Managing Your Fabric Software, Release 4.1.1

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
Nexus Dashboard 4.1.1	Improved fabric software navigation and workflow.	Beginning with Nexus Dashboard 4.1.1, the navigation and workflow for fabric software in Nexus Dashboard have been enhanced.

Understand Fabric Software for NX-OS and IOS-XE fabrics

This section provides detailed information for the Fabric Software feature in Nexus Dashboard for NX-OS/IOS-XE fabrics.

Fabric Software deploys Cisco software images to switches which allows network stability and feature consistency. The benefits of Fabric Software workflows include the following:

- Comprehensive image management policies allow you to specify a version and patch level for a set of switches
- Nexus Dashboard validates compliance for the image policy associated with each switch
- Image staging, validation, and in-service software upgrade (ISSU) operations are independent, allowing mass upgrades and downgrades, and the ability to perform staging and validation in a single step
    - You can perform the following operations before the maintenance window:
        - Stage image files

          This copies the image files to the switch bootflash.
        - Validate Network Operating System (NOS) and electronic programmable logic device (EPLD) compatibility where possible

          This checks if the image is complete, if the image is valid for the individual hardware, and if the upgrade can be non-disruptive.
        - Run reports
        - Modify groups
        - Generate snapshot
- The ability to run reports and compare the results
- The ability to generate snapshots of the pre/post updates
- The **View Details** column provides Live log status to monitor each operation
- Allows you to make use of maintenance mode to minimize the impact of disruptive upgrades, especially for multi-reload upgrade situations
- Upgrade groups allows bulk upgrades and downgrades. Upgrade groups have checks to avoid unnecessary downtime in redundant fabrics in the following cases:
    - Virtual Port Channel (vPC) peers are placed in different groups by default:
        - Switches that have even numbers or VPC role of primary
        - Switches that have odd numbers or VPC role of secondary
- Provides visibility into previous and current upgrade details as well as high level summarization
- Visibility into current NOS, EPLD and patch consistency at a switch, fabric, and group level

ℹ Telemetry must be enabled to run the Pre/Post Update Analysis Reports.

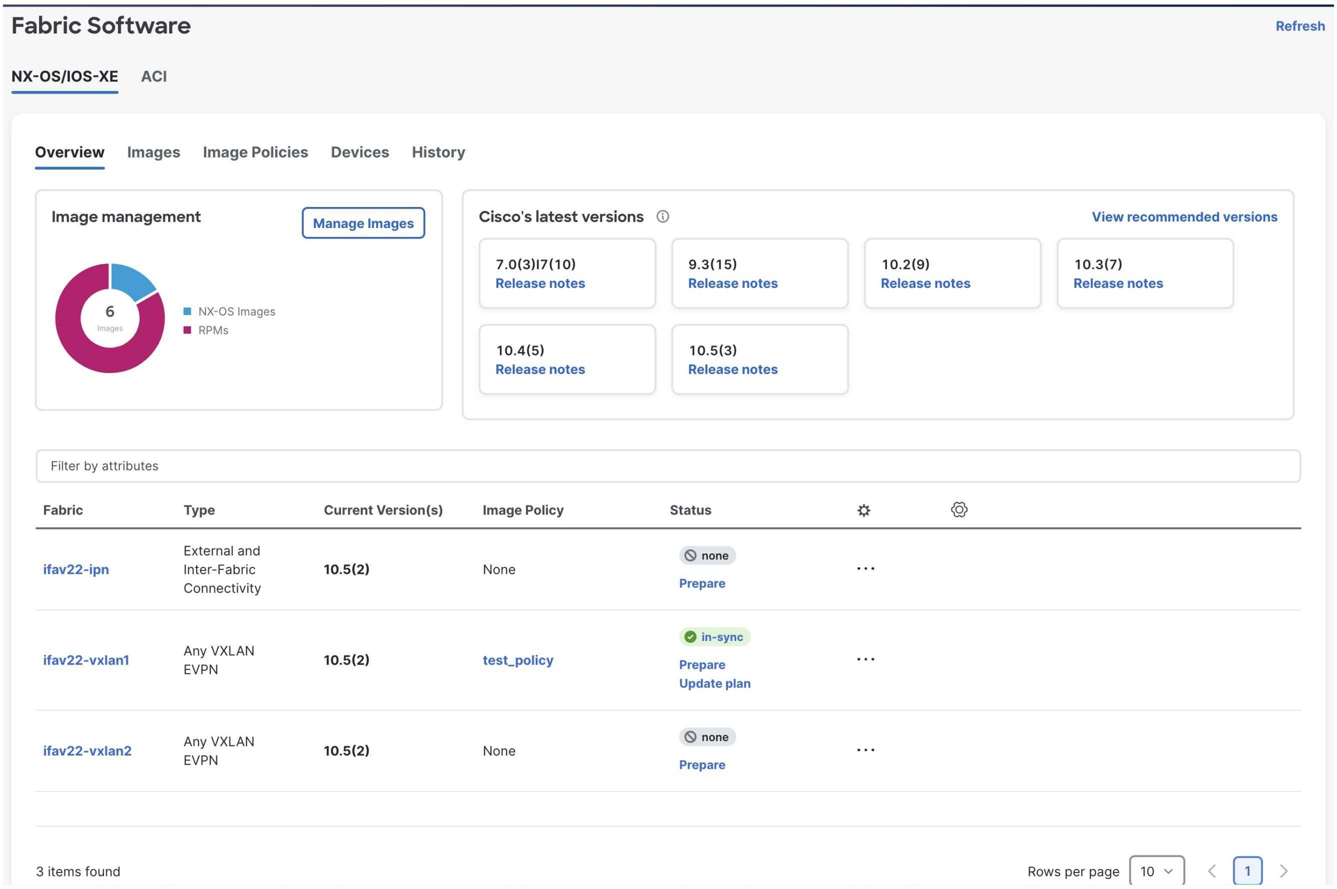
Navigate to the Fabric Software page for NX-OS and IOS-XE fabrics

To navigate to the Fabric Software page:

1. Click **Manage > Fabric Software**.
2. Click the **NX-OS/IOS-XE** tab.

Understand the information provided in the Fabric Software page for NX-OS and IOS-XE fabrics

The **Overview** tab displays the images, policies, platforms, release versions, and fabric information.



Fabric	Type	Current Version(s)	Image Policy	Status
ifav22-ipn	External and Inter-Fabric Connectivity	10.5(2)	None	none Prepare
ifav22-vxlan1	Any VXLAN EVPN	10.5(2)	test_policy	in-sync Prepare Update plan
ifav22-vxlan2	Any VXLAN EVPN	10.5(2)	None	none Prepare

The **Fabric Software** page has the following functional areas:

- **Overview**: This displays the images, policies, platforms, release versions, and fabric information.
  - The **Image management** card displays the number of images and the type of packages or patches.
  - The **Cisco's latest versions** card displays the latest versions of the switch software that are available, the versions of the switch software that Cisco recommends, and the corresponding release notes.
  - The fabric area displays information about the configured fabrics.

Field	Description

Fabric	The name of the fabric.
Type	The type of fabric.
Current version(s)	The current versions of software running on the switches in the fabric.
Image policy	The fabric-level image policy that is being used for the switches in the fabric, if applicable. See Upgrade or downgrade switches in a fabric for more information.
Status	The status of the fabric-level image policy: - **None**: No fabric-level image policy has been configured for this fabric. - **In-Sync**: The current image versions on each switch in the fabric is in-sync with the expected image versions. - **Out-of-Sync**: The current image versions on one or more switches in the fabric is out-of-sync with the expected image versions. Click the **Out-of-Sync** text in the **Status** column to bring up a slide-in pane that shows which switches in the fabric are out-of-sync with the expected image versions. See Recalculate compliance for more information. - **Prepare**: Click to prepare a software image policy that can be used at the fabric level. See Prepare a fabric image policy for more information. - **Update plan**: The system is ready to apply the necessary software updates to certain switches in the fabric. Click **Update plan** to bring up the **Software Update Plan** for the fabric. See Install or upgrade software on devices in a fabric for more information.

- **Images**: This displays the images. You can upload or delete 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 ▪ MDS ▪ CAT9 ▪ CAT8 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.**
NOS Version	Specifies the NX-OS or IOS-XE image version for only Cisco switches.
Size (Bytes)	Specifies the size of the image, RPM, or SMU files in bytes.
Reference Count	Specifies the number of image policies this image is part of.
Image Present	Determines if the uploaded image is present after a successful Nexus Dashboard restore process and/or Nexus Dashboard upgrade process.
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**.

- **Image Polices**: This displays the image policies. You can create, delete, or edit image policies.

Field	Description
Policy Name	Specifies the name of the image policy.

Platform	Specifies the name of the platform. Images, RPMs, or SMUs are categorized as follows: · N9K/N3K · N6K · N7K · N77K · N5K · Other · Third Party · MDS · CAT9 · CAT8 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.
NOS Version	Specifies the NX-OS or IOS-XE image version for only Cisco switches.
Image Name	Specifies the filename of the image, RPM, or SMU that you uploaded.
EPLD Name	Specifies the name of the electronic programmable logic device (EPLD).
Package Name(s)	Specifies the name of the package.
Disable RPM(s)	Shows whether the **RPM/SMU Disable** option is enabled (true) or not (false).
Reference Count	Specifies the number of switches this policy is assigned to.
Image Present	Determines if the uploaded image is present after a successful Nexus Dashboard restore process and/or Nexus Dashboard upgrade process.
Policy Description	Specifies a description of the image policy.

- **Devices**: This displays the devices. You can stage image, upgrade, validate, change mode, attach group, detach group, attach policy, or detach policy.

You cannot attach or detach fabric policies from the **Devices** tab. Only image policies can be attached or detached from the **Devices** tab.

Field	Description
Device name	Specifies the name of the device.
IP address	Specifies the IP address of the device.
Fabric	Specifies the fabric that the device resides in.
Software version	Specifies the NX-OS or IOS-XE image version for only Cisco switches.

Policy	Specifies the image policy that is being used by the device.
Status	Specifies the configuration status. Status will be either **In-Sync** or **Out-of-sync**.
Model	Specifies the switch model.
View Details	Click the link to view details for the switch, if available. For example, click **Compliance** to view the compliance check details.
Image Staged	Specifies whether the image has been staged or not.
Validated	Specifies whether the image has been validated or not.
Upgraded	Specifies whether the image has been upgraded or not
Update Groups	Specifies the name of the upgrade group.
Mode	Specifies the upgrade mode (Maintenance or Normal).
vPC Role	Specifies the VPC role, if applicable (Primary or Secondary).
vPC Peer	Specifies which switch is the VPC peer with this switch, if applicable.
Role	Specifies the role for the switch.
Last Upgrade Action	Specifies when the last upgrade was performed on the switch.

- **History**: This displays the history of all the operations performed on the switches.

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 which action was performed.
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.

Terminology

This describes the terms that you must be familiar with:

Term	Acronym	Description
Electronic Programmable Logic Device	EPLD	The EPLD image upgrades to enhance hardware functionality or to resolve known issues.
In-Service Software Upgrade	ISSU	ISSU allows you to upgrade the software version of the release on a chassis device with no network downtime.
Local Area Network	LAN	LAN consists of a series of computers linked together to form a network in a circumscribed location.
Network Operating System	NOS	A specialized operating system designed for a network device such as a router, switch or firewall. Some examples include NX-OS for Nexus switches, IOS XE for Cisco Catalyst switches and so on.
Rendezvous Points	RP	RP is a router that acts as the place where sources and receivers of multicast data can find each other.
Route Reflector	RR	Route Reflector is a router that acts as a routing information exchange server for all other iBGP routers.
Secure Copy	SCP	SCP is used by fabric software to transfer files between devices.
Secure File Transfer Protocol	SFTP	SFTP is a network protocol that allows you to securely access, transfer, and manage large files and sensitive data.

Required software versions

For Cisco Nexus Dashboard services compatibility information, see the Cisco Data Center Networking Applications Compatibility Matrix.

