Image Management

SAN, Release 12.1.3

Table of Contents

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
NDFC release 12.1.3	Reorganized content	Content within this document was originally provided in the *Cisco NDFC-Fabric Controller Configuration Guide* or the *Cisco NDFC-SAN Controller Configuration Guide*. Beginning with release 12.1.3, this content is now provided solely in this document and is no longer provided in those documents.

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. Image management is supported only for Cisco Nexus switches.

> **ⓘ**
> - 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 under the Credential Management page. You will not be able to execute ISSU operations without first setting the proper 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 uploaded image and related information.
Images	Uploading an Image
Image Policies	Creating an Image Policy
Devices	Staging an Image
	Validating an Image
	Upgrading an Image
	Modifying a Policy
	Recalculating Compliance
History	History

Ensure that your user role is **network-admin** or **device-upg-admin** and you didn't freeze the 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**, **network-stager**, **network-operator**, or **device-upg-admin**. You can also view them if your Nexus Dashboard Fabric Controller is in freeze mode.

Here's the process 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 **Operations > Image Management > Overview.**

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

It lists procedure 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 **Operations > Image Management > Images**.

Field	Description
Platform	Specifies the name of the platform. Images, RPMs, or SMUs are categorized as follows: ・ N9K/N3k ・ N6K ・ N7K ・ N77K ・ N5K ・ Other ・ Third Party The images are the same for N9K and N3K platforms.The platform is **Other** if the uploaded images are not mapped to any of the existing platforms. The platform is **N9K/N3K** for RPMs.
Bits	Specifies the bits of the image
Image Name	Specifies the filename 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	Specifies the file type of the image, EPLD, RPM, or SMU.The file type EPLDs are **epld**. The file types of images are **nxos**, **system** or **kickstart**. The file type for RPMs is **feature** and for SMUs the file type is **patch**.
NXOS Version	Specifies the NXOS image version for only Cisco switches.
Image Version	Specifies the image version for all devices, including the non-Cisco devices as well.
Size (Bytes)	Specifies the size of the image, RPM, or SMU files in bytes.

Field	Description
Checksum	Specifies the checksum of the image. The checksum checks if there's any corruption 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.

The following table describes the action items, in the **Actions** menu drop-down list, that appears on **Operations > Image Management > Images**.

Action Item	Description
Refresh	Refreshes the Images table.
Upload	Click to upload a new image. For instructions, see Uploading an Image.
Delete	Allows you to delete the image from the repository. Choose an image, click **Actions**, and choose **Delete**. A confirmation window appears. Click **Yes** to delete the image. ⓘ 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 switch console, allow maximum of 24 hours to refresh and view update on NDFC. Else, on NDFC UI, navigate **LAN > Fabrics > Switches**, choose switch for which image is deleted and click **Actions > Discover > Rediscover** to view updates.

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. All the images, RPMs, and SMUs are used in the **Image Policies** window.
Your user role should be **network-admin**, or **device-upg-admin** to upload an

image. You can't perform this operation with the **network-stager** user role.

1. Choose **Operations > Image Management > Images**.

2. Click **Actions** and choose **Upload**.

   The **Upload Image** dialog box appears.

3. Click **Choose file** to choose a file from the local repository of your device.

4. Choose the file and click **OK**.

   You can upload a ZIP or TAR file as well. Cisco Nexus Dashboard Fabric Controller processes and validate the image file and categorize it under the existing platforms accordingly. If it doesn't fall under **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.

5. Click **OK**.

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

   > 🛈 If only EPLD files are uploaded, you cannot create policy as Release drop-down list is empty for EPLD images.

   All NX-OS, 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.

   > 🛈 You can upload images for all Cisco Nexus Series Switches.
   > You can upload EPLD images only for Cisco Nexus 9000 Series Switches.

   If your network speed is slow, increase the wait time of Cisco Nexus Dashboard Fabric Controller to 1 hour so that the image upload is complete. To increase the wait time from Cisco Nexus Dashboard Fabric Controller Web UI, perform the following steps:

   a. Choose **Settings > Server Settings**.

   b. Search for the **csrf.refresh.time** property, and set the value as **60**.

      The value is in minutes.

   c. Click **Apply Changes**.

   d. Restart the Nexus Dashboard Fabric Controller server.

