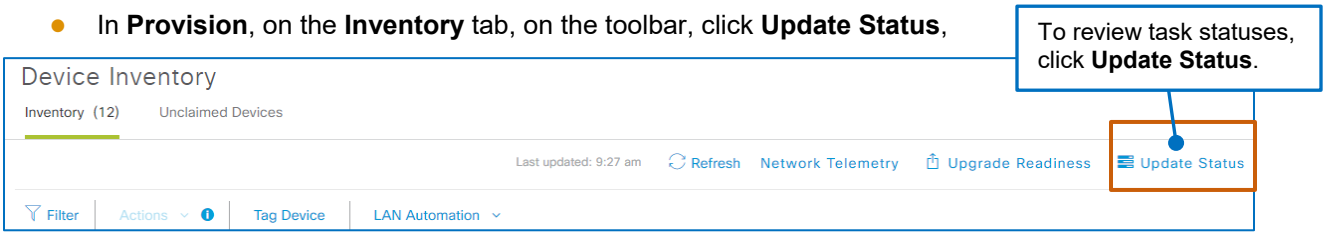
  When the **Outdated** status no longer appears below the image name in the device's **OS Image** column, the device is running the standardized image successfully.



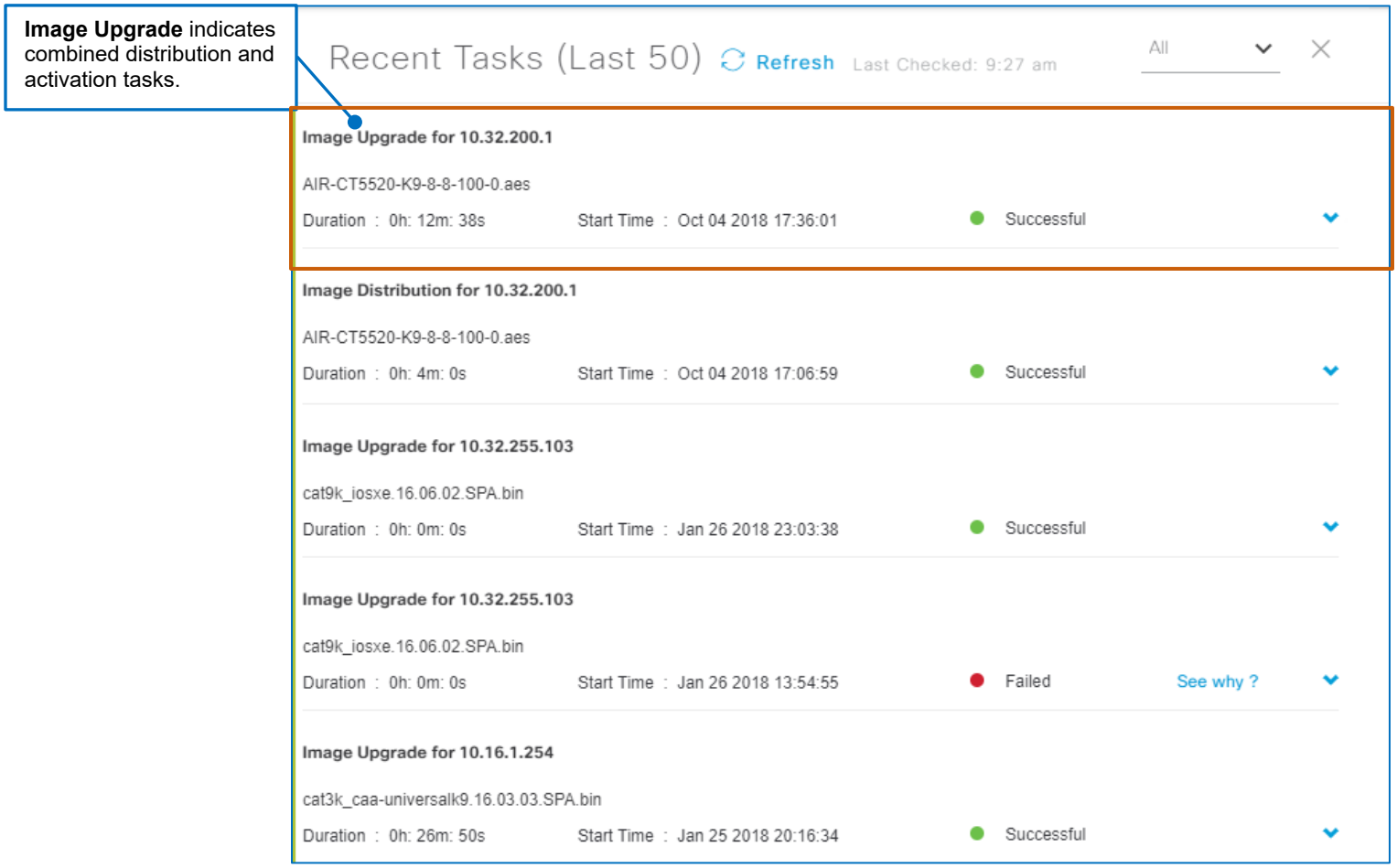
Reviewing Immediately Scheduled, Ongoing, Or Completed Task Results