Prerequisites

This section describes the prerequisites. This document assumes that the reader has a fundamental knowledge of Nexus Dashboard.

- SCP is used by Fabric Software. Both SCP and SNMP are always enabled by default and a minimum of 2 external service pool IPs are needed when you enable the Nexus Dashboard.
- Ensure that your user role is network-admin or device-upg-admin.
- Ensure that there is a fabric, the fabric must have the " Deployment Enabled" flag set, and the switches are managed by the Nexus Dashboard in this fabric.
- Ensure you have LAN credential set.

Upgrade or downgrade switches in a fabric

You can perform switch upgrades or downgrades at the fabric level.

This feature applies only to LAN and IPFM fabrics.

Prepare a fabric image policy

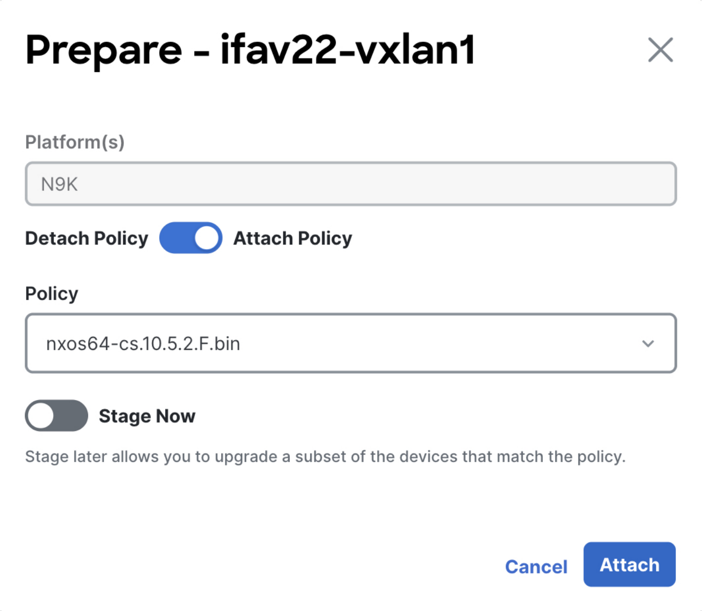
This section describes how to prepare a software image policy that can be used at the fabric level.

1. Navigate to the Fabric Software page for NX-OS and IOS-XE fabrics.
2. In the **Fabric Software** window, verify that the **Overview** tab is selected.

   See Understand Fabric Software for NX-OS and IOS-XE fabrics for more information on the **Overview** tab and the other tabs in the **Fabric Software** window.

3. In the list of fabrics shown in the **Overview** page, locate the fabric where you want to prepare a software image policy that will be used for that fabric.
4. In the **Status** column, click **Prepare** in the row for the fabric where you want to prepare a software image policy.

   The **Prepare** dialog box appears.



Prepare - ifav22-vxlan1

Platform(s): N9K

Detach Policy / Attach Policy

Policy: nxos64-cs.10.5.2.F.bin

Stage Now

Stage later allows you to upgrade a subset of the devices that match the policy.

5. In the **Prepare** dialog box, make the appropriate configurations for this fabric-level image policy.

   a. Review the types of devices listed in the **Platform(s)** area.

      The list will consist of device types that are detected in this fabric. Use this list to verify that the software policy that you select in the next step aligns with the type of devices that you have in this fabric.

      For example, if you see CAT9K,N9K listed in the **Platforms** area, when you select the policy in the next step, you would want to verify that any policy that you select aligns with either Catalyst 9000 or Nexus 9000 series switches.

b. Click the radio button to either **Attach Policy** or **Detach Policy**.

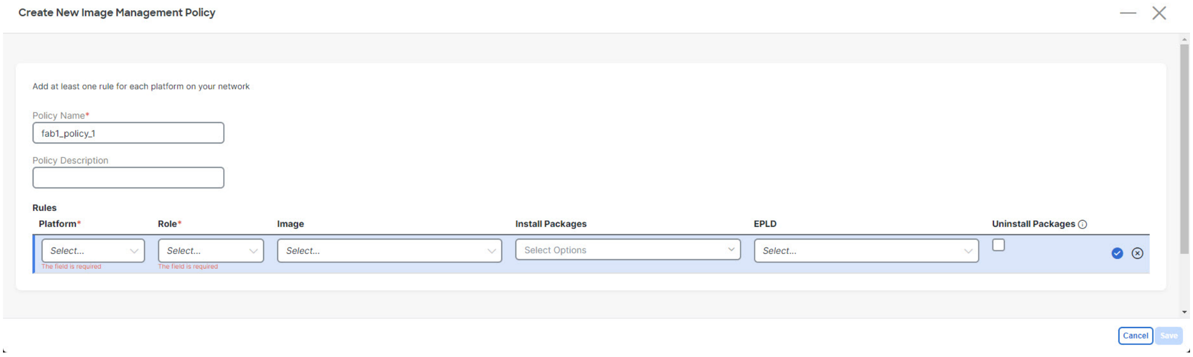
   - If you select **Detach Policy**, click **Detach** to detach the fabric-level image policy from these switches in this fabric. While detached, if a fabric-level image policy is not used any more, then it is deleted implicitly.
   - If you select **Attach Policy**, proceed with the instructions below to attach an existing image policy or to create a new one.

c. In the **Policy** drop-down list, attach an existing image policy or create a new one.

   - If you already have fabric-level image policies created and you want to use one of those existing image policies, scroll through the list of image policies and select the one that you want to use. Go to Step 4d.
   - If you do not have any fabric-level image policies created yet, or if you do not want to use one of the existing image policies for any reason, click **+Create Policy**.

     The **Create New Image Management Policy** window appears.

     For NX-OS images, you need to create implicit fabric-level image policies.



Create New Image Management Policy

Add at least one rule for each platform on your network

Policy Name*: fab1_policy_1

Policy Description:

Rules

Platform*	Role*	Image	Install Packages	EPLD	Uninstall Packages
Select... The field is required	Select... The field is required	Select...	Select Options	Select...	□

   i. In the **Create New Image Management Policy** window, enter a unique name for the fabric-level image policy in the **Policy Name** field or leave the automatically-generated policy name as-is, if desired.

   ii. Enter a description for the new fabric-level image policy in the **Policy Description** field, if necessary.

   iii. In the **Rules** area, click **+Add Row**.

   iv. Enter the necessary information in the **Rules** area to configure this new fabric-level image policy.

   - **Platform**: Select the types of switches in the fabric that will use this new fabric-level image policy.
   - **Role**: Select the roles for the switches in the fabric that will use this new fabric-level image policy.
   - Use one of the following options to be used with this new fabric-level image policy:
     - **Image**: Select the software image that will be used with this new fabric-level image policy.
     - **Install Packages**: Select the installation packages that will be used with this

new fabric-level image policy.

- **EPLD**: Select the electronic programmable logic device (EPLD) image that will be used with this new fabric-level image policy.

- **Uninstall Packages**: Check the box to uninstall packages from the switches in the fabric as part of this new fabric-level image policy.

v. Click the checkbox in the row to complete the configuration for this image policy rule.

vi. Repeat these steps to configure a new set of rules for this fabric-wide image policy, if necessary.

For example, you might configure a new set of rules with a different option in the **Platform** field selected to configure a new set of rules for other types of switches in the fabric, or with a different option in the **Role** area selected to configure a new set of rules for switches with a different role in the fabric.

vii. Click **Save** when you have configured all the necessary rules in the fabric-level image policy.

You are returned to the **Prepare - <fabric>** window, with this new fabric-level image policy automatically selected in the **Policy** field.

d. Determine when you want to stage the fabric-level image policy.

- Leave the **Stage Now** option unselected to stage the fabric-level image policy later.

  Staging the fabric-level image policy later allows you to stage the images in the fabric to be used later (for example, by copying the images onto the switch bootflash) so that you can upgrade a subset of the devices later that match the policy.

- Click the **Stage Now** option to enable this option.

  The fabric-level image policy will stage after you click **Attach** in the next step.

e. Click **Attach**.

The image policy is now attached to this fabric, and is displayed in the **Image Policy** column in the **Overview** page. Click the policy name in the **Image Policy** column to see details of the applied policy.

clicking on which will show more details about the policy applied

6. Make additional configurations for each fabric, if necessary, based on the status shown in the **Status** column:

   - **None**: No fabric-level image policy has been configured for this fabric.
   - **In-Sync**: The current image versions on each switch in the fabric is in-sync with the expected image versions. No further configurations are needed for the fabric-level image policy for this fabric. Click the **In-Sync** text in the **Status** column to bring up a slide-in pane that shows which switches in the fabric are in-sync with the expected image versions.
   - **Out-of-Sync**: The current image versions on one or more switches in the fabric is out-of-sync with the expected image versions. Click the **Out-of-Sync** text in the **Status** column to bring up a slide-in pane that shows which switches in the fabric are out-of-sync with the

expected image versions. See Recalculate compliance for more information.

- **Prepare**: Click to prepare a software image policy that can be used at the fabric level, as described in this topic.
- **Update plan**: The system is ready to apply software updates to the appropriate switches in the fabric. Click **Update plan** to bring up the **Software Update Plan** for the fabric. See Install or upgrade software on devices in a fabric for more information.

Once you have prepared a software image policy that will be used for a fabric, you cannot then edit that policy directly. You can delete a fabric-level image policy, using **Detach Policy** in the **Prepare** dialog box, only if the policy is not attached to any fabric. However, you can delete uploaded images, even if the ref count is greater than 0.

If uploaded images are used in a software image policy but you have not attached that software image policy to any devices yet, then you can delete those software image policies along with the selected images. However, if you created multiple software image policies using one image and you attached one of those policies to devices in a fabric, then you cannot delete the image and you cannot delete any of the other software image policies that use that image, even if those software image policies aren’t attached to any devices in the fabric yet.

Change number of concurrent switches for staging/validating/updating

As you go through the procedures in Install or upgrade software on devices in a fabric, there are points during the staging/validating or updating processes where you might be taking actions on a group of switches concurrently. Following are the default values for the number of switches that are grouped together when you are taking an action on a group of switches concurrently:

- Staging/validating: Default number of switches is 10
- Updating: Default number of switches is 20

Follow these procedures if you want to change these default values.

1. Navigate to:

   Admin > System Settings > Fabric management

2. In the **Advanced Settings** area, click the **Admin** tab.
3. Modify the values in the following fields, if necessary:
   - **Image update thread pool size**: The number of switches that can be updated concurrently. Default value is 20. Valid range is 10-200.
   - **Image stage/validate thread pool size**: The number of switches that can be staged and validated concurrently. Default value is 10. Valid range is 5-200.
4. Click **Save** when you have completed any configuration changes on this page.

Install or upgrade software on devices in a fabric

This section describes how to install or upgrade software on the devices in a fabric using a fabric-level image policy.

1. Navigate to the Fabric Software page for NX-OS and IOS-XE fabrics.
2. In **Fabric Software**, verify that **Overview** is selected.
3. In the list of fabrics shown in the **Overview** page, locate the fabric where you want to install or upgrade software on the devices in that fabric.
4. In the row for a fabric, select **Update plan** in the **Status** column to install or update the software on the devices in that fabric.

   > You will see the **Update plan** option only after you prepare the fabric.

   To prepare the fabric:

   Click **Prepare** in the **Status** column of the fabric that you want to install or upgrade.

