



Image Management

LAN, Release 12.2.2

Table of Contents

New and Changed Information	1
Image Management	2
Overview	4
Images	5
Uploading an Image	6
Image Policies	8
Creating an Image Policy	8
Devices	10
Staging an Image	10
Validating an Image	10
Upgrading an Image	11
Change the Mode	12
Modifying the Groups	13
Modifying a Policy	14
Recalculating Compliance	14
Run Reports	14
Generate Snapshot	15
History	16
Copyright	17

New and Changed Information

The following table provides an overview of the significant changes up to this current release. The table does not provide an exhaustive list of all changes or of the new features up to this release.

Release Version	Feature	Description
There were no major changes from the previous release.		

Image Management

Upgrading your devices to the latest software version manually might take a long time and prone to error, which requires a separate maintenance window. To ensure rapid and reliable software upgrades, image management automates the steps associated with upgrade planning, scheduling, downloading, and monitoring.



- Before you upgrade, ensure that the POAP boot mode is disabled for Cisco Nexus 9000 Series switches and Cisco Nexus 3000 Series switches. To disable POAP, run the `no boot poap enable` command on the switch console. You can however, enable it after the upgrade.
- In order to execute any ISSU operations, any new NDFC user must first set the necessary device credentials in Credential Management. You will not be able to execute ISSU operations without setting the device credentials.

The **Image Management** window has the following tabs. You can perform the operations listed in the Actions column.

Tabs	Actions
Overview	You can view dashlets for uploading an image and related information.
Images	Uploading an Image
Image Policies	Creating an Image Policy
Devices	Staging an Image Validating an Image Upgrading an Image Change the Mode Modifying a Policy Recalculating Compliance Run Reports
History	History

Ensure that your user role is **network-admin** or **device-upg-admin** and that you do not freeze Nexus Dashboard Fabric Controller to perform the following operations:

- Upload or delete images.
- Install, delete, or finish installation of an image.
- Install or uninstall packages and patches.
- Activate or deactivate packages and patches.
- Add or delete image management policies (applicable only for **network-admin** user role).
- View management policies.

You can view any of the image installations or device upgrade tasks if your user role is **network-admin** or **device-upg-admin**. You can also view them if your Nexus Dashboard Fabric Controller is in freeze mode.

Follow these steps to upgrade the switch image:

1. Discover the switches into Nexus Dashboard Fabric Controller.
2. Upload images.
3. Create image policies.
4. Attach the image policies to the switches.
5. Stage the images on switches.
6. (Optional) Validate if the switches support non-disruptive upgrade.
7. Upgrade the switches accordingly.

Overview

Choose **Manage > Fabric Software > Overview**.

In the **Overview** tab, you can view dashlets for uploading images, policies, fabric status, and Switch Upgrade group status.

The tab lists the procedures and link to upload an appropriate image and configure the required properties for an image.

Images


You can view the details of the images and the platform under this tab. You can upload or delete images to a device.

The following table describes the fields that appear on **Manage > Fabric Software > Images**.

Field	Description
Platform	<p>Specifies the name of the platform. Images, RPMs, or SMUs are categorized as follows:</p> <ul style="list-style-type: none">▪ CAT9K▪ N9K/N3k▪ N6K▪ N7K▪ N77K▪ N5K▪ Other▪ Third-party <p>The images are the same for N9K and N3K platforms.</p> <p>The platform is Other if the uploaded images are not mapped to any of the existing platforms.</p> <p>The platform is N9K/N3K for RPMs.</p>
Bits	Specifies the bits of the image.
Image Name	Specifies the file name of the image, RPM, or SMU that you uploaded.
Image Type	Specifies the file type of the image, EPLD, RPM, or SMU.
Image Sub Type	<p>Specifies the sub type of the image, EPLD, RPM, or SMU.</p> <p>The file type EPLDs are epld. The file types of images are iosxe, nxos, system or kickstart. The file type for RPMs is feature and for SMUs the file type is patch.</p>
NOS Version	Specifies the NOS image version for the Cisco switches.
Image Version	Specifies the image version for all devices, including the non-Cisco devices.
Size (Bytes)	Specifies the size of the image, RPM, or SMU files in bytes.
Reference Count	