To review detailed information for ongoing or completed distribution, activation or upgrade tasks:

- In **Provision**, on the **Inventory** tab, on the toolbar, click **Update Status**,



The **Recent Tasks** panel opens and lists the IP address of each device on which a distribution, activation, or combined upgrade task is running or has completed.



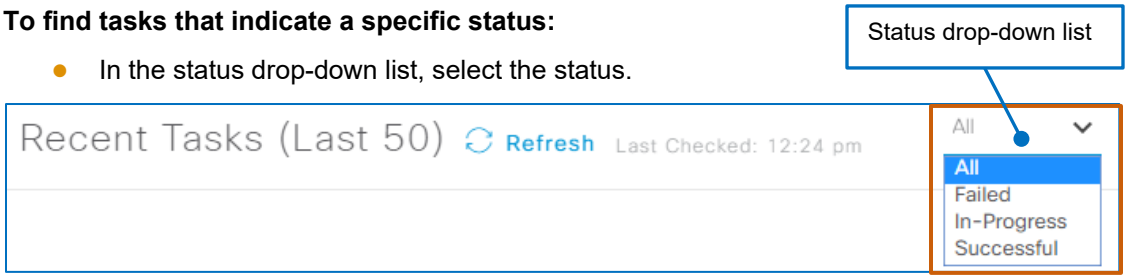
When more than one device is included in distribution and activation tasks, the system indicates each device's status for each task separately when each task is complete.

The list of devices can indicate the following task statuses:

- **Successful**
  Indicates that the task is complete, and the device is running the golden image or add-on
- **In-Progress**
  Indicates that the system is in the process of executing the task
- **Failed**
  Indicates that while executing the task, an issue has occurred that caused the task to fail

To find tasks that indicate a specific status:

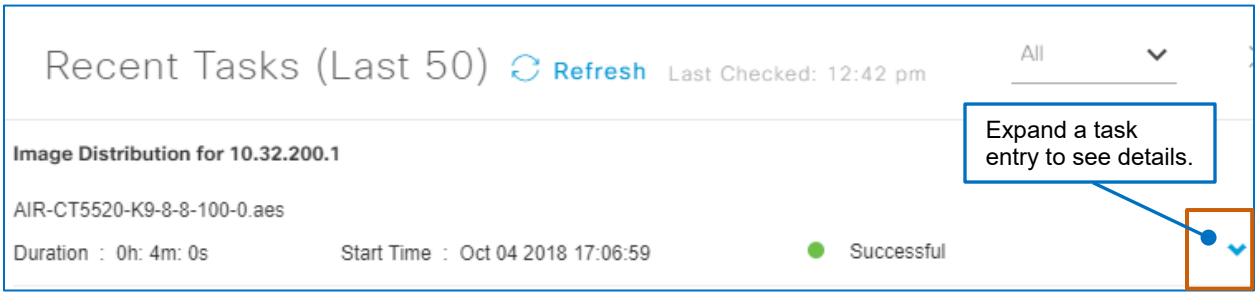
- In the status drop-down list, select the status.