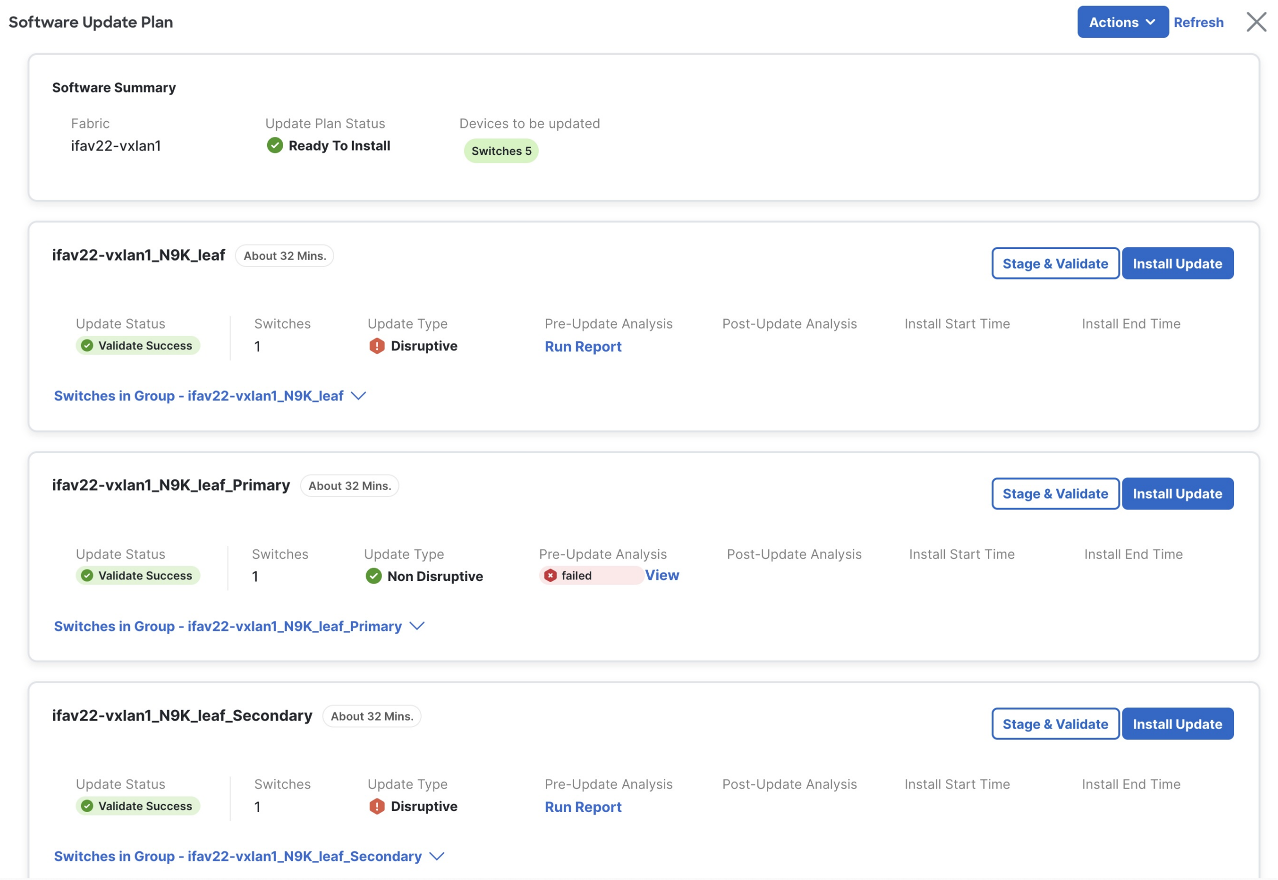
   The **Prepare - *Fabric Name*** dialog box opens.

   a. The platform name is chosen by default in the **Platform(s)** field.
   b. In the **Policy** field, select a policy that you want to attach to the fabric.
   c. Click **Attach** to create an update plan.

      > You can also stage from here.

5. After you prepare the Fabric, in the **Fabric Software** page, select **Update plan** in the **Status** column to install or update the software on the devices in that fabric.

   The **Software Update Plan** page appears.



Software Update Plan

Software Summary

Fabric	Update Plan Status	Devices to be updated
ifav22-vxlan1	✓ Ready To Install	Switches 5

ifav22-vxlan1_N9K_leaf About 32 Mins.

Update Status	Switches	Update Type	Pre-Update Analysis	Post-Update Analysis	Install Start Time	Install End Time
✓ Validate Success	1	Disruptive	Run Report			

Switches in Group - ifav22-vxlan1_N9K_leaf

ifav22-vxlan1_N9K_leaf_Primary About 32 Mins.

Update Status	Switches	Update Type	Pre-Update Analysis	Post-Update Analysis	Install Start Time	Install End Time
✓ Validate Success	1	✓ Non Disruptive	failed View			

Switches in Group - ifav22-vxlan1_N9K_leaf_Primary

ifav22-vxlan1_N9K_leaf_Secondary About 32 Mins.

Update Status	Switches	Update Type	Pre-Update Analysis	Post-Update Analysis	Install Start Time	Install End Time
✓ Validate Success	1	Disruptive	Run Report			

Switches in Group - ifav22-vxlan1_N9K_leaf_Secondary

6. Based on their roles, switches are automatically assigned groups, by default.

   To automatically assign groups, click **Actions> Auto-Assign Groups**.

   You can automatically assign groups based on the following criteria:

   - **Role Based**: All switches of a given role for a fabric in the same group
   - **Even Odd**: Switches that are grouped in odd or even groups:
     - Switches that have even numbers or vPC role of primary
     - Switches that have odd numbers or vPC role of secondary

       Nexus Dashboard uses the following calculations to balance the number of switches in the even and odd groups as much as possible:

       a. Nexus Dashboard will first divide the switches by role between the even and odd groups; this is done to reduce the likelihood of having most or all of one type of switch in only one of the two groups.

       b. Nexus Dashboard will then alternate switch assignments between the even and odd groups, where the first switch of one type goes into the odd group, the second switch of that same type goes into the even group, and so on.

7. Review the information provided in the **Software Summary** area.
   - **Fabric**: The name of the fabric where you will be installing or upgrading software on the devices in that fabric.
   - **Update Plan Status**: The status of the update plan.
   - **Devices to be Updated**: The number of devices in this fabric that will be updated.

8. Review the general information provided in the switch group area.
   - The first area shows whether the update has yet to start and any warnings about the update.
   - **Update Status**: Shows the status of the update.
   - **Switches**: Shows the number of switches in this switch group.
   - **Update Type**: Shows the nature of update.
   - **Pre-update Analysis**: Shows if any warnings are triggered prior to the update. You can also **Run Report** and view the pre-update analysis.
   - **Post-update Analysis**: Shows when the post-update analysis is scheduled for or if the update triggered any warnings.
   - **Install Start Time**: Shows the time when the update installation started.
   - **Install End Time**: Shows the time when the update installation ended.

9. Review the more detailed information provided in the switch group area.

   Click the down arrow next to the switch group name to display more detailed information on that switch group.

Field	Description
Switch	The switch that belongs to this switch group. Click the switch name to bring up additional information on that switch.

IP Address	The IP address for a switch in the switch group.
Model	The model of the switch in the switch group.
Role	The role of the switch in the switch group
Current Software	The current software image version running on this switch in the switch group.
Update Type	The update type for this switch in the switch group. This can be either **Disruptive** or **Non-Disruptive**, based on the compatibility check.
Update Status	The update status of this switch in the switch group.
Logs	The install logs for this switch in the switch group. Click **View Logs** for additional information on the install log.
Mode	The mode for the switch in the switch group.
vPC Role	The vPC role of the switch in the switch group, if applicable.
vPC Peer	The vPC peer of the switch in the switch group, if applicable.
Policy	The policy associated with this switch in the switch group. Click **Policy** for details of the fabric-level image policy.
Last Upgrade Action	The time for the **Last Upgrade Action** for this switch in the switch group.

10. Determine if you want to make changes to the switches in the update group.

    For each of the actions listed below, you can click the box next to single switch in the update group or click the box next to **Switch** to select all the switches in the update group. The following options are then displayed above the update group:

    - **Remove from Update Group**: Click to remove the selected switch(es) from the update group. These switches are categorized under **None** in the **Update Group**.
    - **Create New Update Group**: Click to create a new update group with the selected switch(es).
    - **Move to Update Group**: Click to move the selected switch(es) to a different update group.

11. To upgrade the switches in an update group, perform the following steps in that group's area in the **Software Update Plan** page:

    > ℹ The default number of switches that you can stage and validate concurrently is 10, and the number of switches that you can update concurrently is 20. To change the default values, see Change number of concurrent switches for staging/validating/updating.

    - Click **Stage & Validate** to stage and validate the update. This step downloads the NX-OS image on the switch and performs a compatibility check before installing the update.

      Note that it is preferred to perform staging first, as it will perform compatibility checks on the switch before installing updates.

    - Click **View** to view the actions that take place on the NX-OS switches as they relate to Nexus Dashboard.

      The **Post-update report for Switches** page appears.

> ℹ In some cases, the **Post-update report for Switches** page does not accurately display the correct information for the switches. This might happen due to a timing issue, such as when the version is getting updated in the telemetry pipeline at the same time as the post upgrade is being triggered. Wait for around 10 minutes, then click **Rerun report** in the **Post-update report for Switches** page to address this issue. You can also verify the telemetry data availability by checking the telemetry status at **Admin > System Status > Telemetry > Telemetry Status**.

- Click **Install Update** to perform the software update on the switches in this update group.

  Install Update allows you to trigger either a software upgrade or downgrade for all the switches in that update group.

  > ℹ You must check the **Update Status** under **Software Summary** area before clicking **Install Update**. If the update status is "failed", the **Install Update** button will still be available but should not be clicked. A "failed" status indicates that it didn't clear the compatibility check.

  The **Install Update** dialog box opens. It provides the following details:

  - The number of switches that are in an update group. By default, updates are performed concurrently on 20 switches at a time, so if you have 40 switches in an update group, updates are first performed on the first batch of 20 switches, and then a second pass is performed on the second batch of 20 switches.
  - Advanced options that are described in the next step, which may change the estimated timeframe, depending on the advanced option.

    In the **Install Update** confirmation dialog, click the **Advanced options** arrow to make the advanced selections for the installation, if necessary.

  - In the **Execution paradigm** field, select a **Serial** or **Parallel** execution:
    - **Serial**: Switches are updated one at a time, serially, where the update process must fully complete on one switch before it begins on the next switch in the update group.
    - **Parallel**: Switches are updated all at one time, depending on the number of switches that can be updated concurrently. For example, if you have 40 switches in the update group but 20 switches are updated at a time concurrently, then a **Parallel** setting will result in the first set of 20 switches going through the update process, all at one time, and then the second set of 20 switches going through the same concurrent update process after the update process has completed for the first set.
  - In the **Snapshot analysis** field, choose one of the following options: **No analysis**, **Use existing pre-analysis**, **Snapshot**, or **Full analysis**.

    > ℹ
    > - The **Use existing pre-analysis** and **Full analysis** options are only available when the **Telemetry** option is enabled and Premier licensed for the fabric. See Creating LAN and ACI Fabrics and Fabric Groups for more information.
    >   - The snapshot option is essentially a reporting mechanism to compare the state of the system before and after an upgrade; the

> snapshot option in this case is not used to create a checkpoint (snapshot) of the system. See Snapshots for more information about this option.

- Make the proper selection in the **Installation Type** field, if necessary. You can choose between Disruptive or Non-Disruptive.

  When you click **Stage/Distribute** earlier in these procedures, Nexus Dashboard will determine if the switches in the update group are set with disruptive or non-disruptive upgrade settings.

  - If all of the switches are shown as non-disruptive in the initial staging point of the process, then the default value for this field will be for the drop-down list next to the **Force Disruptive** field as unchecked (not enabled).
  - However, if any of the switches are shown as disruptive in the initial staging point of the process, then the default value for this field will be for the box next to the **Force Disruptive** field as checked (enabled) for all of the switches in this update group.

    Refer to the *Understanding In-Service Software Upgrades* for more information about this option.

- Check the box next to **Use Maintenance Mode** if you want to enable this option.

  Maintenance mode, along with normal mode, are part of Graceful Insertion and Removal, or GIR. When the **Maintenance Mode** option is enabled, Nexus Dashboard will place the switches in the update group in the maintenance mode during the update process, where all configured Layer 3 control-plane protocols are isolated from the network, and will return the switches to normal mode after the update process is completed. Refer to the *Configuring Graceful Insertion and Removal* for more information on GIR.

