



# Upgrade or Downgrade the Nexus 9000 Series NX-OS Software

---

- [Software image, on page 1](#)
- [Upgrade paths, on page 3](#)
- [NX-OS software upgrade, on page 3](#)
- [Prerequisites for NX-OS software upgrade, on page 6](#)
- [NX-OS software upgrade guidelines, on page 7](#)
- [ISSU platform support, on page 13](#)
- [Upgrade the NX-OS software, on page 18](#)
- [In-Service Software Upgrade, on page 22](#)
- [NX-OS upgrade history, on page 24](#)
- [Examples of upgrade types, on page 25](#)
- [Prerequisites for NX-OS software downgrade, on page 51](#)
- [NX-OS software downgrade guidelines, on page 51](#)
- [Downgrade to an earlier software release, on page 54](#)

## Software image

The NX-OS software image is an image that

- consolidates the necessary system components into one image,
- includes a bundled EPLD image beginning with Release 10.5(3)F, and
- uses a 64-bit format.

Each Nexus switch is shipped with the NX-OS software preinstalled. The NX-OS software consists of one NX-OS software image, and this image is required to load the NX-OS operating system.



---

**Note** Beginning with Release 10.5(3)F, NX-OS no longer provides a separate EPLD image. The EPLD image is bundled with all NX-OS images, increasing image sizes. For more information, refer to [Cisco Nexus 9000 Series FPGA/EPLD Upgrade Release Notes](#).

---

NX-OS Release 10.6(x) supports only 64-bit images, which are listed in this table.

Table 1: Software image

Image prefix	Example	Remarks
nxos64-cs	nxos64-cs.10.5.3.F.bin	Supported on all Nexus 9000 series switches except Nexus 9500 -R and -R2 switches and line cards, Nexus 9800 switches, and N9364E-SG2 switches
nxos64-ms11	nxos64-ms11.10.5.3.F.bin	Supported only on Nexus 9500 Series -R and -R2 modular switches
nxos64-s1	nxos64-s1.10.5.3.bin	Mandatory on Nexus 9800 and N9364E-SG2 switches. This image is supported from NX-OS Release 10.5(1)F on Nexus 9800 switches and from 10.5(3)F on N9364E-SG2 switches.
nxos64-s1-dpu	nxos64-s1-dpu.10.6.2.F.bin	Mandatory on N9324C-SE1U and N9348Y2C6D-SE1U Smart switches. This image is supported from NX-OS Release 10.6(2)F. Currently, these switches work in networking mode only.  <b>Note</b> <ul style="list-style-type: none"> <li>• Only disruptive upgrade is supported on the Smart switches.</li> <li>• Service-acceleration feature is not supported in 10.6(2)F.</li> </ul>
nxos64-msx	nxos64-msx.10.6.2n.F.bin	Mandatory on N9164E-NS4-O switch from NX-OS Release 10.6(2n). Currently, only disruptive upgrade is supported.

The Nexus 9000 Series switches support disruptive software upgrades and downgrades by default.

For information about the supported upgrade paths, see the [CiscoNexus 9000 and 3000 Upgrade and ISSU Matrix](#).

**Note**

- Until NX-OS Release 10.5(2)F, we provided separate electronic programmable logic device (EPLD) image upgrades to enhance hardware functionality or to resolve known hardware issues. For more information on the EPLD image and the upgrade process, see the [Cisco Nexus 9000 Series FPGA/EPLD Upgrade Release Notes](#).
- Until NX-OS Release 10.5(2)F, ISSU supports EPLD 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, first upgrade to 10.5(3) NX-OS using the **install all**<nxos-image> command. Then, after the NX-OS upgrade is complete, upgrade EPLD using the **install epld** command.
- Beginning with NX-OS Release 10.5(3)F, EPLD upgrade takes place during an ISSU system upgrade. 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.

**SMU image**

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 and generally include the ID number of the resolved defect in the filename (for example, n9000-dk10.1.1.CSCab00001.gbin). For more information on SMUs, see the Cisco Nexus 9000 Series NX-OS System Management Configuration Guide.

## Upgrade paths

For a list of specific releases from which you can perform a disruptive upgrade or a non-disruptive ISSU, see the [Cisco Nexus 9000 Series NX-OS Release Notes](#) for your particular release.

For ISSU compatibility for all releases and information about the upgrade paths, see the [Cisco Nexus 9000 and 3000 Upgrade and ISSU Matrix](#).

In general, ISSU is supported from

- a major release to any associated maintenance release
- the last two maintenance releases to the next two major releases, and
- an earlier maintenance release to the next two major releases.

## NX-OS software upgrade

A software upgrade on a switch involves updating the operating system (OS) or firmware running on the switch and is performed to provide:

- Security patching: Addressing known vulnerabilities to protect the network from potential exploits.
- Bug fixes: Resolving software-related issues that may cause instability or unexpected behavior.

- Feature enhancement: Enabling new software-defined networking (SDN) capabilities, improved management protocols, or better traffic optimization features.

Upgrading a Nexus switch running NX-OS is a critical operation that requires careful planning to ensure network stability. The process typically involves, downloading the [software image](#), verifying the compatibility between the current version and the target version, checking for hardware requirements, and utilizing the `install all command`, which automates the upgrade process and performs compatibility checks.

The two types of NX-OS software upgrade are:

- Disruptive upgrade
- Non-disruptive In-Service Software Upgrade (ND ISSU)

### Disruptive upgrade

A disruptive upgrade is the default upgrade process that requires a reload or cold reboot of the Nexus device and any connected Fabric Extenders (FEX). This reload disrupts both the control plane and the data plane, causing downtime and traffic interruption.

Disruptive upgrades are necessary when non-disruptive upgrade prerequisites are not met, or when upgrading between incompatible images, which may result in configuration loss, for example, unified ports, breakout, and FEX configurations.

Disruptive upgrade is supported on all NX-OS platforms but causes downtime during the upgrade. For example, in Nexus 9000 Series with single supervisors, disruptive upgrade causes the supervisor CPU to reset and reload the new software, disrupting control plane and data plane during the process.

The reload causes disruptions to connected servers and hosts, but in vPC deployments, traffic is minimized by routing through the peer switch during upgrade.

Use the **`install all nxos bootflash:<filename>`** command for disruptive upgrade.

Example

```
install all nxos bootflash:nxos64-cs.10.6.2.F.bin
```

For a sample display for disruptive upgrade, refer to the Disruptive ISSU for [CloudScale TOR](#) and [Silicon One EOR](#) sections.

### Non-disruptive In-Service Software Upgrade

Non-disruptive In-Service Software Upgrade (ND ISSU) allows upgrading the device software while the switch continues to forward traffic, minimizing or eliminating downtime.

Non-disruptive ISSU requires meeting specific prerequisites, such as compatible software releases, supported hardware platforms, and ISSU-ready topology and features. Few features and configurations are not supported during non-disruptive ISSU, and certain platforms or configurations only support disruptive ISSU.

Non-disruptive ISSU requires careful configuration, such as setting appropriate BGP graceful restart timers and avoiding configuration changes during the upgrade.

Non-disruptive ISSU is further classified as:

- Non-Disruptive ISSU for Cloud Scale switches
  - Enhanced ISSU (default)

Enhanced ISSU uses Linux containers (LXC) to run virtual instances of supervisor modules and line cards, enabling the upgrade with minimal impact. With Enhanced ISSU, the software runs inside a separate Linux container for the supervisor and line card. On the TOR, two additional containers are created and brought up as the standby supervisor and standby line card respectively.

The virtual instances or linux containers communicate with each other using an emulated Ethernet connection. In the normal state, only two Linux containers are instantiated: vSup1, a virtual SUP container in an active role, and vLC, a virtual linecard container.

Use the **install all nxos bootflash:<filename> non-disruptive** command for disruptive upgrade.

Example:

```
install all nxos bootflash:nxos64-cs.10.6.2.F.bin non-disruptive.
```



**Note** For switches in LXC boot mode, the enhanced LXC upgrade falls back to standard ND ISSU because the target image kernels are likely different from the current image. In standard ISSU, the CPU reset domain uses a kexec system call to boot into the new image after NX-OS components save their state. Kexec allows a new Linux kernel-based image to be loaded and booted from the currently running kernel.

For samples of display for Non-disruptive ISSU, refer to the [Non-Disruptive ISSU for Cloudscale TOR](#) section.

- Min-disruptive ISSU for Silicon One switches

- Standard ISSU only

Beginning with NX-OS Release 10.6(3)F, min-disruptive (MD) ISSU, or minimally disruptive ISSU, is introduced only on Nexus 9364E-SG2 Silicon One-based TORs. While performing MD ISSU, any minimal packet disruption is displayed to the user.

The drop-time information is also shown in the output of the `show install all min-disruptive drop-time` command.

```
switch# show install all min-disruptive drop-time
Estimated traffic outage time for current upgrade : about 65 ms
```

While performing a min-disruptive ISSU, increase the routing protocol graceful restart timer to a higher value. The recommended value for graceful restart timer is 240 seconds, although this value can be adjusted based on the configuration scale.

If network topology changes during MD ISSU cause few SUP apps not to proceed with the upgrade, then MD ISSU is aborted and the upgrade becomes disruptive. Furthermore, if any SUP app responds with failure, MD ISSU is aborted and the upgrade becomes disruptive.

The output of the **show install all status** command now shows min-disruptive.

Use the **install all nxos bootflash:<filename> min-disruptive** command for disruptive upgrade.

Example

```
install all nxos bootflash:nxos64-s1.10.6.2.F.bin min-disruptive.
```

For a sample of display for min-disruptive ISSU, refer to the [Min-Disruptive ISSU on Silicon One TOR](#) section.