Field	Description
Checksum	<p>Specifies the checksum of the image.</p> <p>The checksum checks if there are any corruptions in the file of the image, RPM, or SMU. You can validate the authenticity by verifying if the checksum value is same for the file you downloaded from the Cisco website and the file you upload in the Image Upload window.</p>

The following table describes the action items, in the **Actions** menu drop-down list, that appears on **Manage > Fabric Software > Images**.

Action Item	Description
Upload	Click to upload a new image. For instructions, see Uploading an Image .
Delete	<p>Allows you to delete the image from the repository.</p> <p>Choose an image, click Actions, and choose Delete. A confirmation window appears. Click Yes to delete the image.</p> <div style="display: flex; align-items: center;">  <ul style="list-style-type: none"> ▪ Before deleting an image, ensure that the policy attached to the image, is not attached to any switches. ▪ If you delete an image on a switch in the switch console, allow a maximum of 24 hours to refresh and view updates on NDFC. Else, on the NDFC UI, navigate to Manage > Fabrics > Switches, choose the switch for which the image is deleted and choose Actions > Discover > Rediscover to view the updates. </div>

Uploading an Image

You can upload 32-bit and 64-bit images. To upload different types of images to the server from the Cisco Nexus Dashboard Fabric Controller Web UI, perform the following steps:



- Devices use these images during POAP or image upgrade.
- Your user role should be **network-admin**, or **device-upg-admin** to upload an image.

1. Choose **Manage > Fabric Software > Images**.
2. Click **Actions** and choose **Upload**.

The **Upload Image** dialog box appears.

3. You can upload the file from a local directory, import from SCP or SFTP.

4. Click **Choose file** to choose a file from the local repository of your device.
5. Choose the file and click **Verify**.

You can upload a ZIP or TAR file as well. Cisco Nexus Dashboard Fabric Controller processes and validates the image file and categorizes it under the existing platforms accordingly. If it doesn't fall under **CAT9K**, **N9K/N3K**, **N6K**, **N7K**, **N77K**, or **N5K** platforms, the image file is categorized under **Third Party** or **Other** platform. The **Third Party** platform is applicable only for RPMs.

6. Click **OK**.

The EPLD images, RPMs, and SMUs are uploaded to the repository in the following path:
`/var/lib/dcnm/upload/<platform_name>`

All NOS, kickstart and system images are uploaded to the repository in the following paths:
`/var/lib/dcnm/images` and `/var/lib/dcnm/upload/<platform_name>`

The upload takes some time depending on the file size and network bandwidth.




- o You can upload images for all Cisco Nexus and Cisco Catalyst Series switches.
- o You can upload EPLD images only for Cisco Nexus 9000 Series switches.

Image Policies

The image management policies will have the information of intent of NOS images along with RPMs or SMUs. The policies can belong to a specific platform. Based on the policy applied on a switch, Cisco Nexus Dashboard Fabric Controller checks if the required NOS and RPMs or SMUs are present on the switch. If there is any mismatch between the policy and images on the switch, a fabric warning is generated.

The following table describes the action items in the **Actions** list, that appears on **Manage > Fabric Software > Image Policies**.

Action Item	Description
Create	Allows you to create a policy that can be applied to images. See Creating an Image Policy section.
Delete	<p>Allows you to delete the policy.</p> <p>Choose a policy, click Actions, and choose Delete. A confirmation window appears. Click Confirm to delete the policy.</p> <div style="display: flex; align-items: center;"><p>An error message appears if you try to delete a policy that is attached to a device.</p></div>
Edit	Allows you to edit the policy.

Creating an Image Policy

To create an image policy from the Cisco Nexus Dashboard Fabric Controller Web UI, perform the following steps:

Before you begin:

Upload the images under the **Images** tab before creating an image policy. See [Uploading an Image](#) for more information about uploading images.