- In the **Error handling/On failure** field, determine if you want the installation to **Continue** or to **Pause** if there is a failure that occurs during the update. A failure might occur for a number of reasons, such as a switch failing to come back online or a failure to successfully establish an ssh session between Nexus Dashboard and the switch.

  The actions taken with this setting may also be affected by settings in other areas.

  For example, assume that you have **Pause** as the setting for this field, and you have **Serial** as the setting in the **Execution Paradigm** field. If a set of 20 switches in an update group are going through a serial update and an issue arises with the sixth switch in the set, the update will pause at that sixth switch's update process and will not proceed with the update process for the remaining 14 switches in the set until you manually begin the update process again.

  However, if you have **Parallel** as the setting in the **Execution Paradigm** field and there is an issue with the sixth switch in a set in the update group, the update process will complete for the other 14 switches in the set that are being updated concurrently, and the update process will pause before moving to the update process for the next set of switches in the update group.

Recalculate compliance

This section describes how to recalculate compliance on devices in a fabric where software was installed or upgraded using a fabric-level image policy.

The **Recalculate compliance** option checks if the versions on the switch and the policy are same. You might want to recalculate compliance when the information on the **Overview** page does not correctly reflect the expected status for the devices in a fabric or to change the Status from **Out-of-Sync** to **In-Sync**. If you made a change directly on the switch CLI, you might also use the **Recalculate compliance** option so that the system fetches those updates from the switch and compares them with those in the fabric policy rules.

1. Navigate to the Fabric Software page for NX-OS and IOS-XE fabrics.
2. In the **Fabric Software** window, verify that the **Overview** tab is selected.
3. In the list of fabrics shown in the **Overview** page, locate the fabric where you want to recalculate compliance on the devices in that fabric.
4. In the row for that fabric, click the ellipsis at the end of that row (…), then select **Recalculate compliance**.

   The status provided in the **Status** column might get updated to **In-Sync** or **Out-of-Sync**, based on a comparison between the switch CLI and the fabric policy. Click on the status entry to show additional in-sync or out-of-sync details.

Upgrade or downgrade a group of switches

You have two upgrade methods and one downgrade method:

- Disruptive upgrade or downgrade: During the upgrade or downgrade process the switches go down temporarily, which results in a disruption in your fabric traffic.

  For more information, see Upgrade or downgrade switches (disruptive).

- Non-disruptive upgrade: This allows the switches to run without disruption in your fabric traffic.

  For more information, see Upgrade a group of switches (non-disruptive).

- Non-disruptive downgrade: Not supported.

Upgrade or downgrade switches (disruptive)

This section describes a disruptive method for upgrading or downgrading a group of switches.

Guidelines and limitations: Disruptive upgrade

- If you are downgrading a group of switches, the process is identical to the process for upgrading a group of switches, except that the target image that you choose will be earlier than the currently installed image. The text for dialogs, fields, buttons, and other controls in the UI specify “upgrade” even though you are downgrading the software.
- For switches running on NX-OS 9.3(11), there is an issue when upgrading the EPLD along with NX-OS using the `install all` option. This is not an issue with switches running on a release after

NX-OS 9.3(11).

To resolve this issue, follow these steps for an upgrade in this situation:

1. Install the NX-OS image from 9.3(11) to the destination version.
2. After the NX-OS upgrade, install the EPLD image.

Download an image from the Software Download website

This section describes how to download an image from the software download website.

1. Go to the Software Download website.

   Software Download Website

2. Login with your credentials. You must login to download the software.
3. Navigate to **Switches**, choose a series and a switch.
4. Choose a software type:
   - For Nexus switches:
     - NX-OS EPLD Updates
     - NX-OS Firmware
     - NX-OS Patch Release
     - NX-OS Software Maintenance Upgrades (SMU)
     - NX-OS System Software
   - For Cisco Catalyst switches: IOS XE Software

     For Cisco Catalyst switches, Nexus Dashboard provides support for software upgrade using CAT9K and CAT9K_LITE image types.
5. Choose the software file you want to download and click the download icon.

Upload the image to Nexus Dashboard

This section describes how to upload the image.

- In some cases, you can download an SMU image from the Software Download website wherein multiple RPMs are bundled together as a .tar file, and Nexus Dashboard allows you to upload this type of bundled .tar file to Nexus Dashboard. However, Nexus Dashboard normally does not allow you to upload any other type of bundled .tar file, so if you try to upload a bundled .tar file and you see an error message, use a .zip format instead for the bundle.
- If you are about to upload a compacted NX-OS image to the Nexus Dashboard image repository and another NX-OS image with the same name is currently in the repository, you might overwrite the existing (older) NX-OS image with the newer NX-OS image that you are about to upload. You can avoid overwriting the existing image using the following method:
  1. Upgrade the switches that can use normal NX-OS image first.

> 2. Delete the normal NX-OS image from the Nexus Dashboard repository using the Image Upload screen.
> 3. Upload the compact image and upgrade the other set of switches.

1. Navigate to the Fabric Software page for NX-OS and IOS-XE fabrics.
2. In the **Fabric Software** window, choose **Images**.
3. From the **Actions** drop-down list, select **Upload**.
4. In the **Upload Image** dialog box, either upload the file from a local device or or import from SCP or SFTP.

   > ℹ Uploading an image to SCP or SFTP server from a non-Unix based device is not supported.

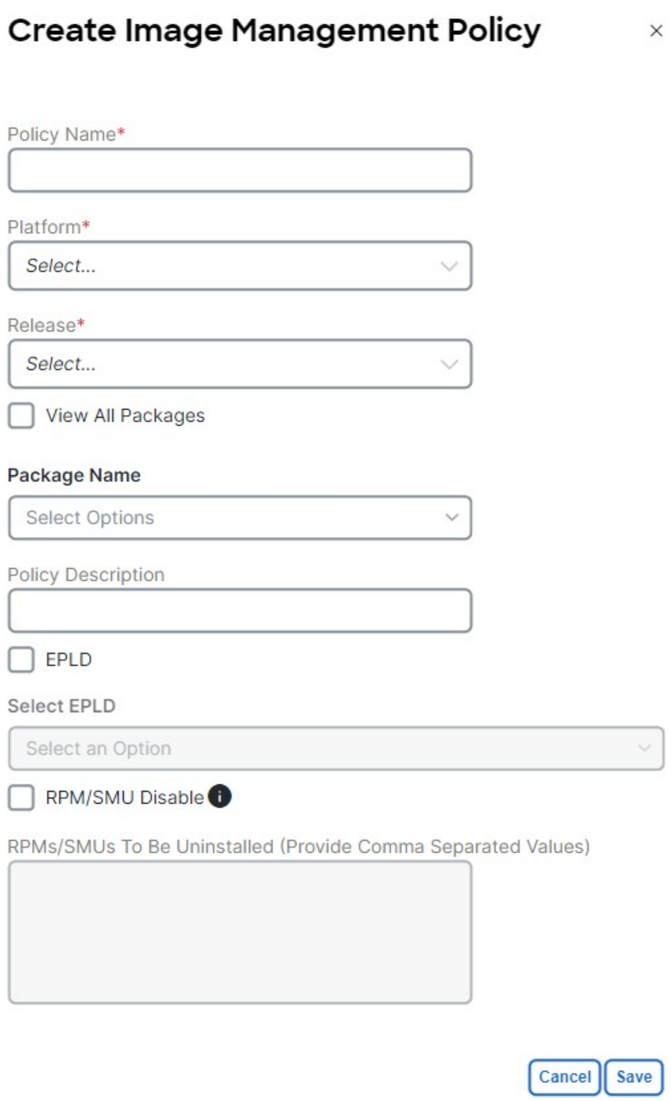
5. Click **Verify**.

   Now, the uploaded image is validated, downloaded and copied, and then verified.

Create the image policies

This section describes how to create the image policies.

1. Navigate to the Fabric Software page for NX-OS and IOS-XE fabrics.
2. In the **Fabric Software** window, choose **Image Policies**.
3. From the **Actions** drop-down list, select **Create**.
4. In the **Create Image Management Policy** dialog box, enter the following information:



Create Image Management Policy ×

Policy Name*

Platform*
Select...

Release*
Select...

□ View All Packages

Package Name
Select Options

Policy Description

□ EPLD

Select EPLD
Select an Option

□ RPM/SMU Disable

RPMs/SMUs To Be Uninstalled (Provide Comma Separated Values)

Cancel Save

Depending on the switch type, not all fields in the **Create Image Management Policy** dialog box are available to all the devices.

5. Click **Save**.

Attach or detach update groups to the switches

This section describes how to attach or detach switches to or from an update group. Grouping allows you to track upgrades for a set of switches. You can create several groups and select a switch regardless of the group, role, or type of switch.

We recommend that you create update groups based on the roles of the switches. For example, if a fabric has multiple switches with different roles, such as Leaf, Spine, Border, and more, creating groups based on different roles is recommended. This clearly separates roles and responsibilities during switch image management operations. Switches with different roles perform critical functionality and respond differently based on the control plane, data plane, and system-level convergence. For example, a user with the admin role can create multiple groups as follows:

- Group-Leaf-Even for Leaf switches that have even numbers or VPC role of primary
- Group-Leaf-Odd for Leaf switches that have odd numbers or VPC role of secondary

Typically, Spine and Border devices are limited to fabric, while the role of the Leaf is the most common one. Therefore, users with the admin role can upgrade individual Spines followed by Individual Borders, or create different groups for Spines and Borders. Users with the admin role can still leverage groups to divide the Leaf role switches and perform bulk actions.

1. Navigate to the Fabric Software page for NX-OS and IOS-XE fabrics.
2. In the **Fabric Software** window, choose **Devices**.
3. In the **Devices** window, place a checkmark in the checkbox for the devices you want to group.
4. From the **Actions** drop-down list, select **Modify groups**.
5. In the **Modify groups** dialog box, click the radio button to either **Attach Group** or **Detach Group**.
   - Select **Attach Group** and choose **Create Group** to create a new group or select an existing group from the **Group** drop-down list.
     - To create a group, enter a group name in the **Modify groups** dialog box.
     - Click **Save**.
   - Select **Detach Group** and click **Detach** to detach the devices from a group.

Attach a policy to the switches

This section describes how to attach a policy to the switches in disruptive mode.

1. Navigate to the Fabric Software page for NX-OS and IOS-XE fabrics.
2. In the **Fabric Software** window, choose **Devices**.
3. In the **Devices** window, select the devices you want to attach a policy.
4. From the **Actions** drop-down list, select **Modify policy**.
5. In the **Modify policy** dialog box, click the **Attach Policy** radio button and choose the required policy from the **Policy** drop-down list.
6. Clear the the **Stage & Validate** checkbox, if needed.

   This option deploys the image on to the switch and validates for compatibility with the existing software version on the switch. The checkbox is selected by default. This runs the compatibility check with non-disruptive mode by default. If this check fails, then the compatibility check is run in disruptive mode.

   You can uncheck this field while attaching the policy and perform a manual stage and validate, if required. For more information, see Copy the image to the switches and Validate the switches (optional).

7. Click **Attach**.

   The table in the **Devices** tab displays the status of the stage and validate operations.

8. Click the link in the **View Details** column to view the install log for details about these operations. You can use the log to learn about errors, if any.

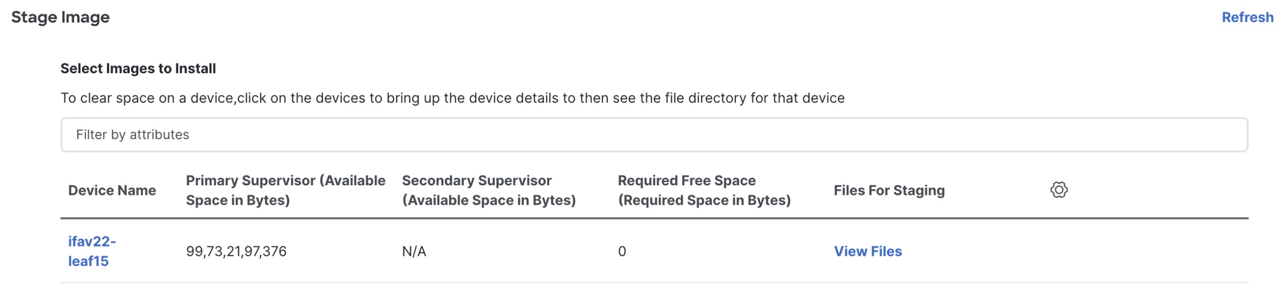
   The **History** tab also provides logs for all the configuration changes and details about the errors.