## Prerequisites for NX-OS software upgrade

The prerequisites that you must meet before upgrading the NX-OS software are:

- Verify the recommended upgrade paths between releases are specified in the [Cisco Nexus 9000 and 3000 Upgrade and ISSU Matrix](#).
- Ensure that no user—who has access to the device or the network—is configuring the device or the network during the upgrade. You cannot configure a device during an upgrade. To verify that you have no active configuration sessions, use the **show configuration session summary** command.
- Save, commit, or discard any active configuration sessions before upgrading or downgrading the NX-OS software image on your device. While upgrading NX-OS software on a device with dual supervisors, the active supervisor module cannot switch over to the standby supervisor module if there is an active configuration session.
- To transfer NX-OS software images to the Nexus switch through a file transfer protocol such as TFTP, FTP, SFTP, and SCP, verify that the Nexus switch can connect to the remote file server where the NX-OS software images are stored. If you do not have a router to route traffic between sub nets, ensure that the Nexus switch and the remote file server are on the same sub network. To verify connectivity to the remote server, transfer a test file using a file transfer protocol of your choice or use the ping command if the remote file server is configured to respond to ICMP Echo Request packets. Here is an example of using the **ping** command to verify connectivity to a remote file server 192.0.2.100.

```
switch# ping 192.0.2.100 vrf management
PING 192.0.2.100 (192.0.2.100): 56 data bytes
64 bytes from 192.0.2.100: icmp_seq=0 ttl=239 time=106.647 ms
64 bytes from 192.0.2.100: icmp_seq=1 ttl=239 time=76.807 ms
64 bytes from 192.0.2.100: icmp_seq=2 ttl=239 time=76.593 ms
64 bytes from 192.0.2.100: icmp_seq=3 ttl=239 time=81.679 ms
64 bytes from 192.0.2.100: icmp_seq=4 ttl=239 time=76.5 ms

--- 192.0.2.100 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 non-disruptive ISSU in spanning tree topology, before running the **show spanning-tree issu-impact** command, the criteria that you must verify include
  - no topology change must be active in any STP instance
  - Bridge Assurance (BA) should not be active on any port (except MCT and vPC peer link)
  - there should be no Non-Edge Designated Forwarding port (except MCT and vPC peer link), and
  - ISSU criteria must be met on the vPC peer switch.

A pre-upgrade generic checklist includes:

- 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 consoleports to maintain connectivity when switchovers occur during a software upgrade. For more information about your specific chassis, refer to the relevant [Hardware Installation Guide](#).

- Perform the installation on the active supervisor module, not the standby supervisor module.



---

**Note** For more information about configuration sessions, refer to the [Cisco Nexus 9000 Series NX-OS System Management Configuration Guide](#) specific to your release.

---

## Nexus health and configuration checks

A Nexus health and configuration check is an automated diagnostic service that

- analyzes Nexus switch logs to identify issues and provides recommendations
- checks critical configurations such as virtual Port Channel (vPC), multicast, and Layer 3 uplinks, and
- ensures best practices and detects inconsistencies in complex environments.

We recommend performing a Nexus health and configuration check before performing an upgrade. The benefits include identification of potential issues, susceptible Field Notices, security vulnerabilities, and missing recommended configurations. For more information about the procedure, see [Perform Nexus Health and Configuration Check](#).

## NX-OS software upgrade guidelines

Before attempting to upgrade to any software image, follow the guidelines and limitations listed under these sub sections to ensure compatibility, minimize disruptions, and maintain operational stability.



---

**Note** For ISSU compatibility for all releases, see the [Cisco Nexus 9000 and 3000 Upgrade and ISSU Matrix](#).

---

- [Generic](#)
- [Software image and SMU](#)
- [EPLD](#)
- [Release specific](#)
- [Switch specific](#)
- [Disruptive and non-disruptive ISSU](#)
- [Feature specific](#)
- [Unsupported PIDs](#)

### Generic

The guidelines that apply to all upgrades irrespective of the releases are

- 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.
- During upgrade, while performing device reload, if ASCII replay is triggered without binary restore, primary key gets lost. The primary key must be reconfigured after device reload. Use the **key config-key ascii** command to reconfigure the primary key and avoid encryption issues. However, upgrade with binary restore retains the primary key after the reboot.
- ISSU is blocked if **boot poap enable** is configured.
- Make sure that both vPC peers are in the same mode (regular mode or enhanced mode) before performing a non-disruptive upgrade.




---

**Note** vPC peering between an enhanced ISSU mode (boot mode lxc) configured switch and a non-enhanced ISSU mode switch is not supported.

---

- During an ISSU, the software reload process on the first vPC device locks its vPC peer device by using CFS messaging over the vPC communications channel. Only one device at a time is upgraded. When the first device completes its upgrade, it unlocks its peer device. The second device then performs the upgrade process, locking the first device as it does so. During the upgrade, the two vPC devices temporarily run different releases of NX-OS; however, the system functions correctly because of its backward compatibility support.
- ISSU is not supported when onePK is enabled. You can run the **show feature | include onep** command to verify that this feature is disabled before performing an ISSU or enhanced ISSU.
- Occasionally, while the switch is operationally up and running, the Device not found logs are displayed on the console. This issue is observed because the switch attempts to find an older ASIC version and the error messages for the PCI probe failure are enabled in the code. There is no functionality impact or traffic loss due to this issue.
- For secure POAP, ensure that DHCP snooping is enabled and set firewall rules to block unintended or malicious DHCP servers. For more information on POAP, see the [Cisco Nexus 9000 Series Fundamentals Configuration Guide](#).
- When you upgrade from an earlier release to a 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 on configuration, see the [Cisco Nexus 9000 Series NX-OS System Management Configuration Guide](#).
- Guest Shell is disabled during an ISSU and reactivated after the upgrade. All applications running in the Guest Shell are affected.
- While performing an ISSU, VRRP and VRRPv3 display these messages:

- If VRRPv3 is enabled:

```
2015 Dec 29 20:41:44 MDP-N9K-6 %$ VDC-1 %$ %USER-0-SYSTEM_MSG: ISSU ERROR: Service
"vrrpv3" has sent the following message: Feature vrrpv3 is configured. User can
change
vrrpv3 timers to 120 seconds or fine tune these timers based on upgrade time on all
Vrrp
Peers to avoid Vrrp State transitions. - sysmgr
```

- If VRRP is enabled:

