Upgrading or Downgrading the Cisco Nexus 3600 Series NX-OS Software

This chapter describes how to upgrade or downgrade the Cisco NX-OS software. It contains the following sections:

Software Image

Each device is shipped with the Cisco NX-OS software. The Cisco NX-OS software consists of one NXOS software image. The image filename begins with **nxos**.

Only this image is required to load the Cisco NX-OS operating system. This image runs on all Cisco Nexus 3600 Series switches.

Note

- Starting from Cisco NX-OS Release 10.5(3)F, Cisco NX-OS no longer provides a separate EPLD image. The EPLD image is bundled with the NX-OS images and so the image sizes are correspondingly larger.
- Until Cisco NX-OS Release 10.5(2)F, Cisco provided separate electronic programmable logic device (EPLD) image upgrades to enhance hardware functionality or to resolve known hardware issues. For more information on EPLD images and the upgrade process, refer to the relevant version of *Cisco Nexus 3600 Platform FPGA/EPLD Upgrade Release Notes* on Cisco.com
- Another type of binary file is the software maintenance upgrade (SMU) package file. SMUs contain fixes for specific defects. They are created to respond to immediate issues and do not include new features. SMU package files are available for download from Cisco.com and generally include the ID number of the resolved defect in the filename. For more information on SMUs, see the *Performing Software Maintenance Upgrades (SMUs)* chapter in Cisco Nexus 3600 System Management Configuration Guide.
- For information about the supported upgrade paths, see Cisco Nexus 9000 and 3000 Upgrade and ISSU Matrix .

EPLD image

The Cisco Nexus 3636C-R and 36180YC-R NX-OS mode switches contain several programmable logical devices (PLDs) that provide hardware functions in all modules. Cisco provides electronic programmable logic device (EPLD) image upgrades to enhance hardware functions or to resolve known issues. PLDs include electronic programmable logic devices (EPLDs), field programmable gate arrays (FPGAs), and complex programmable logic devices (CPLDs), but they do not include ASICs. In this document, the term EPLD is used for FPGA and CPLDs.

Note

- For more information regarding EPLD, refer to *Cisco Nexus 3600 Platform FPGA/EPLD Upgrade Release Notes* on Cisco.com.
- Until Cisco NX-OS Release 10.5(2)F, ISSU supports EPLD image upgrades using the **install all nxos**<*nxos-image*>**epld**<*epld-image*> command during disruptive system (NX-OS) upgrade.
- While upgrading from pre-10.5(3)F releases to 10.5(3)F and later, you need to upgrade to 10.5(3) NX-OS first using the **install all**<*nxos-image*> command. After the NX-OS upgrade is complete, you can upgrade EPLD using the **install epld** command.
- Beginning with Cisco NX-OS Release 10.5(3)F, EPLD upgrade takes place during an ISSU system upgrade. If you need to avoid EPLD upgrade, use the **skip-epld** option. Do not use the **epld**<*epld-image*> option as the EPLD image is bundled with the NX-OS images and a separate EPLD image is no longer provided.

Recommendations for Upgrading the Cisco NX-OS Software

Cisco recommends performing a Nexus Health and Configuration Check before performing an upgrade. The benefits include identification of potential issues, susceptible Field Notices and Security Vulnerabilities,

missing recommended configurations and so on. For more information about the procedure, see Perform Nexus Health and Configuration Check.

Cisco NX-OS Software Upgrade Guidelines

Note The Cisco Nexus 3600 Series NX-OS Release Notes contain specific upgrade guidelines for each release. See the Release Notes before starting the upgrade.

Before attempting to upgrade to any software image, follow these guidelines:

- Schedule the upgrade when your network is stable and steady.
- Avoid any power interruption, which could corrupt the software image, during the installation procedure.
- On devices with dual supervisor modules, both supervisor modules must have connections on the console ports to maintain connectivity when switchovers occur during a software upgrade. See the Hardware Installation Guide for your specific chassis.
- If you upgrade from a Cisco NX-OS release that supports the CoPP feature to a Cisco NX-OS release that supports the CoPP feature with additional classes for new protocols, you must either run the setup utility using the **setup** command or use the **copp profile** command for the new CoPP classes to be available. For more information on these commands, see the "Configuring Control Plane Policing" chapter in the Cisco Nexus 3600 Series NX-OS Security Configuration Guide.
- When you upgrade from an earlier release to a Cisco NX-OS release that supports switch profiles, you have the option to move some of the running-configuration commands to a switch profile. For more information, see the Cisco Nexus 3600 Series NX-OS System Management Configuration Guide.
- By default, the software upgrade process is disruptive.
- Beginning with Cisco NX-OS Release 10.4(2)F, for Nexus 3600-R platform, to upgrade bios to the latest version you should first upgrade to nxos image. This release onwards, the install all nxos command only upgrades the nxos sw to the latest version but the bios image will be upgraded to the last bios released prior to 10.4(2)F version.