   On successful completion, the **Image Staged** and **Validated** columns will display a green icon for the respective devices.

Copy the image to the switches

The section describes how to copy the image to the switches.

1. Navigate to the Fabric Software page for NX-OS and IOS-XE fabrics.
2. In the **Fabric Software** window, choose **Devices**.
3. In the **Devices** window, place a checkmark in the checkbox for the device you want.
4. From the **Actions** drop-down list, select **Stage image**.
5. In the **Stage image** window, ensure there is enough space. The **Primary Supervisor (Available Space in Bytes)** displays in red if there is not enough space.



Stage Image

Select Images to Install

To clear space on a device,click on the devices to bring up the device details to then see the file directory for that device

Device Name	Primary Supervisor (Available Space in Bytes)	Secondary Supervisor (Available Space in Bytes)	Required Free Space (Required Space in Bytes)	Files For Staging	⚙
ifav22-leaf15	99,73,21,97,376	N/A	0	View Files	

To make more space:

- In the **Stage image** window, click on the device name.
- In the **Switch Overview** window, ensure you are on the **HardwareBootflash** tab, you will need to delete files to create space so you can stage the image.
- Place a checkmark on the file names that you want to delete.
- Click **Actions** and **Delete files**.
- In the **Warning Are you sure you want to delete?** dialog box, click **Confirm** to delete the files.
- Go back to the **Stage image** window and ensure the **Required Free Space** column displays 0.
- In the **Files for staging** column, click **View Files** to view details such as **File Name** and **Size** of the image files to be staged.

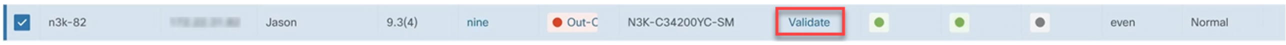
6. Click **Stage**.

Validate the switches (optional)

This section describes how to validate the switches to find out which switches can be upgraded by doing a compatibility check. This checks if the image is complete, if the image is valid for the individual hardware, and if the upgrade can be non-disruptive. The log files provide detailed information for each switch.

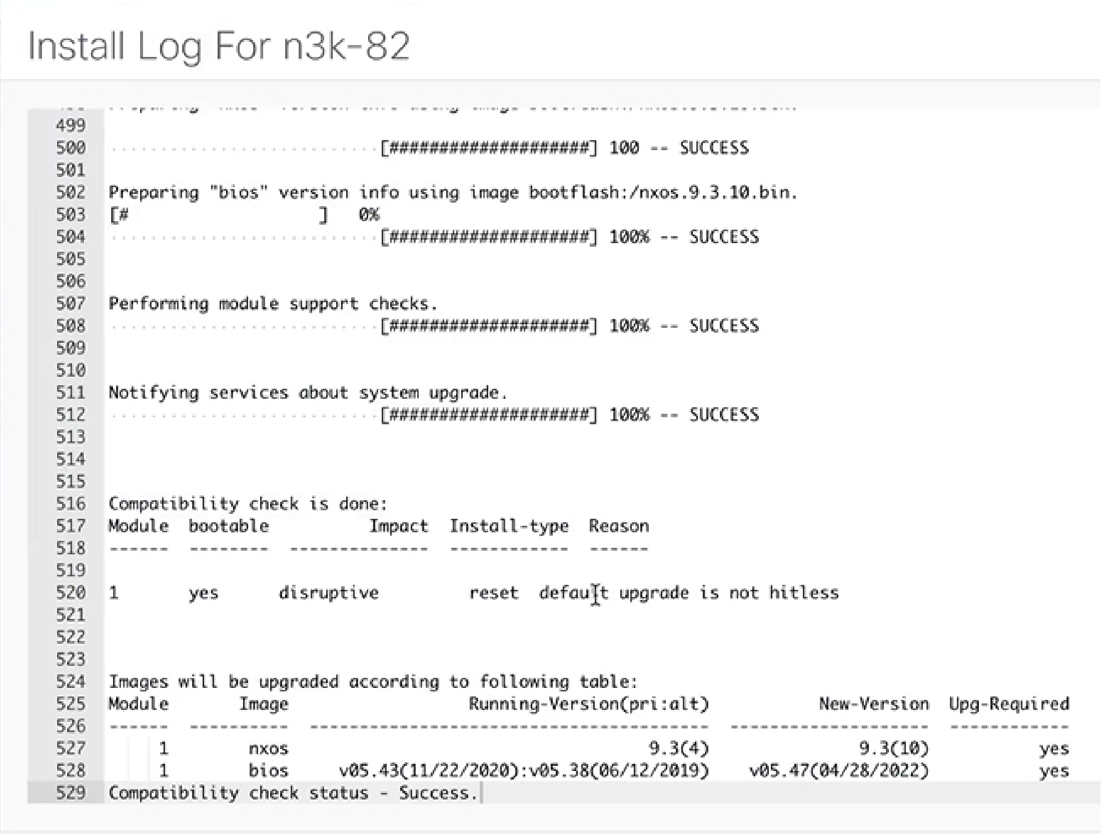
1. Navigate to the Fabric Software page for NX-OS and IOS-XE fabrics.
2. In the **Fabric Software** window, choose **Devices**.
3. In the **Devices** window, place a checkmark in the checkbox for the device you want to validate.
4. From the **Actions** drop-down list, select **Validate**.
5. In the **Validate** dialog box, place a checkmark in the checkbox if you want a non-disruptive upgrade.

6. Click **Validate**.
7. In the **Fabric Software** window, under the **View Details** column, click **Validate** to check on the log file for that switch.



☑ n3k-82 [redacted] Jason 9.3(4) nine ● Out-C N3K-C34200YC-SM Validate ● ● ● even Normal

8. In the **Fabric Software** window, under the **Validated** column, you can see the validation progress until it completes.
   - If the validation completed successfully, it shows green.
   - If the validation fails, it shows red. Check the log file under the **View Details** column. You will need to fix the errors before proceeding.



Install Log For n3k-82

```

..........................[####################] 100 -- SUCCESS

Preparing "bios" version info using image bootflash:/nxos.9.3.10.bin.
[#                   ]   0%
..........................[####################] 100% -- SUCCESS


Performing module support checks.
..........................[####################] 100% -- SUCCESS


Notifying services about system upgrade.
..........................[####################] 100% -- SUCCESS



Compatibility check is done:
Module  bootable          Impact  Install-type  Reason
------  --------  --------------  ------------  ------

1       yes      disruptive         reset  default upgrade is not hitless



Images will be upgraded according to following table:
Module       Image                  Running-Version(pri:alt)           New-Version  Upg-Required
------  ----------  ----------------------------------------  --------------------  ------------
    1        nxos                                    9.3(4)                9.3(10)           yes
    1        bios     v05.43(11/22/2020):v05.38(06/12/2019)    v05.47(04/28/2022)           yes
Compatibility check status - Success.
```

Create and run the pre-ISSU report on the switches (optional)

This section describes how to create and run the pre-ISSU report on the switches (optional).

1. Navigate to the Fabric Software page for NX-OS and IOS-XE fabrics.
2. In the **Fabric Software** window, choose **Devices**.
3. In the **Devices** window, place a checkmark in the checkbox for the devices you want to run a report.
4. From the **Actions** drop-down list, select **Run reports**.
5. In the **Create Report** dialog box, choose **Pre ISSU** radio button.
   a. Click **Select a Template**.
   b. In the **Select Report Template** dialog box, choose the **custom_swift_issu** template and click **Select**.

c. In the **Report Name** field, enter a name for the report.

   Ensure that you provide the same name for the pre and the post-ISSU reports which allows the system to associate the two reports.

d. Use the default values that are available in the fields and click **Generate**.

   > You cannot run the pre-ISSU report more than once. The system generates the report when ready. Ensure the status displays successful.

e. You can click on the link under the **Results** column to view the HTML version of the report.

Generate pre-upgrade or post-upgrade snapshots of the switch configuration (optional)

This topic describes how to generate snapshots of the configuration of a switch. It is a best practice to generate snapshots of the switch configuration before entering and after exiting the maintenance mode for performing an upgrade. You can use this to compare the configuration of the switch before it was moved into maintenance mode and after bringing back to normal mode.

1. Navigate to the Fabric Software page for NX-OS and IOS-XE fabrics.
2. In the **Fabric Software** window, choose **Devices**.
3. In the **Devices** window, place a checkmark in the checkbox for the required device.
4. From the **Actions** drop-down list, choose **Generate snapshot**.
5. In the **Generate snapshot** dialog box, click either **Pre-Upgrade-Snapshot** or **Post-Upgrade-Snapshot**.
6. Click **Save**.

   Based on the selection in the previous step, the system generates a pre-upgrade or post-upgrade snapshot for the switch.

7. Click the link in the **View Details** column for the respective switch to view the generated snapshot. These snapshots are only available after the pre-upgrade and post-upgrade snapshots are run.

   The **History** tab also provides logs for all the configuration changes and details about the errors.

Change mode for a switch

This section describes how to change mode for a switch.

1. Navigate to the Fabric Software page for NX-OS and IOS-XE fabrics.
2. In the **Fabric Software** window, choose **Devices**.
3. In the **Devices** window, place a checkmark in the checkbox for the device you want.
4. From the **Actions** drop-down list, select **Change Mode**.
5. In the **Change Mode** dialog box, choose between **Normal** or **Maintenance** modes.
6. Click **Deploy Now** or **Deploy Later**.

Upgrade or downgrade switches

This section describes how to upgrade or downgrade a switch or a group of switches or uninstall RPMs.

1. Navigate to the Fabric Software page for NX-OS and IOS-XE fabrics.
2. In the **Fabric Software** window, choose **Devices**.
3. Do one of the following:
    - Place a checkmark in the checkbox for the device you want to upgrade.
    - To upgrade a group of switches, filter on the **Update Groups**, select all, and place a checkmark in the checkbox for all the devices you want.
4. From the **Actions** drop-down list, select **Upgrade**.

    > You can choose to either upgrade NOS, EPLD, or RPM separately or all at once. EPLD Golden must be upgraded separately.

    a. Click on the **Upgrade** radio button.

    b. In the **Select Upgrades** field, place a checkmark on the upgrades you want.

    For Cisco Catalyst switches, you can only upgrade the NOS. EPLD and SMU upgrades are currently not supported.

    c. From the **Upgrade Options** drop-down list, select **Disruptive** or **Non-Disruptive**.

    d. If you selected **Disruptive** in the previous step, you can choose to enable **BIOS Force**.

    > Selecting this option requires a reload.

    If you chose **Non-Disruptive** in the previous step, then **BIOS Force** is disabled by default.

    e. You can view the **Validation Status** and filter, if needed.

    f. Click **Upgrade**.

Run the post-ISSU report on the switches (optional)

This section describes how to run the post-ISSU report on switches only if the mode was changed to normal mode.

> You must wait until the switch is fully operational before running the Post-ISSU.

1. Navigate to the Fabric Software page for NX-OS and IOS-XE fabrics.
2. In the **Fabric Software** window, choose **Devices**.
3. In the **Devices** window, place a checkmark in the checkbox for the devices you want to run the post-ISSU.
4. From the **Actions** drop-down list, select **Run reports**.
5. In the **Create Report** dialog box, choose **Post ISSU** radio button.

    a. Click **Select a Template**.

b. In the **Select Report Template** dialog box, choose the **custom_swift_issu** template and click **Select**.

c. From the **Report Name** drop-down list, select the name of the pre-ISSU report that you have generated and click **Generate**.

d. Use the default values that are available in the fields and click **Generate**. The system generates the report when ready. Ensure the status displays successful.

e. You can click on the link under the **Results** column to view the HTML version of the report.