```

2015 Dec 29 20:45:10 MDP-N9K-6 %$ VDC-1 %$ %USER-0-SYSTEM_MSG: ISSU ERROR: Service
"vrrp-
eng" has sent the following message: Feature vrrp is configured. User can change
vrrp
timers to 120 seconds or fine tune these timers based on upgrade time on all Vrrp
Peers to
avoid Vrrp State transitions. - sysmgr

```

- An error occurs when you try to perform an ISSU if you changed the reserved VLAN without entering the copy running-config save-config and reload commands.

### Software image and SMU

- Beginning with NX-OS Release 10.6(2n), `-msx` image (for example, `nxos64-msx.10.6.2n.F.bin`) is introduced for N9164E-NS4-O switch. Currently, only disruptive upgrade to any future releases is supported on this switch.
- Beginning with NX-OS Release 10.5(1)F, `s1` image is introduced specifically for Nexus 9800 switches. Upgrade of Nexus 9800 switches from earlier releases that have `cs` image format to the `s1` image format in NX-OS Release 10.5(1)F and later is supported.
- Loading an unsupported image on Nexus 9800 platform switches cause the switch to be stuck. Only a power cycle can reset it.
- The **install all** command is the recommended method for software upgrades because it performs configuration compatibility checks and BIOS upgrades automatically. In contrast, changing the boot variables and reloading the device bypasses these checks and the BIOS upgrade and therefore is not recommended.
- You can detect an incomplete or corrupt NX-OS software image prior to performing an upgrade by verifying the MD5, SHA256 or SHA512 checksum of the software image. To verify the MD5 checksum of the software image, run the **show file bootflash:<IMAGE-NAME>md5sum** command and compare the resulting value to the published MD5 checksum for the software image on the *Software Download* website. To verify the SHA512 checksum of the software image, run the **show file bootflash:<IMAGE-NAME>sha512sum** command and compare the resulting value to the published SHA512 checksum for the software image on the *Software Download* website.
- The **install all** command is the recommended method for software upgrades because it performs configuration compatibility checks and BIOS upgrades automatically. In contrast, changing the boot variables and reloading the device bypasses these checks and the BIOS upgrade and therefore it is not recommended.

### EPLD

- From 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.
- From NX-OS Release 10.5(3)F, while installing nx-os using the **install all nx-os** command on switches affected by secure boot vulnerability, 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.

- ISSU supports EPLD image upgrades using **install all nxos** *<nxos-image>* **epld** *<epld-image>* command, during disruptive system (NX-OS) upgrade. Beginning with NX-OS Release 10.5(3)F, do not use the **epld** *<epld\_image>* option as the EPLD image is bundled with the NXOS images and a separate EPLD image is no longer provided.

### Release specific

- Upgrade from release 10.4(6)F to 10.5(1)F, 10.5(2)F, or 10.5(3)F releases is not supported and can result in configuration loss or its corruption. To upgrade from 10.4(6)M or 10.4(7)M release to 10.6(x) releases, the recommended path is to first upgrade to 10.5(4)M and then to 10.6(x). See [CSCwr21007](#) in the [Cisco Nexus 9000 Series NX-OS Release Notes, Release 10.4\(6\)M](#) and [Release 10.4\(7\)M](#).
- ISSU is blocked when the delay configuration is present in track list Boolean/weight.
- If the IPv6 ND timeouts during ISSU, then the IPv6 BFD session may flap after the ISSU.

### Switch specific

- During an ISSU on a Nexus 9300 Series switch, all First-Hop Redundancy Protocols (FHRPs) will cause the other peer to become active if the node undergoing the ISSU is active.
- Beginning with NX-OS Release 10.6(2)F, Nexus 9300-GX2, H2R, and H1 series switches support non-disruptive ISSU on switches that have MACsec-enabled interfaces.
- While performing non-disruptive ISSU from NX-OS Release 10.4(6)M to 10.6(1)F and later releases, on 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.
- Non-disruptive ISSU is not supported on interfaces with 2.5G or 5G speed on N9K-C93108TC-FX3P platform. For more information, refer to [CSCWq38959](#).
- ISSU with with FCoE (Fiber Channel over Ethernet)/FC (Fiber Channel) NPV (N-port Virtualization) is supported on some Nexus 9000 switches. An ISSU allows you to upgrade the device software while the switch continues to forward traffic. You can perform an in-service software upgrade (ISSU), also known as a nondisruptive upgrade, for some Nexus 9000 switches. The default upgrade process is disruptive. Using the nondisruptive option helps ensure a nondisruptive upgrade.

Fibre Channel N-port Virtualization (NPV) can co-exist with VXLAN on different fabric uplinks but on same or different front panel ports on the Nexus 93180YC-FX, N9K-C9336C-FX2-E, and N9k-C93360YC-FX2 switches.

### Disruptive and non-disruptive ISSU

- When upgrading Nexus 9300-FX2 switch from NX-OS Release 10.5(3)F to any later releases, only disruptive upgrade is supported, and ND ISSU is not supported when the system is enabled with routing template security group. However, ND ISSU is supported from NX-OS Release 10.6(1)F.

- While performing ND ISSU, if a router is configured with BGP prefix peers, prefix-peer-timeout (default value - 30s) should be greater than GR timer (default value - 120s), to allow the prefix peers to resume the connection after ISSU.
- The recommended routing protocol graceful restart timer is 240 seconds and nve source-interface hold-down-time is 400 seconds. For higher scale deployments adjust the graceful restart timer as required.
- It is recommended to set **disable-fka** on VFC interfaces in E or F mode, when invoking ND native ISSU on switch mode testbed. If not, it can be disruptive.
- Beginning from NX-OS Release 10.2(8)M onwards, Nexus 9300-FX3 supports non-disruptive upgrade.
- When performing ND ISSU using BGP non-default hold timers, ensure that the BGP graceful-restart timer is at least 180 seconds or higher.
- If there is a VRF scale, for a non-disruptive ISSU under each VRF, you must configure graceful restart timer to 300 seconds.
- OpenFlow and LACP fast timer rate configurations are not supported for Non-Disruptive ISSU.

### Feature specific

- From NX-OS Release 10.6(1)F, on Nexus modular switches, if the Backplane diagnostic test fails and a BACKPLANE\_AUTHENTICATION\_FAIL syslog appears, do not perform an upgrade or a system reload.
- While upgrading from an earlier release to 10.5(3)F or later releases, as a part of sFlow ISSU Consistency Checker, pre and post configuration files are created in the bootflash. To remove the snapshot files, use the **clear system internal sflow consistency pss-snapshot** command. However, if the snapshot files are removed, the **show system internal sflow consistency issu-pss** command does not provide the expected output. For more information, refer to [Cisco Nexus 9000 Series NX-OS System Management Configuration Guide](#).
- Enhanced ISSU is not supported with IPFM.

### Unsupported PIDs

The table displays the list of unsupported PIDs from various NX-OS Releases.

Unsupported PIDs	NX-OS Release
N9332C and N9364C	10.6(1)F
N9K-C92348GC-X	10.6(1)F
9700-EX line cards	10.6(1)F
<b>Note</b> N9K-X97160YC-EX line card is supported.	

## MACsec non-disruptive ISSU

Media Access Control Security (MACsec) non-disruptive ISSU is a feature that

- allows in-service software upgrades on switches with MACsec-enabled interfaces
- ensuring continued encryption and authentication of Ethernet traffic during the upgrade process, and
- is based on IEEE 802.1X-2014 REV of the MACsec Key Agreement (MKA) protocol. This protocol makes provision for MACsec-enabled switches to support ISSU by incorporating an additional parameter set.

MACsec is a Layer 2 security feature that provides encryption and authentication for traffic traversing Ethernet links. Nexus 9300-GX2, H2R, and H1 switches supports non-disruptive ISSU on switches that have MACsec-enabled interfaces.




---

**Note** Non-Disruptive ISSU is only supported on MACsec PSK-enabled interface.

---

To perform a non-disruptive ISSU on MACsec-enabled interfaces, the conditions that must be met include:

- The MACsec interfaces must use XPN cipher suites; otherwise, the upgrade is aborted.
- Both peers must run supported software versions with MKA version 2 or above. If any switch runs an older software version with MKA REV1, ISSU is aborted.




---

**Note** After completing ISSU, MACsec control plane transitions from the suspended to the secured state.

---

During the upgrade process, the MACsec interface can enter a new state called `suspended`. When an interface is in suspended state, it continues to encrypt outgoing data packets and decrypt incoming data packets on the interface. However, control packets may not be delivered sometimes when the interface control plane has a downtime. Due to this, a suspended interface does not support:

- Rekey results from policy timer expiry or packet number exhaustion. Packet number exhaustion-based rekey should not be triggered when using XPN cipher suites. XPN cipher suites provide a much wider window in which rekeying should occur.
- MACsec configuration changes after the interface enters a suspended state.




---

**Note** Any key expiry triggered after an interface moves to suspended state is handled only when the interface exits suspension and moves back to secured state.

---

Two new commands are introduced at the MACsec policy level to support this feature. For more information, refer to the *Configuring a MACsec policy* section in [Cisco Nexus 9000 Series NX-OS Security Configuration Guide](#).

### System messages for MACsec non-disruptive ISSU

A few system messages or logs are added to notify when an interface is suspended and when it exits suspension.

- `switch %CTS-5-CTS_SUSPENSION_START: MACsec control plane operation suspended for interface: Ethernet1/18`  
- This system log indicates that an interface has moved to suspended state.

- switch %CTS-5-CTS\_SUSPENSION\_REQUESTED: Requesting suspension of MACsec control plane operation for interface: Ethernet1/18
  - This system log indicates that the peer interface has requested suspension to be started.
- switch %CTS-5-CTS\_SUSPENSION\_STOP: MACsec control plane operation resumed for interface: Ethernet1/18
  - This system log indicates that the suspension has ended and the interface is back to its original state.

## ISSU platform support

The tables in this section summarize which Nexus platforms support standard and enhanced ISSU, the software release when support was introduced, and any features not supported for non-disruptive upgrades.



---

**Note** Enhanced ISSU cannot be supported if there is kernel update in the target release without reloading the container. The system prompts the `Host kernel is not compatible with target image. Full ISSU will be performed and control plane will be impacted. message`. In effect, the system performs non-disruptive ISSU instead of enhanced ISSU.

---

## ISSU for Nexus 9300-FX platform switches

ISSU Type	Release and Supported Platforms	Features Not Supported with Non-disruptive ISSU
Standard	<p>NX-OS Release 9.3(1) and 9.3(2): None</p> <p>Beginning with NX-OS Release 9.3(3):</p> <ul style="list-style-type: none"> <li>• Nexus 9336C-FX2</li> <li>• Nexus 93240YC-FX2</li> <li>• Nexus 93240YC-FX2Z</li> <li>• Nexus 9348GC-FXP</li> <li>• Nexus 93108TC-FX</li> <li>• Nexus 93180YC-FX</li> </ul> <p>Beginning with NX-OS Release 10.2(8)M:</p> <ul style="list-style-type: none"> <li>• Nexus 93180YC-FX3</li> <li>• Nexus 93180YC-FX3S</li> </ul> <p>Beginning with NX-OS Release 10.3(1)F:</p> <ul style="list-style-type: none"> <li>• Nexus 93180YC-FX3H</li> </ul> <p>Beginning with NX-OS Release 10.4(1)F:</p> <ul style="list-style-type: none"> <li>• 9348GC-FX3</li> <li>• 9348GC-FX3PH</li> </ul> <p>Beginning with NX-OS Release 10.4(2)F:</p> <ul style="list-style-type: none"> <li>• 93108TC-FX3</li> </ul>	<p>Standard ISSU is disruptive for Nexus 9300-FX platform switches configured with features such as</p> <ul style="list-style-type: none"> <li>• Segment Routing</li> <li>• TRM Feature, and</li> <li>• MACsec</li> </ul> <p><b>Note</b> Beginning with NX-OS Release 10.2(1), Standard ISSU is non-disruptive for Nexus 9300-FX platform switches configured with Straight-Through FEX and Dual-Homed FEX.</p> <p>Beginning with NX-OS Release 10.3(3)F, standard ISSU is not supported on Nexus 93180YC-FX3 and FX3S platform switches.</p> <p>Beginning with NX-OS Release 10.4(1)F, standard ISSU is not supported on Nexus 9300-FX and 9300-FX2 platform switches.</p> <p><b>Note</b> Beginning with NX-OS Release 10.4(2)F, non-disruptive ISSU is supported for segment routing traffic engineering (SR-TE) features with BGP as underlay only on Nexus 9300 platform switches. For more information about the features that are not supported, see <a href="#">NX-OS software upgrade guidelines, on page 7</a></p>

ISSU Type	Release and Supported Platforms	Features Not Supported with Non-disruptive ISSU
Enhanced	<p>NX-OS Release 9.3(1), 9.3(2), and 9.3(3): None</p> <p>Beginning with NX-OS Release 9.3(5):</p> <ul style="list-style-type: none"> <li>• Nexus 9336C-FX2</li> <li>• Nexus 93240YC-FX2</li> <li>• Nexus 93216TC-FX2</li> <li>• Nexus 93360YC-FX2</li> <li>• Nexus 93240YC-FX2Z</li> <li>• Nexus 9348GC-FXP</li> <li>• Nexus 93108TC-FX</li> <li>• Nexus 93180YC-FX</li> </ul> <p>Beginning with NX-OS Release 10.1(1), Enhanced ISSU is supported on the following platforms with FC/FCoE features:</p> <ul style="list-style-type: none"> <li>• Nexus 93360YC-FX2</li> <li>• Nexus 93180YC-FX</li> </ul> <p>Beginning with NX-OS Release 10.2(8)M, Enhanced ISSU is supported on the following platforms:</p> <ul style="list-style-type: none"> <li>• Nexus 93180YC-FX3</li> <li>• Nexus 93180YC-FX3S</li> </ul> <p>Beginning with NX-OS Release 10.3(1)F:</p> <ul style="list-style-type: none"> <li>• Nexus 93180YC-FX3H</li> </ul> <p>Beginning with NX-OS Release 10.4(1)F:</p> <ul style="list-style-type: none"> <li>• 9348GC-FX3</li> <li>• 9348GC-FX3PH</li> </ul> <p>Beginning with NX-OS Release 10.4(2)F:</p> <ul style="list-style-type: none"> <li>• 93108TC-FX3</li> </ul> <p>Beginning with NX-OS Release 10.2(2)F, Enhanced ISSU is supported on the following platform with FC/FCoE features:</p> <ul style="list-style-type: none"> <li>• N9K-C9336C-FX2-E</li> </ul>	

ISSU Type	Release and Supported Platforms	Features Not Supported with Non-disruptive ISSU
		<p>Enhanced ISSU is disruptive for Nexus 9300-FX platform switches configured with features such as</p> <ul style="list-style-type: none"> <li>• Segment Routing</li> <li>• TRM Feature, and</li> <li>• MACsec</li> </ul> <p><b>Note</b> In NX-OS Release 9.3(x), Enhanced ISSU on Nexus 93360YC-FX2 and Nexus 93180YC-FX with FC/FCoE features will be disruptive.</p> <p><b>Note</b> Beginning with NX-OS Release 10.2(1), Enhanced ISSU is non-disruptive for Nexus 9300-FX platform switches configured with Straight-Through FEX and Dual-Homed FEX.</p> <p>Beginning with NX-OS Release 10.3(3)F, only the LXC mode is supported on Nexus 9300-FX3 and 9300-FX3S switches, which allows you to perform enhanced non-disruptive ISSU with minimal downtime.</p> <p>Beginning with NX-OS Release 10.4(1)F, only the LXC mode is supported on Nexus 9300-FX and 9300-FX2 switches, which allows you to perform enhanced non-disruptive ISSU with minimal downtime.</p> <p><b>Note</b> Beginning with NX-OS Release 10.4(2)F, non-disruptive ISSU is supported for segment routing traffic engineering (SR-TE) features with BGP as underlay only on Nexus 9300 platform switches. For more information about the features that are not supported, see <a href="#">NX-OS software</a></p>

ISSU Type	Release and Supported Platforms	Features Not Supported with Non-disruptive ISSU
		<a href="#">upgrade guidelines, on page 7.</a>

## ISSU for Nexus 9300-GX platform switches

ISSU Type	Release and Supported Platforms	Features Not Supported with Non-disruptive ISSU
Standard	<p>Beginning with NX-OS Release 10.2(8)M:</p> <p>Nexus 9364C-GX</p> <p>Nexus 9316D-GX</p> <p>Nexus 93600CD-GX</p> <p><b>Note</b> Beginning with NX-OS Release 10.3(3)F, standard ISSU is not supported on Nexus 9300-GX platform switches.</p>	<ul style="list-style-type: none"> <li>• TRM Feature</li> <li>• Segment Routing</li> </ul> <p><b>Note</b> Beginning with NX-OS Release 10.3(3)F, standard ISSU is not supported on Nexus 9300-GX platform switches.</p> <p><b>Note</b> Beginning with NX-OS Release 10.4(2)F, non-disruptive ISSU is supported for segment routing traffic engineering (SR-TE) features with BGP as underlay only on Nexus 9300 platform switches. For more information about the features that are not supported, see <a href="#">NX-OS software upgrade guidelines, on page 7.</a></p>
Enhanced	<p>Beginning with NX-OS Release 10.2(8)M:</p> <p>Nexus 9364C-GX</p> <p>Nexus 9316D-GX</p> <p>Nexus 93600CD-GX</p> <p>Beginning with NX-OS Release 10.2(2)F, Enhanced ISSU is supported on Nexus 9300-GX2B platform switches.</p> <p>Beginning with NX-OS Release 10.2(3)F, Enhanced ISSU is supported on Nexus 9300-GX2A platform switches.</p> <p>Beginning with NX-OS Release 10.3(3)F, only the LXC mode is supported on Nexus 9300-GX switches, which allows you to perform enhanced non-disruptive ISSU with minimal downtime.</p>	<ul style="list-style-type: none"> <li>• TRM Feature</li> <li>• Segment Routing</li> </ul> <p><b>Note</b> Beginning with NX-OS Release 10.4(2)F, non-disruptive ISSU is supported for segment routing traffic engineering (SR-TE) features with BGP as underlay only on Nexus 9300 platform switches. For more information about the features that are not supported, see <a href="#">NX-OS software upgrade guidelines, on page 7.</a></p>

## ISSU for Nexus 9300-HX platform switches

ISSU Type	Release and Supported Platforms	Features Not Supported with Non-disruptive ISSU
Enhanced	<p>Boot mode LXC ISSU is supported by default on the following Nexus C9300-HX platform switches:</p> <ul style="list-style-type: none"> <li>• N9K-C9332D-H2R - Beginning with NX-OS Release 10.4(1)F</li> <li>• N9K-C93400LD-H1 - Beginning with NX-OS Release 10.4(2)F</li> <li>• N9K-C9364C-H1 - Beginning with NX-OS Release 10.4(3)F</li> </ul> <p><b>Note</b> ND-ISSU from any 10.4(x) or 10.5(x) releases to 10.5(3)F release is not supported on N9K-C9364C-H1.</p>	<ul style="list-style-type: none"> <li>• SR L2EVPN</li> <li>• ISIS and OSPF underlay</li> <li>• vPC configuration with segment-routing</li> <li>• Egress Peer engineering</li> <li>• Segment routing and GRE co-existence</li> <li>• MACsec</li> </ul>

## ISSU for Nexus 9300-SG2 platform switches

ISSU Type	Release and Supported Platforms	Features Not Supported with Non-disruptive ISSU
Min-disruptive	Beginning with NX-OS Release 10.6(3)F, Min-disruptive Standard ISSU is supported on Nexus 9364E-SG2-O and 9364E-SG2-Q platform switches.	<ul style="list-style-type: none"> <li>• TRM Feature</li> <li>• Segment Routing</li> <li>• MACsec</li> </ul>

## ISSU for Cisco Nexus 9400 platform switches

ISSU Type	Release and Supported Platforms	Features Not Supported with Non-disruptive ISSU
Enhanced	Beginning with NX-OS Release 10.4(1)F, Enhanced ISSU is supported on Nexus C9408 platform switch.	<ul style="list-style-type: none"> <li>• TRM Feature</li> <li>• Segment Routing</li> <li>• MACsec</li> </ul>

## Upgrade the NX-OS software

Use this procedure to upgrade to the latest NX-OS 10.6(x) release.

**Note**

- By default, the software upgrade process is disruptive.
- If an error message appears during the upgrade, the upgrade fails because of the reason indicated. For more information about possible causes and solutions, see the [Cisco Nexus 9000 Series NX-OS Troubleshooting Guide](#).

**Before you begin**

- Read the release notes for the software image file for any exceptions to this upgrade procedure. For more information about software image file, see the [Cisco Nexus 9000 Series NX-OS Release Notes](#).

**Procedure**

**Step 1** Log in to the device on the console port connection.

**Step 2** Ensure that the required space is available for the image file to be copied.