The list updates automatically to display the tasks that match the criteria.

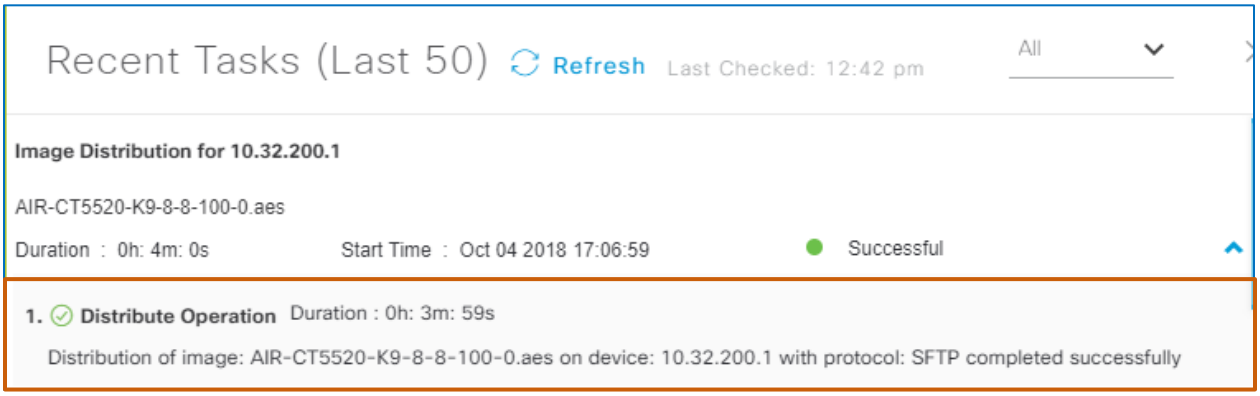
To review task details:

- Expand the entry.

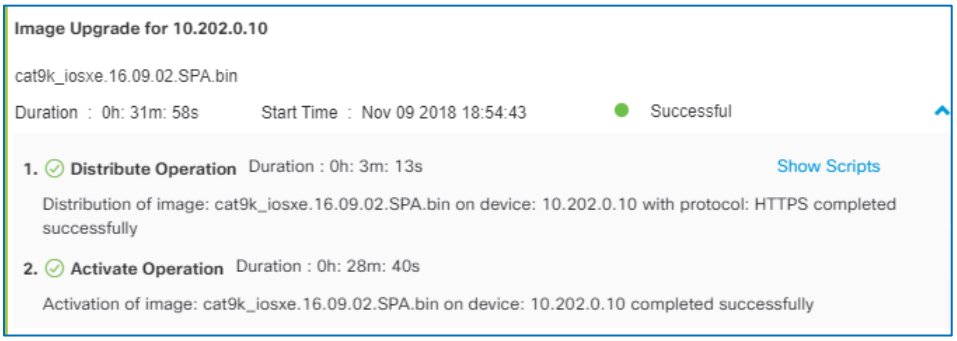


In the list, additional information expands below the entry. The type of information that you see is based on the type of task and its status.

When a task is a single distribution or activation operation and is successful, image, device, protocol and status details appear below the entry.



When a task is combined upgrade operation that includes image distribution and activation, the details list the two dependent tasks and their statuses separately.

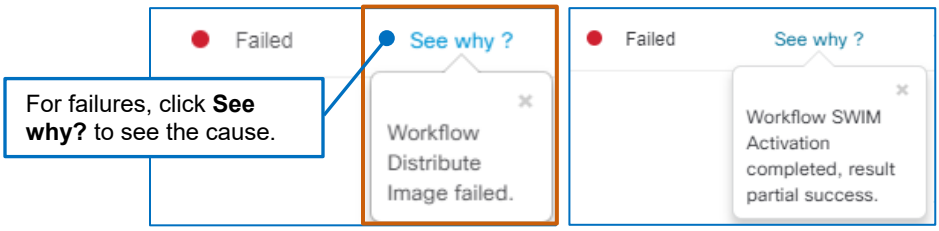


For **Failed** status, the information includes the cause and point in the process at which the failure occurred.