The post-ISSU report displays a summary of the results of the checks performed before and after the upgrade, consecutively. Analyze the report for any errors and take corrective actions, as required.

6. Perform the following to view the reports:

a. Navigate to:

Analyze > Reports

b. In the **Reports** window, click on the link displayed under the **Title** column of the report that you want to view.

c. In the **Report** dialog box, click the expand icon to open the HTML version of the report. The window displays a summary and the details about the errors, warnings, info and success messages. It also displays a snapshot of the configuration before and after the upgrade.

Generate post-upgrade snapshot of the switch configuration (optional)

This topic describes how to generate snapshots of the configuration of a switch. It is a best practice to generate snapshots of the switch configuration before entering and exiting the maintenance mode for performing an upgrade. You can use this to compare the configuration of the switch before it was moved into maintenance mode and after bringing back to normal mode.

1. Navigate to the Fabric Software page for NX-OS and IOS-XE fabrics.
2. In the **Fabric Software** window, choose **Devices**.
3. In the **Devices** window, place a checkmark in the checkbox for the required device.
4. From the **Actions** drop-down list, choose **Generate snapshot**.
5. In the **Generate snapshot** dialog box, click **Post-Upgrade-Snapshot**.
6. Click **Save**.

   The system generates a post upgrade snapshot for the switch.

7. Click the link in the **View Details** column for the respective switch to view the snapshots and the pre and post snapshot comparison summary generated for the switch. The **History** tab also provides logs for all the configuration changes and details about the errors.

Upgrade a group of switches (non-disruptive)

This section describes a non-disruptive method for upgrading a group of switches.

Guidelines and limitations: Non-disruptive upgrade

- An EPLD upgrade using the install all command when upgrading switches using the non-disruptive option is not supported on these switch platforms on the NX-OS 10.5.3 version for the bundled image:
  - N9K-C93180YC-FX
  - N9K-C93108TC-FX
  - N9K-C9348GC-FXP
  - N9K-C93240YC-FX2
  - N9K-C9336C-FX2
  - N9K-C9364C
  - N9K-C9332C
  - N9K-C9232C
  - N9K-SUP-A+
  - N9K-SUP-B+
  - N3K-C36180YC-R
  - N3K-C3636C-R
  - N9K-SUP-A
  - N9K-SUP-B

  In these cases, use the install epld command separately to update the EPLD.

Download an image from the Software Download website

This section describes how to download an image from the software download website.

1. Go to the Software Download website.

   Software Download Website

2. Login with your credentials. You must login to download the software.
3. Navigate to **Switches**, choose a series and a switch.
4. Choose a software type:
   - For Nexus switches:
     - NX-OS EPLD Updates
     - NX-OS Firmware
     - NX-OS Patch Release
     - NX-OS Software Maintenance Upgrades (SMU)
     - NX-OS System Software
   - For Cisco Catalyst switches: IOS XE Software

     For Cisco Catalyst switches, Nexus Dashboard provides support for software upgrade using CAT9K and CAT9K_LITE image types.

5. Choose the software file you want to download and click the download icon.

Upload the image to Nexus Dashboard

This section describes how to upload the image.

> - In some cases, you can download an SMU image from the Software Download website wherein multiple RPMs are bundled together as a .tar file, and Nexus Dashboard allows you to upload this type of bundled .tar file to Nexus Dashboard. However, Nexus Dashboard normally does not allow you to upload any other type of bundled .tar file, so if you try to upload a bundled .tar file and you see an error message, use a .zip format instead for the bundle.
> - If you are about to upload a compacted NX-OS image to the Nexus Dashboard image repository and another NX-OS image with the same name is currently in the repository, you might overwrite the existing (older) NX-OS image with the newer NX-OS image that you are about to upload. You can avoid overwriting the existing image using the following method:
>   1. Upgrade the switches that can use normal NX-OS image first.
>   2. Delete the normal NX-OS image from the Nexus Dashboard repository using the Image Upload screen.
>   3. Upload the compact image and upgrade the other set of switches.

1. Navigate to the Fabric Software page for NX-OS and IOS-XE fabrics.
2. In the **Fabric Software** window, choose **Images**.
3. From the **Actions** drop-down list, select **Upload**.
4. In the **Upload Image** dialog box, either upload the file from a local device or or import from SCP or SFTP.

   > Uploading an image to SCP or SFTP server from a non-Unix based device is not supported.

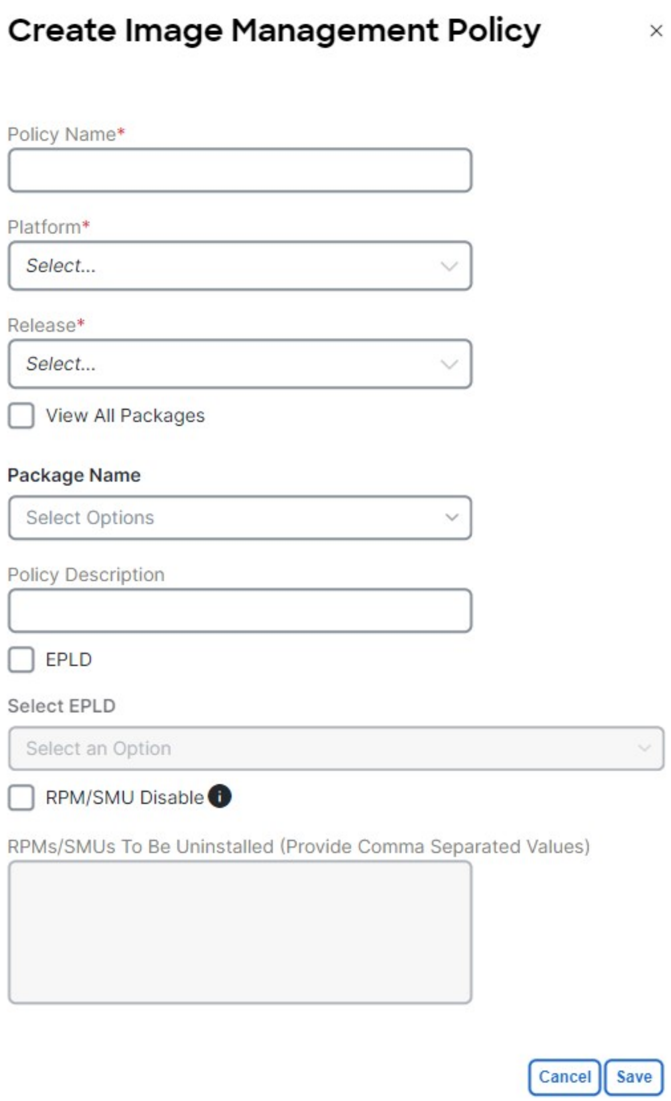
5. Click **Verify**.

   Now, the uploaded image is validated, downloaded and copied, and then verified.

Create the image policies

This section describes how to create the image policies.

1. Navigate to the Fabric Software page for NX-OS and IOS-XE fabrics.
2. In the **Fabric Software** window, choose **Image Policies**.
3. From the **Actions** drop-down list, select **Create**.
4. In the **Create Image Management Policy** dialog box, enter the following information:



Create Image Management Policy ×

Policy Name*

Platform*
Select...

Release*
Select...

□ View All Packages

Package Name
Select Options

Policy Description

□ EPLD

Select EPLD
Select an Option

□ RPM/SMU Disable

RPMs/SMUs To Be Uninstalled (Provide Comma Separated Values)

Depending on the switch type, not all fields in the **Create Image Management Policy** dialog box are available to all the devices.

5. Click **Save**.

Attach or detach update groups to the switches

This section describes how to attach or detach switches to or from an update group. Grouping allows you to track upgrades for a set of switches. You can create several groups and select a switch regardless of the group, role, or type of switch.

We recommend that you create update groups based on the roles of the switches. For example, if a fabric has multiple switches with different roles, such as Leaf, Spine, Border, and more, creating groups based on different roles is recommended. This clearly separates roles and responsibilities during switch image management operations. Switches with different roles perform critical functionality and respond differently based on the control plane, data plane, and system-level convergence. For example, a user with the admin role can create multiple groups as follows:

- Group-Leaf-Even for Leaf switches that have even numbers or VPC role of primary
- Group-Leaf-Odd for Leaf switches that have odd numbers or VPC role of secondary

Typically, Spine and Border devices are limited to fabric, while the role of the Leaf is the most common one. Therefore, users with the admin role can upgrade individual Spines followed by Individual Borders, or create different groups for Spines and Borders. Users with the admin role can still leverage groups to divide the Leaf role switches and perform bulk actions.

1. Navigate to the Fabric Software page for NX-OS and IOS-XE fabrics.
2. In the **Fabric Software** window, choose **Devices**.
3. In the **Devices** window, place a checkmark in the checkbox for the devices you want to group.
4. From the **Actions** drop-down list, select **Modify groups**.
5. In the **Modify groups** dialog box, click the radio button to either **Attach Group** or **Detach Group**.
   - Select **Attach Group** and choose **Create Group** to create a new group or select an existing group from the **Group** drop-down list.
     - To create a group, enter a group name in the **Modify groups** dialog box.
     - Click **Save**.
   - Select **Detach Group** and click **Detach** to detach the devices from a group.

Attach a policy to the switches

This section describes how to attach a policy to the switches in disruptive mode.

1. Navigate to the Fabric Software page for NX-OS and IOS-XE fabrics.
2. In the **Fabric Software** window, choose **Devices**.
3. In the **Devices** window, select the devices you want to attach a policy.
4. From the **Actions** drop-down list, select **Modify policy**.
5. In the **Modify policy** dialog box, click the **Attach Policy** radio button and choose the required policy from the **Policy** drop-down list.
6. Clear the the **Stage & Validate** checkbox, if needed.

   This option deploys the image on to the switch and validates for compatibility with the existing software version on the switch. The checkbox is selected by default. This runs the compatibility check with non-disruptive mode by default. If this check fails, then the compatibility check is run in disruptive mode.

   You can uncheck this field while attaching the policy and perform a manual stage and validate, if required. For more information, see Copy the image to the switches and Validate the switches (optional).

7. Click **Attach**.

   The table in the **Devices** tab displays the status of the stage and validate operations.

8. Click the link in the **View Details** column to view the install log for details about these operations. You can use the log to learn about errors, if any.

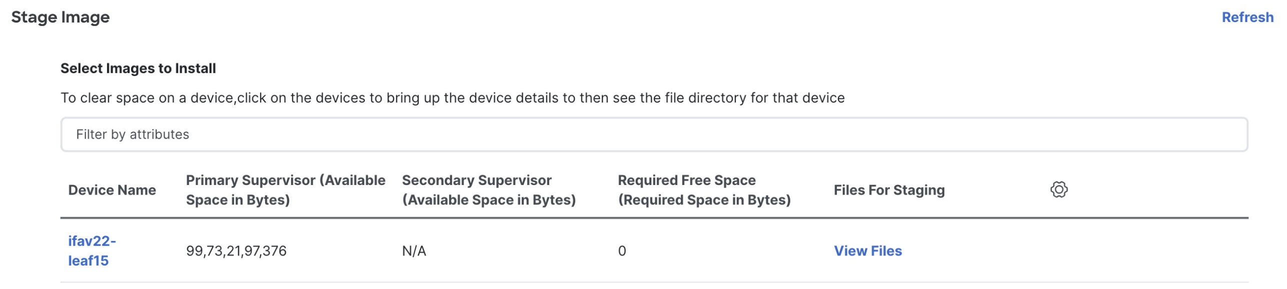
   The **History** tab also provides logs for all the configuration changes and details about the errors.

   On successful completion, the **Image Staged** and **Validated** columns will display a green icon for the respective devices.

Copy the image to the switches

The section describes how to copy the image to the switches.