```
switch# dir bootflash:
16384   Oct 30 17:05:32 2020  lost+found/
1964291584   Dec 08 19:44:33 2020  nxos.10.1.1.bin
...
Usage for bootflash://sup-local
 4825743360 bytes used
16312102912 bytes free
21137846272 bytes total
```

**Note**

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

- a) If you need more space on the active supervisor module, delete unnecessary files to make space available.

```
switch# delete bootflash:nxos.9.2.1.bin
```

- b) Verify that there is space available on the standby supervisor module.

```
switch# dir bootflash://sup-standby/
16384   Oct 30 17:05:32 2020  lost+found/
1964291584   Dec 08 19:44:33 2020  nxos.10.1.1.bin
...
Usage for bootflash://sup-standby
4825743360 bytes used
16312102912 bytes free
21137846272 bytes total
```

- c) (Optional) If you need more space on the standby supervisor module, delete any unnecessary files to make space available.

```
switch# delete bootflash://sup-standby/nxos.9.2.1.bin
```

**Step 3** Log in and choose the software image file for your device from the [Software Download](#) website, and download it to a file server.

**Step 4** 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/nxos64.10.2.1.F.bin bootflash:nxos64.10.2.1.F.bin
```

**Note**

The compaction feature is deprecated from NX-OS Release 10.5(2)F

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

```
switch# copy scp://user@scpserver.cisco.com//download/nxos64.10.2.1.F.bin
bootflash:nxos64.10.2.1.F.bin compact vrf management use-kstack
```

```
user1@10.65.42.196's password:
nxos64.10.2.1.F.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 before 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.

**Note**

Software image compaction is only supported on Nexus 9300-series platform switches.

- a) You can detect an incomplete or corrupt NX-OS software image prior to performing an upgrade by verifying the MD5, SHA256 or SHA512 checksum of the software image. To verify the MD5 checksum of the software image, run the **show file bootflash:<IMAGE-NAME>md5sum** command and compare the resulting value to the published MD5 checksum for the software image on [Software Download](#) website. To verify the SHA512 checksum of the software image, run the **show file bootflash:<IMAGE-NAME>sha512sum** command and compare the resulting value to the published SHA512 checksum for the software image on [Cisco's Software Download](#) website.

```
switch# show file bootflash:nxos.10.1.1.1.bin md5sum
2242a7f876f1304118fd175c66f69b34

switch# show file bootflash:nxos.10.1.1.1.bin sha512sum
7f25cce57ca137a79211fb3835338aae64acf9b021b75cec5d4156e873b4274ca4f98e9a74fe4c8961
f5ace99ed65f3826650599369f84ab07265d7c5d61b57f
```

- b) You can detect an incomplete or corrupt NX-OS software image prior to performing an upgrade by verifying the MD5, SHA256 or SHA512 checksum of the software image. To verify the MD5 checksum of the software image, run the **show file bootflash:<IMAGE-NAME>md5sum** command and compare the resulting value to the published MD5 checksum for the software image on [Cisco's Software Download](#) website. To verify the SHA512 checksum of the software image, run the **show file bootflash:<IMAGE-NAME>sha512sum** command and compare the resulting value to the published SHA512 checksum for the software image on the [Software Download](#) website.

```
switch# show file bootflash:nxos64.10.2.1.F.bin md5sum
c49660952215822afd30bb7958a0765a

switch# show file bootflash:nxos64.10.2.1.F.bin sha256sum
2a64efbb381fabbb52054af74cf3efda1691772a49a70ddd35550431cadecf8e

switch# show file bootflash:nxos64.10.2.1.F.bin sha512sum
3bf6a771aa4a192a8e1383e348b26bb483356a9774d74ba39ecbf7718248483b3391942c8103de8104deea8fda212266e70bd736220cff34943bd8e359432975
```

**Step 5** Check the impact of upgrading the software before actually performing the upgrade.

```
switch# show install all impact nxos bootflash:nxos64.10.2.1.F.bin
```

During the compatibility check, the ISSU-related messages listed in this table can appear in the **Reason** field.

Reason Field Message	Description
Incompatible image for ISSU	The NX-OS image to which you are attempting to upgrade does not support ISSU.
Default upgrade is not hitless	By default, the software upgrade process is disruptive. You must configure the <b>non-disruptive</b> option to perform an ISSU.

**Step 6** Save the running configuration to the startup configuration.

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

**Step 7** Upgrade the NX-OS software using the **install all nxos bootflash:filename [no-reload | non-disruptive | non-interruptive | min-disruptive | serial | skip-epld | skip-bios-upgrade | skip-kernel-upgrade ]** command.