  To upgrade to bios released with 10.4(2)F or higher version, first upgrade the nxos image and then use bios-force option to upgrade the bios. For example,

  1. Install all nxos bootflash:nxos64-msll.10.4.2.F.bin.

     The system reloads and boots up with 10.4(2)F image.

  2. Install all nxos bios-force.

Note The device reloads twice, once for nxos upgrade and then again for bios upgrade.

- Beginning with Cisco NX-OS Release 10.5(3)F, all NX-OS images are bundled with EPLD image and EPLD upgrade is triggered automatically as part of the **install all nxos** command. However, you have the option to skip the EPLD image upgrade.

- From Cisco NX-OS Release 10.6(1)F, while installing nx-os using the **install all nx-os** command on switches affected by secure boot vulnerability, if the IO FPGA version of the device is lower than the Fixed IO FPGA version, EPLD upgrade does not take place. To upgrade the FPGA, use the **install epld** command. For more information about switches affected by secure boot vulnerability and Fixed IO FPGA version, refer to *Table 1* in the FPGA/EPLD Upgrade Procedure to Address Secure Boot Vulnerability document.
- While performing non-disruptive ISSU from Cisco NX-OS Release 10.4(6)M to 10.6(1)F and later releases, on Cisco Nexus 9300-FX switches and line cards, IGMP traffic is forwarded on vPC legs towards the vPC pair. When there are multiple FEX devices on the vPC peer undergoing ISSU, multicast traffic loss can occur during the upgrade of the FEX devices. To resolve this, configure the **ip igmp group-timeout 450** command on all VLANs that carry IGMP traffic across the vPC peer link.

Prerequisites for Upgrading the Cisco NX-OS Software

Upgrading the Cisco NX-OS software has the following prerequisites:

- Ensure that everyone who has access to the device or the network is not configuring the device or the network during this time. You cannot configure a device during an upgrade. Use the **show configuration session summary** command to verify that you have no active configuration sessions.
- Save, commit, or discard any active configuration sessions before upgrading or downgrading the Cisco NX-OS software image on your device.

  On a device with dual supervisors, the active supervisor module cannot switch over to the standby supervisor module during the Cisco NX-OS software upgrade if you have an active configuration session.
- Ensure that the device has a route to the remote server. The device and the remote server must be in the same subnetwork if you do not have a router to route traffic between subnets. To verify connectivity to the remote server, use the **ping** command.

```
switch# ping 172.18.217.1 vrf management
PING 172.18.217.1 (172.18.217.1): 56 data bytes
64 bytes from 172.18.217.1: icmp_seq=0 ttl=239 time=106.647 ms
64 bytes from 172.18.217.1: icmp_seq=1 ttl=239 time=76.807 ms
64 bytes from 172.18.217.1: icmp_seq=2 ttl=239 time=76.593 ms
64 bytes from 172.18.217.1: icmp_seq=3 ttl=239 time=81.679 ms
64 bytes from 172.18.217.1: icmp_seq=4 ttl=239 time=76.5 ms

--- 172.18.217.1 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 76.5/83.645/106.647 ms
```

For more information on configuration sessions, see the *Cisco Nexus 3000 Series NX-OS System Management Configuration Guide*.

Upgrading the Cisco NX-OS Software

Use this procedure to upgrade to a Cisco NX-OS 10.5(x) release. Before upgrading, it is recommended to verify the source (Current Release) and destination (Target Release) version using the Cisco Nexus 9000 and 3000 ISSU Support Matrix available on Cisco.com.

Note To upgrade from Cisco NX-OS Release 9.2(1), you must set the boot variable, copy the running configuration to the startup configuration, and reload the device.