1. Navigate to the Fabric Software page for NX-OS and IOS-XE fabrics.
2. In the **Fabric Software** window, choose **Devices**.
3. In the **Devices** window, place a checkmark in the checkbox for the device you want.
4. From the **Actions** drop-down list, select **Stage image**.
5. In the **Stage image** window, ensure there is enough space. The **Primary Supervisor (Available Space in Bytes)** displays in red if there is not enough space.



Stage Image

Select Images to Install

To clear space on a device,click on the devices to bring up the device details to then see the file directory for that device

Device Name	Primary Supervisor (Available Space in Bytes)	Secondary Supervisor (Available Space in Bytes)	Required Free Space (Required Space in Bytes)	Files For Staging	⚙
ifav22-leaf15	99,73,21,97,376	N/A	0	View Files	

To make more space:

- In the **Stage image** window, click on the device name.
- In the **Switch Overview** window, go to the **Hardware** > **Bootflash** tab. Verify if you need to delete files to create space so you can stage the image.
- Place a checkmark on the file names that you want to delete.
- Click **Actions** and **Delete files**.
- In the **Warning Are you sure you want to delete?** dialog box, click **Confirm** to delete the files.
- Go back to the **Stage image** window to stage the image.
- Verify that the device credentials are configured and **LAN Device Management Connectivity** is updated as per the switch connectivity.

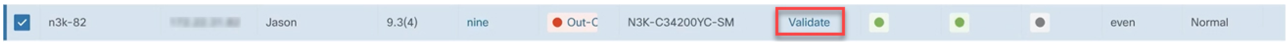
6. Click **Stage**.

Validate the switches (optional)

This section describes how to validate the switches to find out which switches can be upgraded by doing a compatibility check. This checks if the image is complete, if the image is valid for the individual hardware, and if the upgrade can be non-disruptive. The log files provide detailed information for each switch.

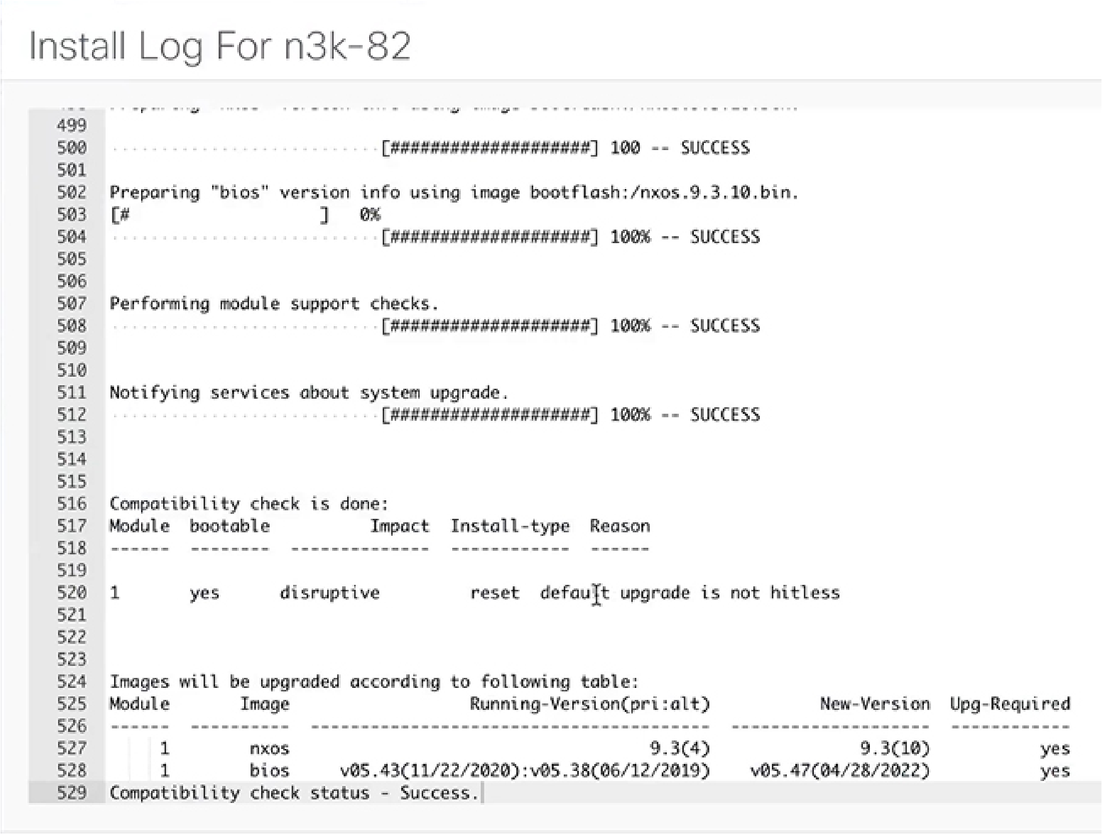
1. Navigate to the Fabric Software page for NX-OS and IOS-XE fabrics.
2. In the **Fabric Software** window, choose **Devices**.
3. In the **Devices** window, place a checkmark in the checkbox for the device you want to validate.
4. From the **Actions** drop-down list, select **Validate**.
5. In the **Validate** dialog box, place a checkmark in the checkbox if you want a non-disruptive upgrade.

6. Click **Validate**.
7. In the **Fabric Software** window, under the **View Details** column, click **Validate** to check on the log file for that switch.



☑	n3k-82	[redacted]	Jason	9.3(4)	nine	● Out-C	N3K-C34200YC-SM	Validate	●	●	●	even	Normal

8. In the **Fabric Software** window, under the **Validated** column, you can see the validation progress until it completes.
   - If the validation completed successfully, it shows green.
   - If the validation fails, it shows red. Check the log file under the **View Details** column. You will need to fix the errors before proceeding.



Install Log For n3k-82

```

..........................[####################] 100 -- SUCCESS

Preparing "bios" version info using image bootflash:/nxos.9.3.10.bin.
[#                    ]   0%
..........................[####################] 100% -- SUCCESS


Performing module support checks.
..........................[####################] 100% -- SUCCESS


Notifying services about system upgrade.
..........................[####################] 100% -- SUCCESS



Compatibility check is done:
Module  bootable          Impact  Install-type  Reason
------  --------  --------------  ------------  ------

1       yes      disruptive         reset  default upgrade is not hitless



Images will be upgraded according to following table:
Module       Image                Running-Version(pri:alt)           New-Version  Upg-Required
------  ----------  ----------------------------------------  --------------------  ------------
    1        nxos                                    9.3(4)                9.3(10)           yes
    1        bios     v05.43(11/22/2020):v05.38(06/12/2019)    v05.47(04/28/2022)           yes
Compatibility check status - Success.
```

Create and run the pre-ISSU report on the switches (optional)

This section describes how to create and run the pre-ISSU report on the switches (optional).

1. Navigate to the Fabric Software page for NX-OS and IOS-XE fabrics.
2. In the **Fabric Software** window, choose **Devices**.
3. In the **Devices** window, place a checkmark in the checkbox for the devices you want to run a report.
4. From the **Actions** drop-down list, select **Run reports**.
5. In the **Create Report** dialog box, choose **Pre ISSU** radio button.
   a. Click **Select a Template**.
   b. In the **Select Report Template** dialog box, choose a template and click **Select**.
   c. Answer all the questions and click **Generate**.

Generate pre-upgrade or post-upgrade snapshots of the switch configuration (optional)

This topic describes how to generate snapshots of the configuration of a switch. It is a best practice to generate snapshots of the switch configuration before entering and after exiting the maintenance mode for performing an upgrade. You can use this to compare the configuration of the switch before it was moved into maintenance mode and after bringing back to normal mode.

1. Navigate to the Fabric Software page for NX-OS and IOS-XE fabrics.
2. In the **Fabric Software** window, choose **Devices**.
3. In the **Devices** window, place a checkmark in the checkbox for the required device.
4. From the **Actions** drop-down list, choose **Generate snapshot**.
5. In the **Generate snapshot** dialog box, click either **Pre-Upgrade-Snapshot** or **Post-Upgrade-Snapshot**.
6. Click **Save**.

   Based on the selection in the previous step, the system generates a pre-upgrade or post-upgrade snapshot for the switch.

7. Click the link in the **View Details** column for the respective switch to view the generated snapshot. These snapshots are only available after the pre-upgrade and post-upgrade snapshots are run.

   The **History** tab also provides logs for all the configuration changes and details about the errors.

Upgrade a group of switches (non-disruptive)

This section describes how to upgrade a group of switches.

1. Navigate to the Fabric Software page for NX-OS and IOS-XE fabrics.
2. In the **Fabric Software** window, choose **Devices**.
3. In the **Devices** window, filter on the **Upgrade Groups**, select all, and place a checkmark in the checkbox for all the devices you want.
4. From the **Actions** drop-down list, select **Upgrade**.

   > You may need to upgrade up to 2 times (NXOS, RPM).

   a. Click on the **Upgrade** radio button.
   b. In the **Select Upgrades** field, place a checkmark on the upgrades you want.
   c. In the Upgrade Options field, select **Force Non-Disruptive**.
   d. Do not check the Bios forced checkbox.
   e. You can view the **Validation Status** and filter if needed.
   f. Click **Upgrade**.
5. After all the switches within the group are fully upgraded. Repeat this procedure for the next group.

Run the post-ISSU report on the switches (optional)

This section describes how to run the post-ISSU report on switches (Optional).

1. Navigate to the Fabric Software page for NX-OS and IOS-XE fabrics.
2. In the **Fabric Software** window, choose **Devices**.
3. In the **Devices** window, place a checkmark in the checkbox for the devices you want to run the post-ISSU.
4. From the **Actions** drop-down list, select **Run reports**.
5. In the **Create Report** dialog box, choose **Post ISSU** radio button.
   a. Click **Select a Template**.
   b. In the **Select Report Template** dialog box, choose a template and click **Select**.
   c. Answer all the questions and click **Generate**.

Generate post-upgrade snapshot of the switch configuration (optional)

This topic describes how to generate snapshots of the configuration of a switch. It is a best practice to generate snapshots of the switch configuration before entering and exiting the maintenance mode for performing an upgrade. You can use this to compare the configuration of the switch before it was moved into maintenance mode and after bringing back to normal mode.

1. Navigate to the Fabric Software page for NX-OS and IOS-XE fabrics.
2. In the **Fabric Software** window, choose **Devices**.
3. In the **Devices** window, place a checkmark in the checkbox for the required device.
4. From the **Actions** drop-down list, choose **Generate snapshot**.
5. In the **Generate snapshot** dialog box, click **Post-Upgrade-Snapshot**.
6. Click **Save**.

   The system generates a post upgrade snapshot for the switch.

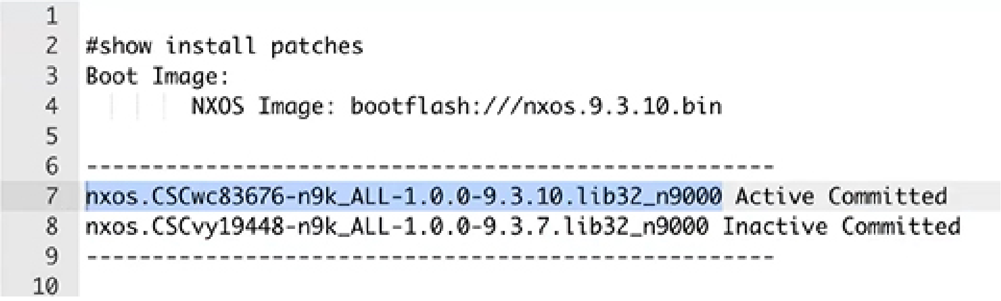
7. Click the link in the **View Details** column for the respective switch to view the snapshots and the pre and post snapshot comparison summary generated for the switch. The **History** tab also provides logs for all the configuration changes and details about the errors.

Uninstall packages from a switch

This section describes how to uninstall packages from a switch. You first need to take note of the patch names, detach the packages, and then uninstall them.