```
switch# install all nxos bootflash:nxos64.10.5.3.F.bin
```

**Note**

From NX-OS Release 10.5(3)F, EPLD upgrade can be performed with either the no-reload or the non-disruptive option.

The available options are:

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

**Note**

When you use **install all** with **no-reload** option, no additional configuration changes can be made before you reload the device. Saving configuration in this state can result in incorrect startup configuration once you reload the device with the new version of NX-OS (along with EPLD from 10.5(3)F). From Release 10.5(3)F onwards, though the EPLD and BIOS are programmed but not upgraded, a switch reload is required for them to take effect.

- **non-disruptive**—Performs an in-service software upgrade (ISSU) to prevent the disruption of data traffic. (By default, the software upgrade process is disruptive.) From Release 10.5(3)F onwards, though the EPLD and BIOS are programmed but not upgraded, a switch reload is required for them to take effect.

**Note**

This option is not available on the Nexus 9364E-SG2 switches.

- **min-disruptive**—Performs an in-service software upgrade (ISSU) with minimal disruption of data traffic. This option is only available on Nexus 9364E-SG2 switches.
- **non-interruptive**—Upgrades the software without any prompts. This option skips all error and sanity checks.
- **serial**—Upgrades the I/O modules in Nexus 9500 Series switches one at a time. (By default, the I/O modules are upgraded in parallel, which reduces the overall upgrade time. Specifically, the I/O modules are upgraded in parallel in this order: the first half of the line cards and fabric modules, the second half of the line cards and fabric modules, the first system controller, the second system controller.)
- **skip-epld**—Installs only the nxos image, and not the epld image. This option is available from 10.5(3)F.

- **skip-bios-upgrade**—Installs only the nxos image, and skips the BIOS upgrade. This option is available from 10.5(3)F.
- **skip-kernel-upgrade**—Installs only the nxos image, and skips the kernel upgrade. This option is available from 10.5(3)F.

**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 NX-OS software image that is currently running on the switch and upgrades the BIOS of various modules from the running image, if necessary.
- Starting from 10.5(3)F, during the 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-disruptive non-interruptive** command.

```
install all nxos nxos64-cs.10.5.3.F.bin.upg package nxos64-cs.CSCab123456
-1.0.0-10.5.3.lib32_64_n9000.rpm non-disruptive non-interruptive
```

**Step 8** (Optional) Post upgrade actions.

- a) Display the entire upgrade process.

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

- b) Log in and verify that the device is running the required software version.

```
switch# show version
```

- c) If necessary, install the relevant licenses to ensure that the required features are available on the device. For more information about the licenses, see the [Cisco NX-OS Licensing Options Guide](#) and [Cisco Nexus 9000 and 3000 Series NX-OS Smart Licensing Using Policy User Guide](#).

## In-Service Software Upgrade

An in-service software upgrade (ISSU) is an upgrade that

- allows you to upgrade the device software while the switch continues to forward traffic, reduces or eliminates the downtime typically caused by software upgrades, and is also known as non-disruptive upgrade.

You can perform an ISSU or non-disruptive upgrade for some switches. (See the [ISSU platform support](#) for a complete list of supported platforms.)

- The default upgrade process is disruptive. Therefore, ISSU needs to be enabled using the command-line interface (CLI), as described in the configuration section of this document.
- Using the non-disruptive option helps ensure a non-disruptive upgrade. The guest shell is disabled during the ISSU process and it is later reactivated after the upgrade.
- Enhanced ISSUs are supported for some Nexus 9000 Series switches.

## ISSU scenarios and platform support

The supported ISSU scenarios include

- performing standard ISSU on Top-of-Rack (ToR) switches with a single supervisor, and
- performing enhanced ISSU on Top-of-Rack (ToR) switches with a single supervisor

Details for each scenario are described below.

### Performing standard ISSU on Top-of-Rack (ToR) switches with a single Supervisor

The ToR Nexus 9300 platform switches are the NX-OS switches with single supervisors. Performing ISSU on the Nexus 9000 Series switches causes the supervisor CPU to reset and to load the new software version. After the CPU loads the updated version of the NX-OS software, the system restores the control plane to the previous known configuration and the runtime state and it gets in-sync with the data plane, thereby completing the ISSU process.

The data plane traffic is not disrupted during the ISSU process. In other words, the data plane forwards the packets while the control plane is being upgraded, any servers that are connected to the Nexus 9000 Series switches do not see any traffic disruption. The control plane downtime during the ISSU process is approximately less than 120 seconds.

### Performing enhanced ISSU on Top-of-Rack (ToR) switches with a single Supervisor



---

**Note** Enhanced ISSU is not supported if there are any underlying kernel differences. In effect, the system performs non-disruptive ISSU instead of enhanced ISSU. The system prompts the message: `Host kernel is not compatible with target image. Full ISSU will be performed and control plane will be impacted.`

---

The NX-OS software normally runs directly on the hardware. However, configuring enhanced or container-based ISSU on single supervisor ToRs is accomplished by creating virtual instances of the supervisor modules and the line cards. With enhanced ISSU, the software runs inside a separate Linux container (LXC) for the supervisors and the line cards. A third container is created as part of the ISSU procedure, and it is brought up as a standby supervisor.

The virtual instances (or the Linux containers) communicate with each other using an emulated Ethernet connection. In the normal state, only two Linux containers are instantiated: vSup1 (a virtual SUP container in an active role) and vLC (a virtual linecard container). Enhanced ISSU requires 16G memory on the switch.

During the software upgrade with enhanced ISSU, the supervisor control plane stays up with minimal switchover downtime disruption and the forwarding state of the network is maintained accurately during the upgrade. The supervisor is upgraded first and the line card is upgraded next.

The data plane traffic is not disrupted during the ISSU process. The control plane downtime is less than 6 seconds.



---

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

---

For information on ISSU and high availability, see the [Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide](#).

## NX-OS upgrade history

During the life of a Nexus 9000 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 can 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.

Nexus 9000 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, and
- Software Maintenance Upgrade (SMU) Installations

View the 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)      06 Mar 2025 03:08:17 Installation End
NXOS system image 10.5(3)      06 Mar 2025 03:01:41 Installation started
NXOS system image 10.5(3)      06 Mar 2025 02:16:25 Installation End
NXOS EPLD          epld.img      06 Mar 2025 02:11:43 EPLD Upgrade completed
NXOS EPLD          epld.img      06 Mar 2025 02:00:22 EPLD Upgrade started
NXOS system image 10.5(3)      06 Mar 2025 01:52:46 Installation started
NXOS system image 10.5(3)      06 Mar 2025 01:19:05 Installation End
NXOS EPLD          epld.img      06 Mar 2025 01:19:04 EPLD Upgrade completed
NXOS EPLD          epld.img      06 Mar 2025 01:07:42 EPLD Upgrade started
NXOS system image 10.5(3)      06 Mar 2025 01:00:48 Installation started
```

View the 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. Here is an sample output of the **show upgrade history details** command.

```
switch# show upgrade history details
      TYPE          VERSION          DATE          LOGIN
      STATUS
NXOS system image 10.5(3)      06 Mar 2025 03:08:17 username/10.1.1.25
Installation End
NXOS system image 10.5(3)      06 Mar 2025 03:01:41 username/10.1.1.25
Installation started
NXOS system image 10.5(3)      06 Mar 2025 02:16:25 username/10.1.1.25
Installation End
NXOS EPLD          epld.img      06 Mar 2025 02:11:43
EPLD Upgrade completed
NXOS EPLD          epld.img      06 Mar 2025 02:00:22
EPLD Upgrade started
NXOS system image 10.5(3)      06 Mar 2025 01:52:46 username/10.1.1.25
Installation started
NXOS system image 10.5(3)      06 Mar 2025 01:19:05 username/10.1.1.25
Installation End
NXOS EPLD          epld.img      06 Mar 2025 01:19:04
EPLD Upgrade completed
NXOS EPLD          epld.img      06 Mar 2025 01:07:42
EPLD Upgrade started
NXOS system image 10.5(3)      06 Mar 2025 01:00:48 username/10.1.1.25
Installation started
```

```

NXOS EPLD          n9000-epld.10.5.1.F.img 05 Mar 2025 23:29:18  username/10.1.1.25
EPLD Upgrade completed
NXOS EPLD          n9000-epld.10.5.1.F.img 05 Mar 2025 23:17:59  username/10.1.1.25
EPLD Upgrade started
NXOS EPLD          epld.img                    05 Mar 2025 22:55:11
EPLD Upgrade completed
NXOS EPLD          epld.img                    05 Mar 2025 22:37:36
EPLD Upgrade started

```

## Examples of upgrade types

This section provides you sample displays of various upgrade types:

- [Disruptive ISSU for Silicon One EOR](#)
- [Disruptive ISSU for CloudScale TOR](#)
- [Non-Disruptive ISSU CloudScale TOR](#)
- [Min-Disruptive ISSU Silicon One TOR](#)

For more information about various types of upgrade in NX-OS, refer to [NX-OS software upgrade, on page 3](#).

### Disruptive ISSU for Silicon One EOR

```

=====
switch# show module
Mod Ports      Module-Type      Model              Status
-----
1    36    36x400G QSFP56-DD Ethernet Module    N9K-X9836DM-A    ok
2    36    36x400G QSFP56-DD Ethernet Module    N9K-X9836DM-A    ok
3    36    36x400G QSFP56-DD Ethernet Module    N9K-X9836DM-A    ok
4    36    36x400G QSFP56-DD Ethernet Module    N9K-X9836DM-A    ok
5    36    36x400G QSFP56-DD Ethernet Module    N9K-X9836DM-A    ok
6    36    36x400G QSFP56-DD Ethernet Module    N9K-X9836DM-A    ok
7    36    36x400G QSFP56-DD Ethernet Module    N9K-X9836DM-A    ok
8    36    36x400G QSFP56-DD Ethernet Module    N9K-X9836DM-A    ok
27   0     Supervisor Module    N9K-C9800-SUP-B  active *
28   0     Supervisor Module    N9K-C9800-SUP-B  ha-standby

Mod  Sw              Hw   Slot
---  -
1    10.6(2)         1.0  LC1
2    10.6(2)         1.0  LC2
3    10.6(2)         1.0  LC3
4    10.6(2)         1.0  LC4
5    10.6(2)         1.0  LC5
6    10.6(2)         1.0  LC6
7    10.6(2)         1.0  LC7
8    10.6(2)         1.0  LC8

```

## Examples of upgrade types

```

27 10.6(2)                1.0  SUP1
28 10.6(2)                1.0  SUP2

```

```

Mod  MAC-Address(es)                Serial-Num
----  -
1    68-87-c6-94-25-b8 to 68-87-c6-94-26-df  FOC2542N39J
2    20-cf-ae-4b-7a-d0 to 20-cf-ae-4b-7b-f7  FOC2533N3VZ
3    14-a2-a0-5a-26-18 to 14-a2-a0-5a-27-3f  FOC2549NKWJ
4    d4-eb-68-9d-71-40 to d4-eb-68-9d-72-67  FOC2537NA00
5    20-cf-ae-e5-82-68 to 20-cf-ae-e5-83-8f  FOC2537N9V2
6    c4-4d-84-e0-ec-18 to c4-4d-84-e0-ed-3f  FOC2543P5D5
7    20-cf-ae-e5-98-60 to 20-cf-ae-e5-99-87  FOC2537N9W3
8    e8-d3-22-7f-69-c0 to e8-d3-22-7f-6a-e7  FOC2620NSU3
27   d4-7f-35-fd-55-00 to d4-7f-35-fd-55-07  FOC2826N2LW
28   d4-7f-35-fd-54-98 to d4-7f-35-fd-54-9f  FOC2826N2MF