SUMMARY STEPS

1. **Read the release notes for the software image file for any exceptions to this upgrade procedure.** See the Cisco Nexus 3600 Series NX-OS Release Notes.
2. Log in to the device on the console port connection.
3. Ensure that the required space is available for the image file to be copied.
4. If you need more space on the supervisor module, delete unnecessary files to make space available.
5. Verify that there is space available on the active and the standby supervisor modules.
6. If you need more space on the supervisor module, delete any unnecessary files to make space available.
7. Log in to Cisco.com, choose the software image file for your device from the following URL, and download it to a file server: http://software.cisco.com/download/navigator.html.
8. Copy the software image to the active supervisor module using a transfer protocol. You can use FTP, TFTP, SCP, or SFTP.
9. Display the SHA256 checksum for the file to verify the operating system integrity and ensure that the downloaded image is safe to install and use.
10. Check the impact of upgrading the software before actually performing the upgrade.
11. Save the running configuration to the startup configuration.
12. Upgrade the Cisco NX-OS software using the **install all nxos bootflash:***filename* [**no-reload** | **no-save** | **non-interruptive** | **skip-epld** | **skip-bios-upgrade** | **skip-kernel-upgrade**] command.
13. (Optional) Display the entire upgrade process.
14. (Optional) Log in and verify that the device is running the required software version.
15. (Optional) If necessary, install any licenses to ensure that the required features are available on the device. See the Cisco NX-OS Licensing Guide.

DETAILED STEPS

Procedure

Step 1 **Read the release notes for the software image file for any exceptions to this upgrade procedure.** See the Cisco Nexus 3600 Series NX-OS Release Notes.

Step 2 Log in to the device on the console port connection.

Step 3 Ensure that the required space is available for the image file to be copied.

```
switch# dir bootflash:
```

Note
We recommend that you have the image file for at least one previous release of the Cisco NX-OS software on the device to use if the new image file does not load successfully.

Step 4 If you need more space on the supervisor module, delete unnecessary files to make space available.

```
switch# delete bootflash:nxos.10.5.3.F.bin
```

Step 5 Verify that there is space available on the active and the standby supervisor modules.

Step 6 If you need more space on the supervisor module, delete any unnecessary files to make space available.

Step 7 Log in to Cisco.com, choose the software image file for your device from the following URL, and download it to a file server: http://software.cisco.com/download/navigator.html.

Step 8 Copy the software image to the active supervisor module using a transfer protocol. You can use FTP, TFTP, SCP, or SFTP.

```
switch# copy scp://user@scpserver.cisco.com//download/nxos.10.1.1.bin bootflash:nxos.10.1.1.bin
```

For software images requiring compaction, you must use SCP, HTTP, or HTTPS as the source and bootflash or USB as the destination. The following example uses SCP and bootflash:

```
switch# copy scp://user@scpserver.cisco.com//download/nxos.10.1.1.bin
bootflash:nxos.10.1.1.bin compact vrf management use-kstack

user1@10.65.42.196's password:
nxos.10.1.1.bin 100% 1887MB 6.6MB/s 04:47
Copy complete, now saving to disk (please wait)...
Copy complete.
```

The **compact** keyword compacts the NX-OS image prior to copying the file to the supervisor module.

Note
Software image compaction is only supported on SCP, HTTP, or HTTPS. If you attempt compaction with any other protocol, the system returns the following error:

```
Compact option is allowed only with source as scp/http/https and destination
as bootflash or usb
```

Note
Compacted images are not supported with LXC boot mode.

Step 9 Display the SHA256 checksum for the file to verify the operating system integrity and ensure that the downloaded image is safe to install and use.

```
switch# show file bootflash://sup-1/nxos.10.5.3.F.bin sha256sum
5214d563b7985ddad67d52658af573d6c64e5a9792b35c458f5296f954bc53be
```

Step 10 Check the impact of upgrading the software before actually performing the upgrade.

```
switch# show install all impact nxos bootflash:nxos.10.5.3.F.bin
```

Step 11 Save the running configuration to the startup configuration.

```
switch# copy running-config startup-config
```

Step 12 Upgrade the Cisco NX-OS software using the **install all nxos bootflash:***filename* [**no-reload** | **no-save** | **non-interruptive** | **skip-epld** | **skip-bios-upgrade** | **skip-kernel-upgrade**] command.

```
switch# install all nxos bootflash:nxos.10.5.3.F.bin
```

The following options are available:

- **no-reload**—Exits the software upgrade process before the device is reloaded.

  Note
  When you use **install all** with **no-reload** option, the saved configuration cannot be used before you reload the device. Saving configuration in this state can result in incorrect startup configuration once you reload the device with new version of NX-OS and EPLD. Though the EPLD and BIOS are programmed but not upgraded, a switch reload is required for them to take effect.