1. Navigate to **Manage > Inventory**.
2. Place a checkmark in the checkbox for the device you want to uninstall packages from.
3. From the **Actions** drop-down list, select **More > Show Commands**.
4. In the **Switch show commands** window, enter the following:
   a. In the **Commands** field, choose **show**.
   b. Under the Variables section, in the **show** field, enter **install patches**.

In the right pane it lists the package names. Take note of the package names you want to uninstall by copying the file name. For example:

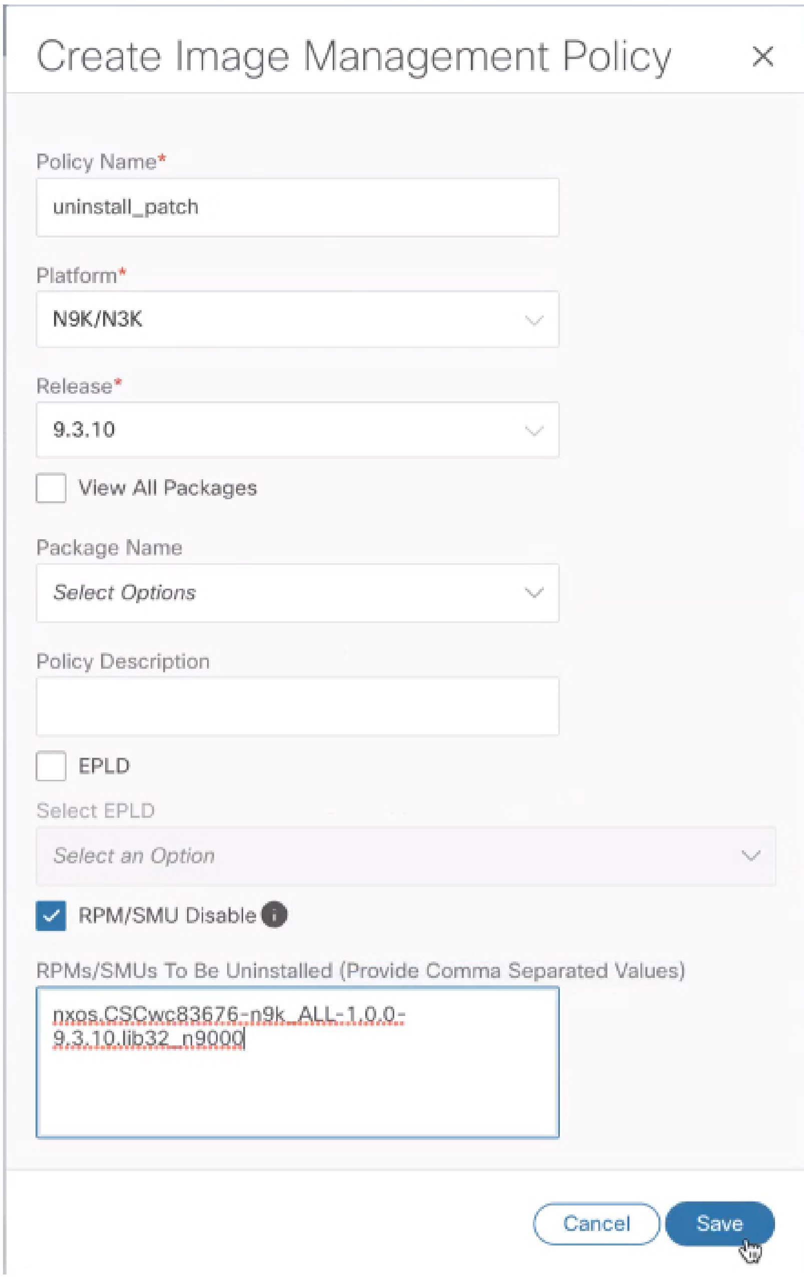


```

#show install patches
Boot Image:
        NXOS Image: bootflash:///nxos.9.3.10.bin

----------------------------------------------------
nxos.CSCwc83676-n9k_ALL-1.0.0-9.3.10.lib32_n9000 Active Committed
nxos.CSCvy19448-n9k_ALL-1.0.0-9.3.7.lib32_n9000 Inactive Committed
----------------------------------------------------

```

c. Exit the window.

5. Navigate to the Fabric Software page for NX-OS and IOS-XE fabrics.
6. In the **Fabric Software** window, choose **Image Policies**.
7. From the **Actions** drop-down list, select **Create**.
8. In the **Created Image Management Policy** dialog box, enter the following:
   a. In the **Policy Name** field, enter a policy name. For example, **uninstall_patch**.
   b. From the **Platform** drop-down list, choose the correct platform.
   c. Do not check the **View All Packages** checkbox.
   d. In the **Package Name** field, leave it blank.
   e. In the **Policy description** field, leave it blank.
   f. Do not check the **ELPD** checkbox.
   g. In the **Select ELPD** field, leave it blank.
   h. Place a checkmark in the **RPM/SMU Disable** in the checkbox.
   i. In the **RPMs/SMUs To Be Uninstalled** field, enter the packages.

Provide a comma to separate the values.



Create Image Management Policy

Policy Name*: uninstall_patch

Platform*: N9K/N3K

Release*: 9.3.10

□ View All Packages

Package Name: *Select Options*

Policy Description:

□ EPLD

Select EPLD: *Select an Option*

☑ RPM/SMU Disable

RPMs/SMUs To Be Uninstalled (Provide Comma Separated Values): nxos.CSCwc83676-n9k_ALL-1.0.0-9.3.10.lib32_n9000

   j. Click **Save**.

9. In the **Fabric Software** window, choose **Devices**.

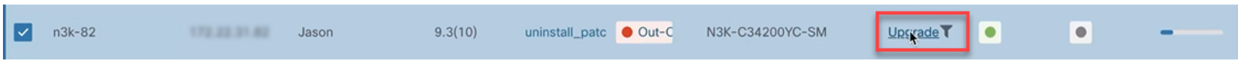
10. In the **Devices** window, place a checkmark in the checkbox for the devices you want to modify the policy.

11. From the **Actions** drop-down list, select **Modify policy**.

12. In the **Modify policy** dialog box, enter the following:

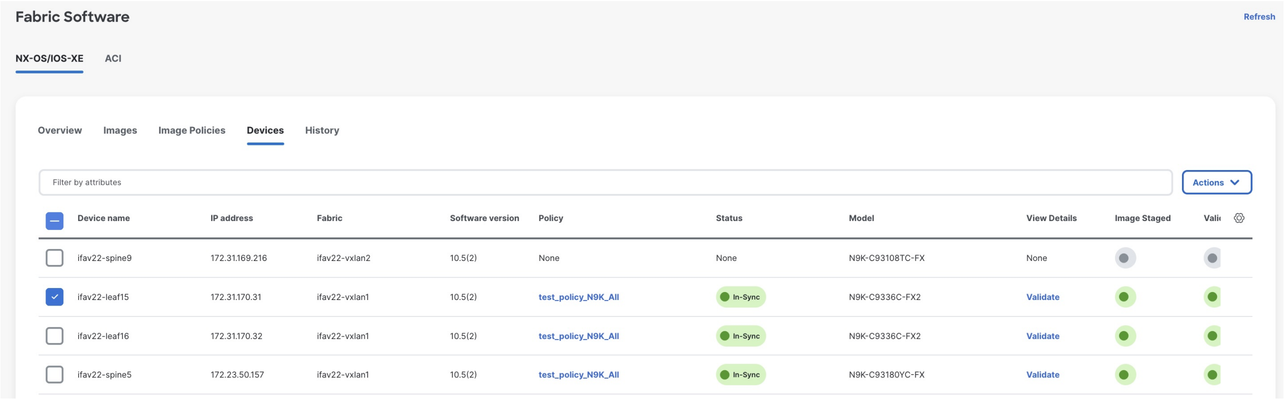
    a. Click on the **Attach Policy** radio button.

    b. In the **Policy** field, select the **Policy** and click **Attach**. For example:



☑ n3k-82 [redacted] Jason 9.3(10) uninstall_patc ● Out-C N3K-C34200YC-SM Upgrade ● ●

13. The switch then recalculates based on the above selection. Click the **Status** column for information about the switch. For example:



Fabric Software

Refresh

NX-OS/IOS-XE ACI

Overview Images Image Policies Devices History

Filter by attributes

Actions

☐	Device name	IP address	Fabric	Software version	Policy	Status	Model	View Details	Image Staged	Vali
☐	ifav22-spine9	172.31.169.216	ifav22-vxlan2	10.5(2)	None	None	N9K-C93108TC-FX	None	●	●
☑	ifav22-leaf15	172.31.170.31	ifav22-vxlan1	10.5(2)	test_policy_N9K_All	● In-Sync	N9K-C9336C-FX2	Validate	●	●
☐	ifav22-leaf16	172.31.170.32	ifav22-vxlan1	10.5(2)	test_policy_N9K_All	● In-Sync	N9K-C9336C-FX2	Validate	●	●
☐	ifav22-spine5	172.23.50.157	ifav22-vxlan1	10.5(2)	test_policy_N9K_All	● In-Sync	N9K-C93180YC-FX	Validate	●	●

14. In the **Status** column, it shows the packages that will be removed.

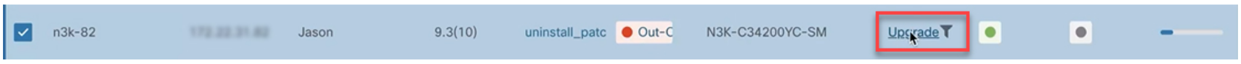
15. To remove the packages, in the **Devices** window, make sure the checkmark is placed in the checkbox for the devices you want to remove the packages from.

16. From the **Actions** drop-down list, select **Upgrade**.

17. In the **Upgrade/Uninstall** window, enter the following:

    a. Click on the **Uninstall** radio button and click **Uninstall**.

    b. In the **Devices** window, you can check the uninstall progress of the device if you click on the **Upgrade** under the View Details column.

☑	n3k-82	[redacted]	Jason	9.3(10)	uninstall_patc	● Out-C	N3K-C34200YC-SM	Upgrade	●	●

    c. Once the packages has been removed, the status will show **In-Sync** in green and **Upgrade** will show a green button.

    d. In the **Devices** window, you can also verify if the packages were uninstalled successfully by viewing the log file. Click on **Upgrade** for that device under the View Details column.

Understand Fabric Software for ACI fabrics

This section provides detailed information for the Fabric Software feature in Nexus Dashboard for ACI fabrics.

Navigate to the Fabric Software window for ACI fabrics

To navigate to the Fabric Software window:

1. Click **Manage > Fabric Software**.
2. Click the **ACI** tab.
   - Cisco's recommended versions: The software versions that Cisco recommends. These are the latest versions available for upgrade or for running an analysis.
   - Current version: This is the software version that the fabric is currently running.
   - Recommended: Displays the recommended software version to upgrade to. This version is determined based on the current version the fabric is running on.

     For example, if the fabric is currently on version 6.0(3d), then the **Recommended version** indicates 6.0(3d). However, if the **Current version** is newer than the recommended versions, then this field will be blank.

NOTE:

- **Delta analysis** is no longer a part of the post-upgrade assist workflow. In **Delta analysis**, you can only run an analysis per fabric unlike **Upgrade assist**, where you can choose a subset of devices to analyse.
- When you initially run an analysis, you can **Rerun the report** from the **Pre-update analysis** drawer to collect fresh data. Once your devices are upgraded, you can run a post-upgrade analysis. However, this disables the **Rerun the report** button in the pre-update analysis drawer.

Understand the information provided in the Fabric Software window for ACI fabrics

1. Connect to Intersight if you are not connected already.

   Hover over the link icon in the Sofware Versions area to see if you are connected to Intersight. Intersight connectivity is required for Nexus Dashboard to automatically check for recommended software versions for the ACI fabrics. See Working with Intersight for more information.

2. Review the information in the **Software Versions** area.

   The **Software Versions** area provides information on recommended software releases for your ACI fabrics and links to the Release Notes for those software releases.

First Published: 2025-01-31
Last Modified: 2025-08-07