```

```

Mod  Online Diag Status
----  -

```

```

1    Pass
2    Pass
3    Pass
4    Pass
5    Pass
6    Pass
7    Pass
8    Pass
27   Pass
28   Pass

```

```

LFM  Ports                Module-Type                Model                Status
----  -
19   0    8-slot Fabric Module        N9K-C9808-FM-A        ok
20   0    8-slot Fabric Module        N9K-C9808-FM-A        ok
21   0    8-slot Fabric Module        N9K-C9808-FM-A        ok
22   0    8-slot Fabric Module        N9K-C9808-FM-A        ok
23   0    8-slot Fabric Module        N9K-C9808-FM-A        ok
24   0    8-slot Fabric Module        N9K-C9808-FM-A        ok
25   0    8-slot Fabric Module        N9K-C9808-FM-A        ok
26   0    8-slot Fabric Module        N9K-C9808-FM-A        ok

```

```

Mod  Sw                Hw    Slot
----  -
19   NA                1.0  FM1
20   NA                1.0  FM2
21   NA                1.0  FM3
22   NA                1.0  FM4
23   NA                1.0  FM5
24   NA                1.0  FM6
25   NA                1.0  FM7
26   NA                1.0  FM8

```

```

LFM  MAC-Address(es)                Serial-Num
----  -
19   NA                FOC2535N6HZ
20   NA                FOC2540N0ZZ
21   NA                FOC2535N6GC

```

```

22  NA                               FOC2540N0WA
23  NA                               FOC2525NP5C
24  NA                               FOC2540N101
25  NA                               FOC2534N308
26  NA                               FOC2546N2GP

LFM Online Diag Status
--- -----
19  Pass
20  Pass
21  Pass
22  Pass
23  Pass
24  Pass
25  Pass
26  Pass

switch# install all nxos bootflash:nxos64-s1.10.6.2.IMG9.0.222.F.bin.tmp
Installer will perform compatibility check first. Please wait.
Installer is forced disruptive

Verifying image bootflash:/nxos64-s1.10.6.2.IMG9.0.222.F.bin.tmp for boot variable "nxos".
[#####] 100% -- SUCCESS

Verifying EPLD/FPGA image //bootflash/nxos64-s1.10.6.2.IMG9.0.222.F.bin.tmp.
[#####] 100% -- SUCCESS

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

Preparing "bios" version info using image bootflash:/nxos64-s1.10.6.2.IMG9.0.222.F.bin.tmp.
[#####] 100% -- SUCCESS

Preparing "nxos" version info using image bootflash:/nxos64-s1.10.6.2.IMG9.0.222.F.bin.tmp.
[#####] 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
2       yes              disruptive    reset         default upgrade is not hitless
3       yes              disruptive    reset         default upgrade is not hitless
4       yes              disruptive    reset         default upgrade is not hitless
5       yes              disruptive    reset         default upgrade is not hitless
6       yes              disruptive    reset         default upgrade is not hitless
7       yes              disruptive    reset         default upgrade is not hitless
8       yes              disruptive    reset         default upgrade is not hitless
27      yes              disruptive    reset         default upgrade is not hitless
28      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
-----

```

## Examples of upgrade types

1	lcn9k		10.6(2)	10.6(3)
yes				
1	bios	v01.05(12/03/2024):v01.00(03/09/2020)		v01.05(12/03/2024)
no				
2	lcn9k		10.6(2)	10.6(3)
yes				
2	bios	v01.05(12/03/2024):v01.02(03/26/2022)		v01.05(12/03/2024)
no				
3	lcn9k		10.6(2)	10.6(3)
yes				
3	bios	v01.05(12/03/2024):v01.00(03/09/2020)		v01.05(12/03/2024)
no				
4	lcn9k		10.6(2)	10.6(3)
yes				
4	bios	v01.05(12/03/2024):v00.01(03/09/2020)		v01.05(12/03/2024)
no				
5	lcn9k		10.6(2)	10.6(3)
yes				
5	bios	v01.05(12/03/2024):v00.01(03/09/2020)		v01.05(12/03/2024)
no				
6	lcn9k		10.6(2)	10.6(3)
yes				
6	bios	v01.05(12/03/2024):v01.00(03/09/2020)		v01.05(12/03/2024)
no				
7	lcn9k		10.6(2)	10.6(3)
yes				
7	bios	v01.05(12/03/2024):v01.00(03/09/2020)		v01.05(12/03/2024)
no				
8	lcn9k		10.6(2)	10.6(3)
yes				
8	bios	v01.05(12/03/2024):v01.00(03/09/2020)		v01.05(12/03/2024)
no				
27	nxos		10.6(2)	10.6(3)
yes				
27	bios	v01.02(03/18/2025):v01.01(03/18/2024)		v01.02(03/18/2025)
no				
28	nxos		10.6(2)	10.6(3)
yes				
28	bios	v01.02(03/18/2025):v01.01(03/18/2024)		v01.02(03/18/2025)
no				

FPGA microcode will be upgraded according to following table:

Module	Type	EPLD	Running-Version	Flashed-Version*	New-Version	Upg-Required
No	1	LC MI FPGA	0x10014	0x10014	0x10014	
No	1	LC IO FPGA	0x10033	0x10033	0x10033	
No	2	LC MI FPGA	0x10014	0x10014	0x10014	
No	2	LC IO FPGA	0x10033	0x10033	0x10033	
No	3	LC MI FPGA	0x10014	0x10014	0x10014	
No	3	LC IO FPGA	0x10033	0x10033	0x10033	
No	4	LC MI FPGA	0x10014	0x10014	0x10014	
No	4	LC IO FPGA	0x10033	0x10033	0x10033	
No	5	LC MI FPGA	0x10014	0x10014	0x10014	

No	5	LC	IO	FPGA	0x10033	0x10033	0x10033
No	6	LC	MI	FPGA	0x10014	0x10014	0x10014
No	6	LC	IO	FPGA	0x10033	0x10033	0x10033
No	7	LC	MI	FPGA	0x10014	0x10014	0x10014
No	7	LC	IO	FPGA	0x10033	0x10033	0x10033
No	8	LC	MI	FPGA	0x10014	0x10014	0x10014
No	8	LC	IO	FPGA	0x10033	0x10033	0x10033
No	19	FM	MI	FPGA	0x10006	0x10006	0x10006
No	20	FM	MI	FPGA	0x10006	0x10006	0x10006
No	21	FM	MI	FPGA	0x10006	0x10006	0x10006
No	22	FM	MI	FPGA	0x10006	0x10006	0x10006
No	23	FM	MI	FPGA	0x10006	0x10006	0x10006
No	24	FM	MI	FPGA	0x10006	0x10006	0x10006
No	25	FM	MI	FPGA	0x10006	0x10006	0x10006
No	26	FM	MI	FPGA	0x10006	0x10006	0x10006
No	27	SUP	MI	FPGA	0x10001	0x10001	0x10001
No	27	SUP	IO	FPGA	0x10010	0x10010	0x10010
No	28	SUP	MI	FPGA	0x10001	0x10001	0x10001
No	28	SUP	IO	FPGA	0x10010	0x10010	0x10010

\* If Running-Version and Flashed-Version are different it implies that the system has not yet been reloaded for the new version to take effect

Additional info for this installation:

-----

Service "sflow" in vdc 1: SFLOW feature is enabled. Upgrade will pause sFlow report for about 1 ~ 2 minutes.

Switch will be reloaded for disruptive upgrade.

Do you want to continue with the installation (y/n)? [n] y

Install is in progress, please wait.

[# ] 0%

Performing runtime checks.

Syncing image bootflash:/nxos64-s1.10.6.2.IMG9.0.222.F.bin.tmp to standby.

[# ] 0%

Syncing image bootflash:/nxos64-s1.10.6.2.IMG9.0.222.F.bin.tmp to standby.

[#####] 100% -- SUCCESS

Setting boot variables.

```

[#           ] 0%
Setting boot variables.
[#####] 100% -- SUCCESS

Performing configuration copy.
[#####] 100%
Performing configuration copy.
[#####] 100% -- SUCCESS

Module 1: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[#           ] 0%
Module 1: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[#####] 100% -- SUCCESS

Module 2: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[#           ] 0%
Module 2: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[#####] 100% -- SUCCESS

Module 3: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[#           ] 0%
Module 3: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[#####] 100% -- SUCCESS

Module 4: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[#           ] 0%
Module 4: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[#####] 100% -- SUCCESS

Module 5: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[#           ] 0%
Module 5: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[#####] 100% -- SUCCESS

Module 6: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[#           ] 0%
Module 6: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[#####] 100% -- SUCCESS

Module 7: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[#           ] 0%
Module 7: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[#####] 100% -- SUCCESS

Module 8: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[#           ] 0%
Module 8: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[#####] 100% -- SUCCESS

```

```
Module 19: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[#           ] 0%
Module 19: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[#####] 100% -- SUCCESS

Module 20: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[#           ] 0%
Module 20: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[#####] 100% -- SUCCESS

Module 21: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[#           ] 0%
Module 21: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[#####] 100% -- SUCCESS

Module 22: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[#           ] 0%
Module 22: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[#####] 100% -- SUCCESS

Module 23: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[#           ] 0%
Module 23: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[#####] 100% -- SUCCESS

Module 24: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[#           ] 0%
Module 24: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[#####] 100% -- SUCCESS

Module 25: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[#           ] 0%
Module 25: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[#####] 100% -- SUCCESS

Module 26: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[#           ] 0%
Module 26: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[#####] 100% -- SUCCESS

Module 27: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[#           ] 0%
Module 27: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[#####] 100% -- SUCCESS
```



```

Installing ata_piix module ... done.
Unsquashing rootfs ...
vm.min_free_kbytes = 368640
Enabling 8250 serial driver spurious INTs workaround
Installing isan procfs ... done.
is_lxc: is_titan_eor: is_stby: suffix: klm_fttrace: /isanboot/lib/modules/klm_fttrace.o
Installing fttrace in non-lxc mode done
Installing SSE module with card index 21262 ... done.
Creating SSE device node 240 ... done.
17.19: card_index: 21262, card_type: 132
Loading I2C driver ... done.
Installing CTRL driver for card_type 132 without NEED_GEM ... [ 21.184436] ENABLING TOP
LEVEL RP INTERRUPT
[ 21.190465] Got RP P2PM intr, Becoming Active !!
21.20: FPGA test device /dev/xr-fpga -c 237 0 created
done.
Loading IGB driver ...
Loading Intel igb driver for S1 platforms...21.44: \nInstalling klm_ins_ixgbe start

Installing klm_ins_ixgbe ... done.

Checking all filesystems.
Extracting rpms from image...
/
Installing SPROM driver ... 21262 IS_N9K done.
Installing pfmsvcs module ...done.
Installing nvram module ... done.
Installing if_index module with port mode 6 ... done.
Installing fcfwd
Installing RNI lcnd ... done.
Installing lcnd ... done.
\n S090setup-eth sup_start
Installing psdev ...
Installing veobc module ... done.
Error: ipv4: Address already assigned.
Clean up previous pcap files present in tmp directory
Checking SR card
Card Index is 21262
64.47: Inserting obfl & mtd spi driver ...
old data: 0 new data: 9f000000
old data: 0 new data: 0
old data: 0 new data: a0901406
[ 64.500854] Initializing panic NMI
[ 64.508912] fpga_setup_probe
64.54: Done..Inserting obfl & mtd spi driver ...
Making OBFL character devices
old data: 9f000000 new data: 9f000000
old data: 0 new data: 0
old data: a0901406 new data: a0901406
mounting plog for N9k!
64.58: mounting plog for N9k!
64.60: Done..mounting plog for N9k!
mounting recovery for N9k!
64.62: mounting recovery for N9k!
Mounting OBFL pstore for mtd
Inserting kernel_services module ... done.
Making kernel_services character devices
cgroups initialized
package cgroup-lite-1.15-r0.corei7_64 is already installed
package util-linux-unshare-2.39.3-r0.corei7_64 is already installed
kernel.core_pattern = |/bin/sparsecore.sh %p %h %P %E
minicoredumper disabled for this platform...
exit code: 1
COPY the image to ORIG_LC_FS_PATH