1. Choose **Manage > Fabric Software > Image Policies**.
2. Click **Actions > Create**.

The **Create Image Management Policy** dialog box appears.

3. Enter information for the required fields.

The following fields appear in the **Create Image Management Policy** dialog box.

Fields	Actions
Policy Name	Enter the policy name.

Fields	Actions
Platform	Choose a platform from the list. The options will be populated based on the images you upload. The options for the Release drop-down list will be auto-populated based on the platform you choose.
Release	Choose the NOS version from the list. The release versions of 64-bit images are appended with 64-bit in the image name.
Package Name	(Optional) Choose the packages. Before you choose a package, View All Packages check box to display all the uploaded packages for a given platform (version agnostic).
Policy Description	(Optional) Enter a policy description.
EPLD	(Optional) Check the EPLD check box if the policy is for an EPLD image.
Select EPLD	(Optional) Choose the EPLD image.
RPM/SMU Disable	(Optional) Check this check box to uninstall the packages.
RPMs/SMUs To Be Uninstalled	(Optional) Enter the packages to be uninstalled separated by commas. You can enter the package names only if you check the RPM Disable checkbox.

4. Click **Save**.

What to do next:

- If you need to edit an image policy that you created, select the policy, then click **Actions > Edit**.
- If you need to delete an image policy that you created, select the policy, then click **Actions > Delete**.
- Attach the policy to a device, if necessary. See [Modifying a Policy](#) for more information.

Devices

The **Devices** window displays all the switches that you discover in the Cisco Nexus Dashboard Fabric Controller. You can view information like the current version of the switch, policy attached to it, status, and other image-related information. You can filter and sort the entries.

You can click the link under the **Policy** column to view the associated policy information for a switch. Click the link in the **View Details** column to view the install log for for a switch. The view details columns can have either **Compliance**, **Validate**, **stage**, or **Upgrade**, or **None**.

Staging an Image

After attaching an image policy to a switch, stage the image. When you stage an image, the files are copied into the bootflash.

Before you begin:

- Attach a policy to the selected devices before staging an image on the device.
- The minimum supported NX-OS image version in Fabric Controller is 7.0(3)I7(9).

To stage an image on Cisco Nexus 9000 or Nexus 3000 switches running NX-OS version earlier than the version mentioned above, you must set **Use KSTACK to SCP on N9K, N3K** value to False. On the Web UI, choose **Admin > System Settings > Server Settings > SSH** tab. Uncheck the **Use KSTACK to SCP on N9K, N3K** check box. If you're staging supported image versions, check this check box.

To stage an image from the Cisco Nexus Dashboard Fabric Controller Web UI, perform the following steps:

1. Choose **Manage > Fabric Software > Devices**.
2. Select the required switches and choose **Actions > Stage Image**.



You can choose more than one switch to stage an image.

The **Stage Image** window appears.

In this window, you can view the available space on the switch and the space required.

3. {Optional} Click the **View Files** link under the **Files For Staging** column to view the files that are getting copied to the bootflash.
4. Click **Stage**.

You will be diverted to the **Devices** tab under the **Image Management** window.

5. (Optional) You can view the status under the **Image Staged** column.

Validating an Image

Before you upgrade the switches, you can validate if they support non-disruptive upgrade. To validate an image from the Cisco Nexus Dashboard Fabric Controller Web UI, perform the following steps:

1. Choose **Manage > Fabric Software > Devices**.
2. Choose a switch by checking the check box.



You can choose more than one switch to stage an image.

3. Choose **Actions > Validate**.

The **Validate** dialog box appears.

4. Check the **Confirm Non-Disruptive Upgrade** check box.
5. Click **Validate**.

Upgrading an Image

You can perform a software image or EPLD upgrade on the switches and install or uninstall packages. Upgrade Groups option allows you to trigger image upgrade on multiple switches at an instant. This option can be selected for upgrading or downgrading the switches.