- **no-save**—Does not save configuration. Manually save the configuration before starting the **install all** command.
- **non-interruptive**—Upgrades the software without any prompts. This option skips all error and sanity checks.
- **skip-epld**—Installs only nxos image, and not the epld image.
- **skip-bios-upgrade**—Installs only nxos image and skips the BIOS upgrade.
- **skip-kernel-upgrade**—Installs only nxos image and skips the kernel upgrade.

Note
- If you enter the **install all** command without specifying a filename, the command performs a compatibility check, notifies you of the modules that will be upgraded, and confirms that you want to continue with the installation. If you choose to proceed, it installs the NXOS software image that is currently running on the switch and upgrades the BIOS of various modules from the running image if required.
- During image upgrade, you can also apply SMUs so the SMU is installed with the new image using the**install all nxos** <*nxos image*> **package** <*smu package*> **non-interruptive** command.

```
switch# install all nxos nxos64-msll.10.5.3.F.bin.upg package
nxos64-msll.CSCeth_core-1.0.0-10.5.3.rpm non-interruptive
```

Step 13 (Optional) Display the entire upgrade process.

```
switch# show install all status
```

Step 14 (Optional) Log in and verify that the device is running the required software version.

```
switch# show version
```

Step 15 (Optional) If necessary, install any licenses to ensure that the required features are available on the device. See the Cisco NX-OS Licensing Guide.

Cisco NX-OS Software Downgrade Guidelines

Before attempting to downgrade to an earlier software release, follow these guidelines:

- On devices with dual supervisor modules, both supervisor modules must have connections on the console ports to maintain connectivity when switchovers occur during a software downgrade. See the Hardware Installation Guide for your specific chassis.

- Cisco NX-OS automatically installs and enables the guest shell by default. However, if the device is reloaded with a Cisco NX-OS image that does not provide guest shell support, the existing guest shell is automatically removed and a %VMAN-2-INVALID_PACKAGE message is issued. As a best practice, remove the guest shell with the **guestshell destroy** command before downgrading to an earlier Cisco NX-OS image.
- You must delete the switch profile (if configured) when downgrading from a Cisco NX-OS release that supports switch profiles to a release that does not. For more information, see the Cisco Nexus 3600 Series NX-OS System Management Configuration Guide.

Note Software downgrades are disruptive. In-service software downgrades (ISSDs), also known as nondisruptive downgrades, are not supported.

Prerequisites for Downgrading the Cisco NX-OS Software

Downgrading the Cisco NX-OS software has the following prerequisites:

- Before you downgrade from a Cisco NX-OS release that supports the Control Plane Policing (CoPP) feature to an earlier Cisco NX-OS release that does not support the CoPP feature, you should verify compatibility using the **show incompatibility nxos bootflash:***filename* command. If an incompatibility exists, disable any features that are incompatible with the downgrade image before downgrading the software.

Downgrading to an Earlier Software Release

Use this procedure to downgrade from the latest Cisco NX-OS Release 10.5(x) to an earlier supported release.

Note To downgrade to Cisco NX-OS Release 9.2(1), you must set the boot variable, copy the running configuration to the startup configuration, and reload the device.

SUMMARY STEPS

1. **Read the release notes for the software image file for any exceptions to this downgrade procedure.** See the Cisco Nexus 3600 NX-OS Release Notes.
2. Log in to the device on the console port connection.
3. Verify that the image file for the downgrade is present on the active supervisor module bootflash:.
4. If the software image file is not present, log in to Cisco.com, choose the software image file for your device from the following URL, and download it to a file server: http://software.cisco.com/download/navigator.html.
5. Copy the software image to the active supervisor module using a transfer protocol. You can use FTP, TFTP, SCP, or SFTP.
6. Check for any software incompatibilities.
7. Disable any features that are incompatible with the downgrade image.

8. Check for any hardware incompatibilities.
9. Power off any unsupported modules.
10. Save the running configuration to the startup configuration.
11. Downgrade the Cisco NX-OS software.
12. (Optional) Display the entire downgrade process.
13. (Optional) Log in and verify that the device is running the required software version.

DETAILED STEPS

Procedure

Step 1 **Read the release notes for the software image file for any exceptions to this downgrade procedure.** See the Cisco Nexus 3600 NX-OS Release Notes.

Step 2 Log in to the device on the console port connection.

Step 3 Verify that the image file for the downgrade is present on the active supervisor module bootflash:.

```
switch# dir bootflash:
```

Step 4 If the software image file is not present, log in to Cisco.com, choose the software image file for your device from the following URL, and download it to a file server: http://software.cisco.com/download/navigator.html.