```

```

/isanboot/bin/images/s1_gibraltar_xc_sdk.bin
/isanboot/bin/images/s1hal_n9000.bin
tune2fs 1.47.0 (5-Feb-2023)
Setting reserved blocks percentage to 0% (0 blocks)
Persistent log store is mounted successfully
Starting rpcbind daemon...done.
creating NFS state directory: done
starting 8 nfsd kernel threads: done
starting mountd: done
starting statd: done
Saving image for img-sync ...
Installing kheaders module ... done.
Loading system software
Installing local RPMS
Patch Repository Setup completed successfully
/logflash/stats_ssd/.ssd_overall_data file exist !!
moving /logflash/stats_ssd/.ssd_overall_data to /logflash/stats_ssd/.ssd_lastboot_data
Starting crond: OK
chown: warning: '.' should be ':': 'root.root'
Stopping crond: OK
Creating /dev/mcelog
Starting mcelog daemon
Starting crond: OK
Remove pltfm_config from eltm.conf for SONE cards
Replacement complete. All system shutdown binaries now point to /sbin/rep_file.
INIT: Entering runlevel: 3
link S1 SDK libs for SUP
SDK Shell for Gibraltar
ASIC_GIBRALTAR is y
ASIC_IRON is
Moving Sone libs for gibraltar
Linking tctrl_usd for GROGU RP2
Moving tctrl_usd_dual_sup.conf to tctrl_usd.conf
..Done
Running S93thirdparty-script...
vlc_card_index 0
S26: sw_id 21262 vp 0
S26 C: sw_id 21262, Retaining libcrdcfgdata.so as is
CAUTION!!!!!!CAUTION!!!!/bootflash/platform.inf File PRESENT
packagegroup-nxos-optional-rpms_pkg_list
Starting lem_drv driver
Inserting klm_lfm IS_LEM_CARD=y
LEM card. Insert driver
0x25
FM DIVF = 0x25
[ 102.637118] Initializing delayed work
[ 102.646884] Finished INIT function for lfm
LEM card. Make device
Executing /isan/etc/rc.d/rc.isan-start/S45s1drv start
done
klm_sone installed successfully
Installing marvell
pcie_proxy module installing for Marvell
Adding Marvel switch to pci_proxy module
dma proxy module installed
Adding Zenith FPGA to pci_proxy module
Netbroker support IS present in the kernel.
done
Executing Prune clis.
Removing exusd cli files if it is not exbl_card in prune_clis
ethernet switching mode Tue Mar 24 09:32:53 PDT 2026
prepare span CLI
[ 117.286629] register_rdn_int : Sent First Heartbeat

```

```
User Access Verification
switch login:
```

### Disruptive ISSU for CloudScale TOR

```
=====

switch# show module
Mod Ports          Module-Type          Model
  Status
-----
1    50    48x400G QSFP-DD + 2x10G SFP+ Ethernet Module  N9K-C9348D-GX2A
ok
27   0    Virtual Supervisor Module                    N9K-C9348D-GX2A
active *
```

Mod	Sw	Hw	Slot
1	10.5(3)	0.2030	NA
27	10.5(3)	0.2030	VSUP

```

Mod  MAC-Address(es)          Serial-Num
---  -----
1    4c-5d-3c-41-af-ae to 4c-5d-3c-41-b0-7b  FDO25210LJX
27   4c-5d-3c-41-af-ae to 4c-5d-3c-41-b0-7b  FDO25210LJX

Mod  Online Diag Status
---  -----
1    Pass
27   Pass

* this terminal session
switch# install all nxos bootflash:nxos64-cs.10.6.1.F.bin
Installer will perform compatibility check first. Please wait.
Installer is forced disruptive

Verifying image bootflash:/nxos64-cs.10.6.1.F.bin for boot variable "nxos".
[#####] 100% -- SUCCESS

Verifying EPLD/FPGA image //bootflash/nxos64-cs.10.6.1.F.bin.
[#####] 100% -- SUCCESS

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

Preparing "nxos" version info using image bootflash:/nxos64-cs.10.6.1.F.bin.
[#####] 100% -- SUCCESS

Preparing "bios" version info using image bootflash:/nxos64-cs.10.6.1.F.bin.
[#####] 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
-----

```

## Examples of upgrade types

```

1       yes      disruptive      reset  default upgrade is not hitless
27      yes      disruptive      reset  default upgrade is not hitless

```

Images will be upgraded according to following table:

Module	Image	Running-Version(pri:alt)	New-Version
1	lcn9k	10.5(3)	10.6(1)
27	nxos	10.5(3)	10.6(1)
27	bios	v01.10(11/28/2024):v01.03(07/14/2021)	v01.10(11/28/2024)

FPGA microcode will be upgraded according to following table:

Module	Type	EPLD	Running-Version	New-Version	Upg-Required
27	SUP	MI FPGA	0x08	0x10	Yes
27	SUP	IO FPGA	0x15	0x16	Yes
27	SUP	MIFPGA2	0x05	0x07	Yes

EPLD Upgrade may result in multiple modules going offline.

Switch will be reloaded for disruptive upgrade.

Do you want to continue with the installation (y/n)? [n] y

Install is in progress, please wait.

Setting boot variables.

[#####] 100% -- SUCCESS

Performing configuration copy.

[#####] 100% -- SUCCESS

Module 1: Refreshing compact flash and upgrading bios/loader/bootrom.

Warning: please do not remove or power off the module at this time.

[#####] 100% -- SUCCESS

Module 27: Refreshing compact flash and upgrading bios/loader/bootrom.

Warning: please do not remove or power off the module at this time.

[#####] 100% -- SUCCESS

EPLD/FPGA upgrade can take upto 12 mins.

Performing EPLD/FPGA upgrade .

[# ] 0%

[#####] 100% -- SUCCESS

2026 Mar 24 10:56:55 switch %\$ VDC-1 %\$ %VMAN-2-ACTIVATION\_STATE: Successfully deactivated virtual service 'guestshell+'

Finishing the upgrade, switch will reboot in 10 seconds.

switch# \$

CISCO MODULE

BIOS Ver: 1.10

Switch G16

RC Revision: 02.09.00

Memory Information:



```

Set fan speed to 60%
Initializing fan controller...
check_bootmode: grub: Continue grub
Trying to read config file /boot/grub/menu.lst.local from (hd0,msdos1)
Trying to read config file /boot/grub/menu.lst.local from (hd1,gpt5)

Security Lock
Booting bootflash:/nxos64-cs.10.6.1.F.bin
Trying diskboot
  Filesystem type is ext2fs, partition type gpt.

Image Signature verification was Successful.

Boot Time: 3/24/2026 18:1:7

Security Lock
62+1 records in
62+1 records out
261570560 bytes (262 MB, 249 MiB) copied, 0.121876 s, 2.1 GB/s
mount: overlay mounted on /newroot/usr.
Installing klm_card_index
done
[ 3.953788] sd 6:0:0:0: [sdb] No Caching mode page found
[ 3.959738] sd 6:0:0:0: [sdb] Assuming drive cache: write through
Linking n9k flash devices
creating flash devices BOOT_DEV= sda
Replacing inittab for node - host
INIT: version 3.01 booting
Setting up sysV scripts for host node
Installing ata_piix module ... done.
Installing kheaders module ... done.
Unsquashing rootfs ...
is_lxc:1 is_titan_eor: is_stby: suffix: klm_ftrace: /isanboot/lib/modules/klm_ftrace.o
Installing ftrace in lxc 0 mode done

Checking all filesystems.cgroups initialized
Generating ssh keys...Done ssh keys
Starting OpenBSD Secure Shell server: sshd ... done sshd.
Checking rpmstore swap in host context.
tune2fs 1.46.5 (30-Dec-2021)
Setting reserved blocks percentage to 0% (0 blocks)
INIT: Entering runlevel: 3
cp: cannot stat '/orig_fs/xr_cpa.img': No such file or directory
grep: /bootflash/platform.inf: No such file or directory

mount: overlay mounted on /usr.
Linking n9k flash devices
creating flash devices BOOT_DEV= sda
Replacing inittab for node - vsup
INIT: version 3.01 booting
Unsquashing rootfs ...
vm.min_free_kbytes = 184320
No TOR virtual chassis
skip untra_klms
Enabling 8250 serial driver spurious INTs workaround
Installing isan procfs isan_proc_name=isan26... done.
Installing SSE module with card index 21211 and vslot ID 26 ... done.
Creating SSE device node 241 ... done.
cg controllers already mounted at /var/cgroup
is_lxc:1 is_titan_eor: is_stby:0 suffix: klm_ftrace: /isanboot/lib/modules/klm_ftrace.o
Inserting kernel_services module ... done.
Making kernel_services character devices