It is recommended to perform upgrade for a maximum of twelve switches at once. If you choose more than twelve switches, the upgrade happens sequentially.

Upgrade Options for NOS Switches

- **Disruptive:** Choose this option for disruptive upgrades.
- **Allow Non-Disruptive:** Choose this option to allow non-disruptive upgrades. When you choose **Allow Non-Disruptive** and if the switch does not support non-disruptive upgrade, then it will go through a disruptive upgrade. When you choose **Force Non-Disruptive** and if the switches you choose do not support non-disruptive upgrade, a warning message appears asking you to review the switch selection. Use the check boxes to add or remove switches.
- When you select multiple switches with different roles to upgrade, a warning message appears to review the switch selection, click **Confirm** to upgrade or click **Cancel**.

Ensure that the below limitation is applicable while adding devices in a same group, else a warning message is displayed to review the switch selection:

- For all Peers, Spines, Borders, Border Gateways, RPs, or RRs in a fabric, if more than one switch is with the same role in a fabric.
- Each FPGA has two memory regions to store its firmware - the Primary region, and the Golden region. In rare situations when one of the regions is corrupted, the FPGA continues to boot firmware from the other operational region. In such a scenario, NDFC shows as 'out of sync'. This is after the EPLD upgrade. Therefore, we need to upgrade the EPLD again with Golden option.



The upgrade groups are automatically deleted, if the attached devices are detached from the group.

To upgrade a switch image from the Cisco Nexus Dashboard Fabric Controller Web UI, perform the following steps:

1. Choose **Manage > Fabric Software > Devices**.
2. Select a switch and choose **Actions > Upgrade**.

The **Upgrade/Uninstall** window appears.

3. Choose the type of upgrade.

The supported options are NOS, EPLD, and Packages(RPM/SMU).

4. Choose an upgrade option from the list based on how you want to upgrade.
 - a. Check the **BIOS Force** check box.

You can view the validation status of all the devices.

- b. Check the **Golden** check box to perform a golden upgrade.
- c. Enter the module number in the **Module Number** field.

You can view the module status below this field.



- If you choose **Packages**, you can view the package details too.
- You can uninstall the packages by selecting the **Uninstall** radio button.

5. Click **Upgrade**.



Upgrade status takes 30 - 40 minutes to update, if multiple switches are upgraded.

For EPLD image, NDFC shows as 'out-of-sync', indicating that one of the regions is corrupted or not modified. You must perform the upgrade procedure again using the **Golden** option to resolve this issue.

Change the Mode

You can change the mode of the device. To change the mode of a device from the Cisco Nexus Dashboard Fabric Controller Web UI, perform the following steps:

1. Choose the switch for which you want to change the mode by checking the check box.



You can choose more than one switch.

2. Click **Actions > Change Mode**.

The **Change Mode** dialog box appears.

3. Choose a mode from the list.

The supported options are **Normal** and **Maintenance**.

4. Click **Deploy Now** or **Deploy Later**.

You will return to the **Overview** tab in **Image Management**.

Modifying the Groups

From Cisco NDFC Release 12.1.1e, you can attach or detach an upgrade group per switch on the **Devices** page.

Modifying groups allow you to select a set of arbitrary switches to perform image management operations at the same instance. Login using the admin role to configure upgrade groups. The admin role can add required switches to an upgrade group. These upgrade groups can be used to perform image management.

You can either attach or detach switches to the groups using this feature. You can attach all switches to a group or only the required switches to the group.

If you choose multiple switches with different roles such as Spines, Borders, Border Gateways, RPs, or RRs to attach to a group, a warning message appears to review the switch selection. Click **Confirm** to attach the switch to the group, or click **Cancel**.

To attach or detach a device from the group, perform the following steps:

1. Choose the device for which you want to upgrade the image.



You can choose more than one device to add to the same group.

2. Choose **Actions > Modify Groups**.

The **Modify Groups** dialog box appears.