To see summary failure information:

- Beside the **Failed** status indicator, click **See why?**

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



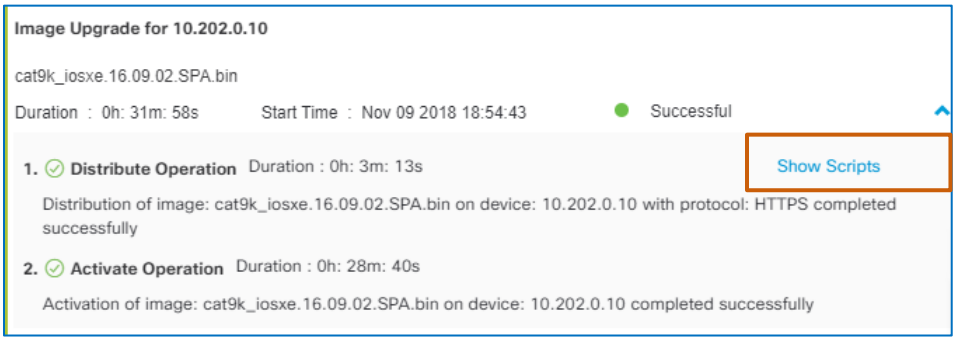
In most cases, Cisco DNA Center runs a **CPU Health Check** test before executing the task.

Script Name	Type	Log Details
✔ CPU Health Check	Pre Check	View

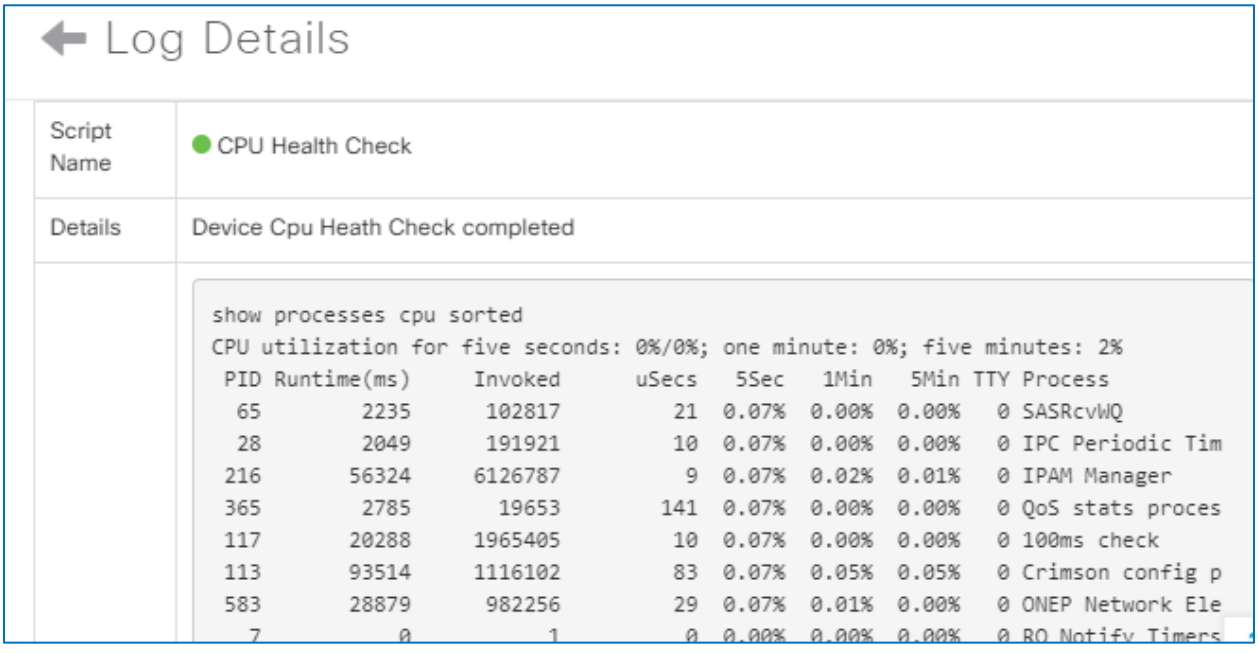
A single **Show Scripts** link is available for activation or combined distribution and activation tasks.