Image Policies

The image management policies will have the information of intent of NX-OS 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 NXOS 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** menu drop-down list, that appear on **Operations > Image Management > 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	Allows you to delete the policy.Choose a policy, click **Actions**, and choose **Delete**. A confirmation window appears. Click **Confirm** to delete the **policy**. ℹ An error message appears if you try to delete a policy that is attached to a device.
Edit	Allows you to edit the policy.

Creating an Image Policy

Before you begin:

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

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

> ℹ While creating a policy for MDS platform and SAN deployment few fields are grayed out.

1. Choose **Operations > Image Management > 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 Platform drop-down list. The options will be populated based on the images you upload in the **Images** window. The options for the **Release** drop-down list will be autopopulated based on the platform you choose.
Release	Choose the NX-OS version from the **Release** drop-down list. The release versions of 64-bit images are appended with 64bit in the image name. NOTE: If only EPLD files are uploaded, you cannot create policy as Release drop-down list is empty for EPLD images.
Package Name	(Optional) Choose the packages. before choose Packages, View All Packages check box to display all uploaded packages for a given platform (its 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 Disable	(Optional) Check this check box to uninstall the packages.
RPMs 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.

1. Click **Save**.

What to do next:

Attach the policy to a device. See Modifying a Policy section 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 on **Policy** column to view associated policy information for the switch. Similarly, click on **View details** column for required switch to view details. The view details columns can have either **Validate**, or **Upgrade**, or **None**.

You can perform the following actions in the **Devices** window:

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.

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

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 SAN Controller is 6.1(2)I1(1).

  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 **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.

Procedure

1. Choose **Operations > Image Management > Devices**.

2. Choose a switch by checking the check box.

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

3. Click **Actions** and choose **Stage Image**.

   The **Select Images to Install window** appears.

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

4. (Optional) Click the hyperlink under the Files For Staging column to view the files that are getting copied to the bootflash.

5. Click **Stage**.

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

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

7. (Optional) Click the hyperlink under the Reason column to view the log.

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 **Operations > Image Management > Devices**.

2. Choose a switch by checking the check box.

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

3. Click **Actions** and choose **Validate**.

   The **Validate** dialog box appears.

4. Check the Confirm non disruptive upgrade check box.

5. Click **Validate**.

   You'll return to the Overview tab under the Image Management window.

6. (Optional) You can view the status under the Validated column.

7. (Optional) Click the hyperlink under the Reason column to view the log.

Upgrading an Image

You can upgrade or uninstall a switch. Upgrade Groups option allows you to trigger image upgrade on multiple switches at an instant. This option can be selected for upgrade/downgrade options.

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

Upgrade Options for NX-OS 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** option 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 choose 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 same role in a fabric.

i The upgrade groups are automatically deleted, if the attached devices are detached from the created or upgrade or modify group.

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

1. Choose **Operations > Image Management > Devices**.

2. Choose a switch by checking the check box.

3. Click **Actions** and choose **Upgrade**.

   The **Upgrade/Uninstall** window appears.

4. Choose the type of upgrade by checking the check box.

   The valid options are NXOS, EPLD, and Packages (RPM/SMU).

5. Choose NXOS, EPLD, or Packages:

   a. Choose an upgrade option from the drop-down list based on how you want to upgrade.

   b. (Optional) Check the BIOS Force check box.

      You can view thee validation status of all the devices.

   c. Check the **Golden** check box to perform a golden upgrade.

   d. Enter the module number in the **Module Number** field.

      You can view the module status below this field.

      NOTE:

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

6. Click **Upgrade**.

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

Modifying a Policy

Modify 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 **Operations > Image Management > Devices**.

2. Choose a switch by checking the check box.

3. Click **Actions** and choose **Apply Policy**.

    The **Modify Policy** dialog box appears.

4. You can either attach or detach a policy, choose required check box.

5. Choose a policy from the Policy drop-down list.

6. Click required **Attach** or **Detach**.

7. (Optional) Click the hyperlink under the Reason column to view the changes.

8. (Optional) Click the hyperlink under thee 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 **Operations > Image Management > Devices**.

2. Choose a switch by checking the check box.

3. Click **Actions** and choose **Recalculate Compliance**.

4. Click the hyperlink under the Reason column to view the changes.

History

You can view the history of all the Image Management operations from **Operations > Image Management > 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)