3. To attach a group to the selected device:

- a. Choose **Attach Group** radio button, from **Group** list choose **Create Group**.

The **New Group Name** text field is displayed.

- b. Enter the required name in the text field and click **Save**.

You can attach all switches or required switches to a group, a warning message appears asking you to review the switch selection. click **Confirm** to attach, or click **Cancel**.

A warning message appears when the devices are added to group for below instances:

- If all devices for a given role for a fabric is added to the same group
- If all RRs in a fabric are in the same group
- If all RPs in a fabric are in the same group
- If both vPC Peers are in the same group
- All In-band Seed devices are in the same group

You can view the attached group name in the **Upgrade Group** column in the **Devices** tab.

4. To detach the device from the group:

- a. Choose the required device, choose **Actions > Modify Groups**.

The **Modify Groups** dialog box appears.

- b. Choose **Detach Group** radio button, click **Detach**.

A confirmation window appears.

- c. Click **OK**.

Modifying a Policy

You can update the image policy that you have attached to a switch. You can change an image policy for multiple switches at the same time.

To attach or change an image policy attached to a switch from the Cisco Nexus Dashboard Fabric Controller Web UI, perform the following steps:

1. Choose **Manage > Fabric Software > Devices**.
2. Choose a switch by checking the check box.
3. Click **Actions** and choose **Modify Policy**.

The dialog box appears.

4. Choose **Attach Policy** or **Detach Policy**, as required.
5. Choose a policy from the **Policy** list.
6. Click **Attach** or **Detach** depending on the action you want to perform.
7. (Optional) Click the link under the **View Details** column to view the changes.
8. (Optional) Click the link under the **Status** column to view the current and expected image versions.

If the switch is in **Out-Of-Sync** status, view the expected image versions and upgrade the switch accordingly.

Recalculating Compliance

To recalculate the configuration compliance of a switch from the Cisco Nexus Dashboard Fabric Controller Web UI, perform the following steps:

1. Choose **Manage > Fabric Software > Devices**.
2. Choose a switch by checking the check box.
3. Click **Actions** and choose **Recalculate Compliance**.
4. Click the hyperlink under the **View Details** column to view the changes.

Run Reports

1. In the **Image Management** window, choose **Devices**.
2. Place a checkmark in the checkbox for the devices you want to run a report.
3. Attach a policy to that device as follows, if not already done.
 - a. Click **Actions > Modify Policy**, then select **Attach Policy**.

- b. From the **Policy** list, select the policy that you want to attach.
- c. Click **Attach**.
4. Click **Actions > Run Reports**.
5. In the **Create Report** dialog box, choose **Pre ISSU** or **Post ISSU** radio button, as required.

For more information about generating the pre-ISSU and post-ISSU reports on the Switches, see [Nexus Dashboard Fabric Controller Image Management](#).

The system generates the report when ready. Ensure the status displays successful. You can click on the link under the **Results** column to view the HTML version of the report.

Generate Snapshot

1. Choose **Manage > Fabric Software > Devices**, then click **Actions > Generate Snapshot**.

The **Generate Snapshot** window appears.

2. Select one of the following options:
 - o Pre-Upgrade-Snapshot
 - o Post-Upgrade-Snapshot
3. Click **Save**.

History

You can view the history of all the Image Management operations from **Manage > Fabric Software > History** tab.

The following table describes the fields that appear on this screen.

Field	Description
ID	Specifies the ID number.
Device Name	Specifies the device name.
Version	Specifies the version of the image on the device.
Policy Name	Specifies the policy name attached to the image.
Status	Displays if the operation was a success or failure.
Reason	Specifies the reason for the operation to fail.
Operation Type	Specifies the type of operation performed.
Fabric Name	Specifies the name of the Fabric.
Created By	Specifies the user name who performed the operation.
Timestamp	Specifies the time when the operation was performed.

Copyright

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

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

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

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

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

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

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2017–2024 Cisco Systems, Inc. All rights reserved.