Step 5 Copy the software image to the active supervisor module using a transfer protocol. You can use FTP, TFTP, SCP, or SFTP.

```
switch# copy scp://user@scpserver.cisco.com//download/nxos.9.2.3.bin bootflash:nxos.9.2.3.bin
```

Step 6 Check for any software incompatibilities.

```
switch# show incompatibility-all nxos bootflash:nxos.9.2.3.bin
Checking incompatible configuration(s)
No incompatible configurations
```

The resulting output displays any incompatibilities and remedies.

Step 7 Disable any features that are incompatible with the downgrade image.

Step 8 Check for any hardware incompatibilities.

```
switch# show install all impact nxos bootflash:nxos.9.2.3.bin
```

Step 9 Power off any unsupported modules.

```
switch# poweroff module module-number
```

Step 10 Save the running configuration to the startup configuration.

```
switch# copy running-config startup-config
```

Step 11 Downgrade the Cisco NX-OS software.

```
switch# install all nxos bootflash:nxos.9.2.3.bin
switch# install all nxos nxos.9.2.3.bin.CCO
```

```
Installer will perform compatibility check first. Please wait.
Installer is forced disruptive

Verifying image bootflash:/nxos.9.2.3.bin.CCO for boot variable "nxos".
[####################] 100% -- SUCCESS

Verifying image type.
[####################] 100% -- SUCCESS

Preparing "nxos" version info using image bootflash:/nxos.9.2.3.bin.CCO.
[####################] 100% -- SUCCESS

Preparing "bios" version info using image bootflash:/nxos.9.2.3.bin.CCO.
[####################] 100% -- SUCCESS

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

Notifying services about system upgrade.
2019 Jun 06 09:59:20 Switch %$ VDC-1 %$ %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configured from vty by admin
 on vsh.bin.30370
[####################] 100% -- SUCCESS



Compatibility check is done:
Module bootable Impact Install-type Reason
------ -------- -------------- ------------ ------
1 yes disruptive reset Incompatible image for ISSU



Images will be upgraded according to following table:
Module Image Running-Version(pri:alt) New-Version Upg-Required
------ ---------- ---------------------------------------- -------------------- ------------
1 nxos 9.3(1) 9.2(3) yes
1 bios v01.11(06/06/2019):v01.11(06/06/2019) v01.10(03/15/2019) no

Switch will be reloaded for disruptive upgrade.
Do you want to continue with the installation (y/n)? [n]
```

Note
If you enter the **install all** command without specifying a filename, the command performs a compatibility check, notifies you of the modules that will be upgraded, and confirms that you want to continue with the installation. If you choose to proceed, it installs the NXOS software image that is currently running on the switch and upgrades the BIOS of various modules from the running image if required.

Step 12 (Optional) Display the entire downgrade process.

Example:

```
switch# show install all status
```

Step 13 (Optional) Log in and verify that the device is running the required software version.

```
switch# show version
```

NX-OS Upgrade History

During the life of a Cisco Nexus 3600 switch, many upgrade procedures can be performed. Upgrades can occur for maintenance purposes or to update the operating system to obtain new features. Over time, switches may be updated on numerous occasions. Viewing the types of upgrades and when they occurred can help in troubleshooting issues or simply understanding the history of the switch.

Cisco Nexus 3600 switches log all upgrade activity performed over time providing a comprehensive history of these events. The stored upgrade history types are:

- Cisco NX-OS System Upgrades
- Electronic Programmable Logic Device (EPLD) Upgrades
- Software Maintenance Upgrade (SMU) Installations

View the Cisco NX-OS upgrade history by entering the **show upgrade history** command. The output displays any upgrade activity that previously occurred on the switch and defines the start and end times for each event. The following is an example output of the **show upgrade history** command:

```
switch# show upgrade history
     TYPE          VERSION                    DATE                STATUS
NXOS system image  10.5(3)              13 Mar 2025 05:21:46     Installation End
NXOS system image  10.5(3)              13 Mar 2025 05:18:28     Installation started
switch#
```

View the Cisco NX-OS upgrade history details by entering the **show upgrade history details** command. The output displays user login details (user name/session ID) under LOGIN column on the switch along with upgrade history. The following is an example output of the **show upgrade history details** command:

```
switch# show upgrade history details
     TYPE          VERSION                       DATE                   LOGIN
           STATUS
NXOS system image  10.5(3)                   13 Mar 2025 05:21:46     admin/console0
       Installation End
NXOS system image  10.5(3)                   13 Mar 2025 05:18:28     admin/console0
       Installation started
switch#
```