Note: In some cases, the script is not available for tasks. For example, this test does not apply to WLCs.

Future release of Cisco DNA Center will make additional pre-task and post-task scripts available.



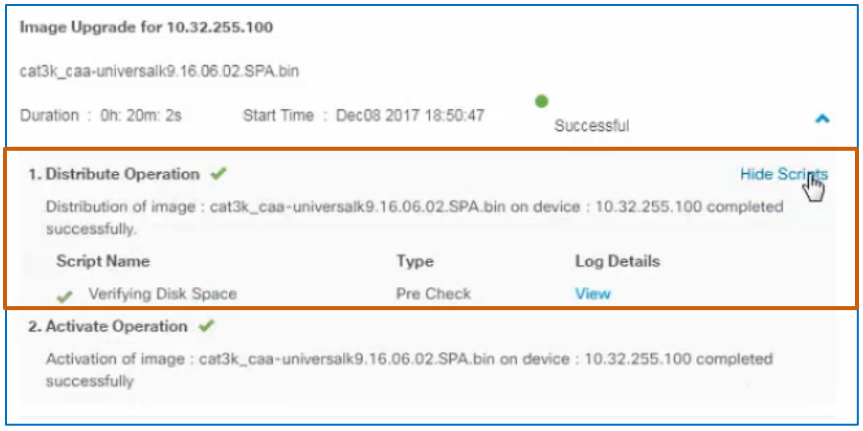
You also can see the log of the data that the script collected before running the task.



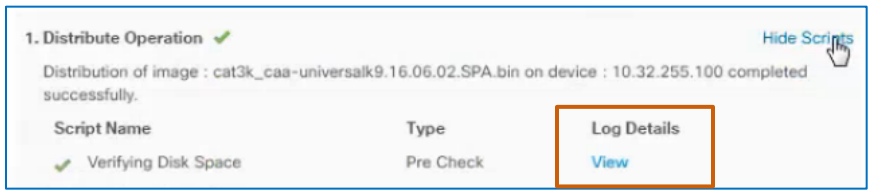
To see scripts or associated logs:

1. Expand a task entry, and beside the operation, click **Show Scripts**.

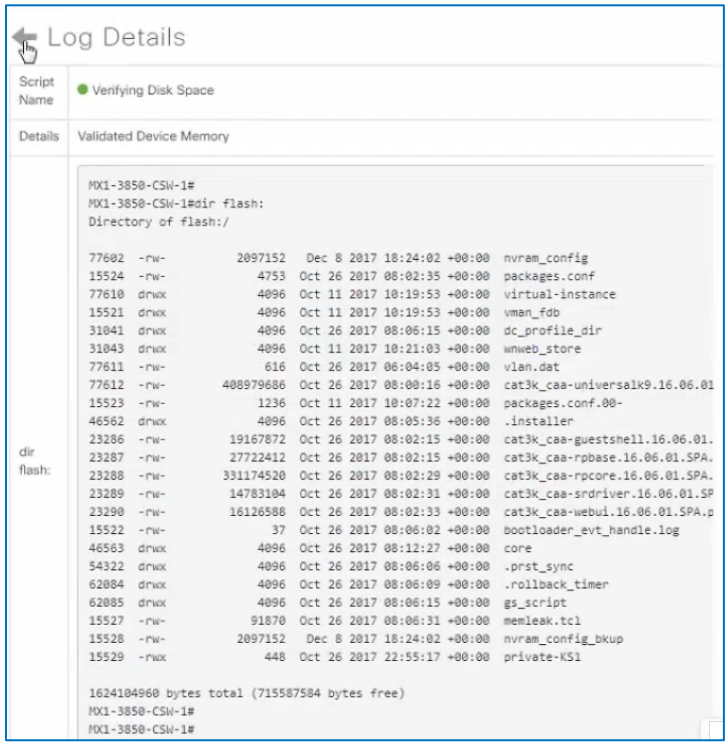
   The section expands and lists the script or scripts that ran.



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



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



Want More?

Find 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**.

Find 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.

Contact Us About This Training

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

Note: Please send messages that address training content only.

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