```

```

klm_fttrace already loaded. skip.
12.63: card_index: 21211, card_type: 129
Loading I2C driver ... done.
Installing CCTRL driver for card_type 129 in vslot ID 26 without NEED_GEM ... done.
Loading IGB driver ...
Checking all filesystems.
done.
Extracting rpms from image...
Installing SPROM driver ... 21211 IS_N9K done.
Installing pfmsvcs module ...done.
Installing nvram module ... done.
Installing if_index module with port mode 6 ... done.
Installing fcfwd
Installing RNI lcnd ... done
Running mode is N9K-ToR ...done
Installing LC netdev container_id=0 is_standby=0 ... done
Installing psdev module ... done.
Installing veobc module ... done.
Clean up previous pcap files present in tmp directory
Checking SR card
Card Index is 21211
SR Card detected.
Inserting eMMC module ...
Inserting OBFL module ... 23.93: eMMC Device found.
23.93: card has mmc
done.
23.94: Making OBFL character devices for mmc
grep: /bootflash/platform.inf: No such file or directory
23.98: SR_START (9635840), size 7
mounting plog for N9k!
23.99: mounting plog for N9k!
24.00: Done..mounting plog for N9k!
Mounting OBFL for eMMC
Attach blkcoops
24.49: Before mounting blkcoops
24.50: After mounting blkcoops
24.51: recreate_mmcfttrace_rr_device
/
Calling install_tor for TOR
copying common rpm to ftp
COPY the image to ORIG_LC_FS_PATH

tune2fs 1.46.5 (30-Dec-2021)
Setting reserved blocks percentage to 0% (0 blocks)
Adding system startup for /etc/init.d/cgroups-init.
Persistent log store is mounted successfully
Loading system software
kernel.core_pattern = |/bin/sparsecore.sh %p %h %P %E
Starting rpcbind daemon...done.
Generating ssh keys...creating NFS state directory: done
starting 8 nfsd kernel threads: done
starting mountd: done
starting statd: done
Saving image for img-sync ...
exit code: 1
Done ssh keys
Starting OpenBSD Secure Shell server: sshd ... done sshd.
Installing local RPMS
Patch Repository Setup completed successfully
/logflash/stats_ssd/.ssd_overall_data file exist !!
moving /logflash/stats_ssd/.ssd_overall_data to /logflash/stats_ssd/.ssd_lastboot_data
Starting crond: OK
Creating /dev/mcelog

```

```

Starting mcelog daemon
Stopping crond: OK
N9K CPA setup done
N9K TOR LC CPA setup done
Remove pltfm_config from eltm.conf for SONE cards
INIT: Entering runlevel: 3
Replacement complete. All system shutdown binaries now point to /sbin/rep_file.
Running S93thirdparty-script...
vlc_card_index 0
S26: sw_id 21211 vp 0
S26 B: sw_id 21211, Moving libcrdcfgdata_tah_tor.so to libcrdcfgdata.so
Starting crond: OK

Starting lem_drv driver
Netbroker support IS present in the kernel.
done
done
Disabling cisco netbroker hooks ... done
Skipping EMON in TOR ...
Executing Prune clis.
Removing exusd cli files if it is not exbl_card in prune_clis
ethernet switching mode Tue Mar 24 11:01:59 PDT 2026
prepare span CLI
2026 Mar 24 11:02:40 switch %$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 1 powered up (Serial
  number FDO25210LJX)

2026 Mar 24 11:02:42 switch %$ VDC-1 %$ %VDC_MGR-2-VDC_ONLINE: vdc 1 has come online

User Access Verification
switch login: 2026 Mar 24 11:05:14 switch %$ VDC-1 %$ %ASCII-CFG-2-CONFIG_REPLAY_STATUS:
Ascii Replay Started.
2026 Mar 24 11:05:22 switch %$ VDC-1 %$ %ASCII-CFG-2-CONFIG_REPLAY_STATUS: Ascii Replay
Done.
2026 Mar 24 11:05:23 switch %$ VDC-1 %$ %ASCII-CFG-2-CONF_CONTROL: System ready
2026 Mar 24 11:05:49 switch %$ VDC-1 %$ %VMAN-2-GUESTSHELL_ENABLED: The guest shell has
been enabled. The command 'guestshell' may be used to access it, 'guestshell destroy' to
remove it.

switch login:

```

### Non-Disruptive ISSU CloudScale TOR

```

=====
switch# show module
Mod Ports      Module-Type      Model              Status
-----
1    108  96x10/25/32G + 12x40/100G Ethernet/FC Module  N9K-C93360YC-FX2  ok
27    0    Virtual Supervisor Module      N9K-C93360YC-FX2  active *

Mod Sw          Hw  Slot
---
1    10.6(2)       1.0  NA
27   10.6(2)       1.0  VSUP

Mod MAC-Address(es)              Serial-Num
---
1    70-ea-1a-d1-69-fa to 70-ea-1a-d1-6a-a5  FDO23240P95
27   70-ea-1a-d1-69-fa to 70-ea-1a-d1-6a-a5  FDO23240P95

```

```
Mod  Online Diag Status
---  -----
1    Pass
27   Pass
```

```
switch# install all nxos bootflash:nxos64-cs.10.6.2.F.bin non-disruptive
Installer will perform compatibility check first. Please wait.
```

```
Verifying image bootflash:/nxos64-cs.10.6.2.F.bin for boot variable "nxos".
[#####] 100% -- SUCCESS
```

```
Verifying EPLD/FPGA image //bootflash/nxos64-cs.10.6.2.F.bin.
[#####] 100% -- SUCCESS
```

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

```
Preparing "nxos" version info using image bootflash:/nxos64-cs.10.6.2.F.bin.
[#####] 100% -- SUCCESS
```

```
Preparing "bios" version info using image bootflash:/nxos64-cs.10.6.2.F.bin.
[#####] 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	non-disruptive	rolling	
27	yes	non-disruptive	reset	

Images will be upgraded according to following table:

Module	Image	Running-Version(pri:alt)	New-Version
1	lcn9k	10.6(1)	10.6(2)
yes			
27	nxos	10.6(1)	10.6(2)
yes			
27	bios	v05.53(01/22/2025):v05.38(06/12/2019)	v05.53(01/22/2025)
no			

FPGA microcode will be upgraded according to following table:

Module	Type	EPLD	Running-Version	Flashed-Version*	New-Version	Upg-Required
27	SUP	MI FPGA	0x4	0x4	0x4	
No						
27	SUP	IO FPGA	0x16	0x16	0x16	
No						
27	SUP	MI FPGA2	0x3	0x3	0x3	
No						

\* If Running-Version and Flashed-Version are different it implies that the system has not yet been reloaded for the new version to take effect

Additional info for this installation:

-----

Service "vpc" in vdc 1: Vpc is enabled, Please make sure both Vpc peer switches have same boot mode using 'show boot mode' and proceed

Service "ptp" in vdc 1: During ISSU PTP protocol state and time synchronization will be disturbed. Time synchronization will resume after ISSU

Do you want to continue with the installation (y/n)? [n] y

Install is in progress, please wait.

[# ] 0%

Notifying services about the upgrade.

Setting boot variables.

[# ] 0%

Setting boot variables.

[#####] 100% -- SUCCESS

Performing configuration copy.

[#####] 100%

Performing configuration copy.

[#####] 100% -- SUCCESS

Module 1: Refreshing compact flash and upgrading bios/loader/bootrom.

Warning: please do not remove or power off the module at this time.

[# ] 0%

Module 1: Refreshing compact flash and upgrading bios/loader/bootrom.

Warning: please do not remove or power off the module at this time.

[#####] 100% -- SUCCESS

Module 27: Refreshing compact flash and upgrading bios/loader/bootrom.

Warning: please do not remove or power off the module at this time.

[# ] 0%

Module 27: Refreshing compact flash and upgrading bios/loader/bootrom.

Warning: please do not remove or power off the module at this time.

[#####] 100% -- SUCCESS

[# ] 0%

[#####] 100% -- SUCCESS

All EPLD/FPGAs are up to date

Upgrade can no longer be aborted, any failure will result in a disruptive upgrade

[# ] 0%

Freeing memory in the file system.

Loading images into memory.

[## ] 5%

Loading images into memory.

[#####] 100% -- SUCCESS

Saving linecard runtime state.

Saving linecard runtime state.

Saving supervisor runtime state.

Saving supervisor runtime state.

Saving mts state.

Saving mts state.

```
Rebooting the switch to proceed with the upgrade.
All telnet and ssh connections will now be temporarily terminated.
switch# incroncd[28730]: stopping service
63+1 records in
63+1 records out
265322496 bytes (265 MB, 253 MiB) copied, 0.178732 s, 1.5 GB/s
mount: overlay mounted on /newroot/usr.
Installing klm_card_index
done
Increase FPGA PCI timeout to 900ms
Linking n9k flash devices
creating flash devices BOOT_DEV= sda
Replacing inittab for node - host
INIT: version 3.01 booting
Setting up sysV scripts for host node
Installing ata_piix module ... done.
Unsquashing rootfs ...
is_lxc:1 is_titan_eor: is_stby: suffix: klm_ftrace: /isanboot/lib/modules/klm_ftrace.o
Installing ftrace in lxc 0 mode done
```

```
Checking all filesystems.cgroups initialized
Generating ssh keys...Done ssh keys
Starting OpenBSD Secure Shell server: sshd ... done sshd.
Checking rpmstore swap in host context.
tune2fs 1.46.5 (30-Dec-2021)
Setting reserved blocks percentage to 0% (0 blocks)
Installing kheaders module ... done.
INIT: Entering runlevel: 3
cp: cannot stat '/orig_fs/xr_cpa.img': No such file or directory
grep: /bootflash/platform.inf: No such file or directory
```

```
mount: overlay mounted on /usr.
Increase FPGA PCI timeout to 900ms
Linking n9k flash devices
creating flash devices BOOT_DEV= sda
Replacing inittab for node - vsup
INIT: version 3.01 booting
Unsquashing rootfs ...
vm.min_free_kbytes = 138240
No TOR virtual chassis
skip untra_klms
Enabling 8250 serial driver spurious INTs workaround
Installing isan procfs isan_proc_name=isan26... done.
Installing SSE module with card index 21172 and vslot ID 26 ... done.
Creating SSE device node 241 ... done.
cg controllers already mounted at /var/cgroup
Inserting kernel_services module ... done.
Making kernel_services character devices
is_lxc:1 is_titan_eor: is_stby:0 suffix: klm_ftrace: /isanboot/lib/modules/klm_ftrace.o
klm_ftrace already loaded. skip.
19.70: card_index: 21172, card_type: 103
Loading I2C driver ... done.
Installing CTRL driver for card_type 103 in vslot ID 26 without NEED_GEM ... done.
Loading IGB driver ...
Checking all filesystems.done.
```

```
Installing SPROM driver ... 21172 Quick rpm extraction...
```

```

IS_N9K done.
Segment 6 already extracted! Continuing...
Installing pfmsvcs module ...done.
Installing nvram module ... done.
Installing if_index module with port mode 6 ... done.
Calling install_tor for TOR
copying common rpm to ftp
Installing fcfwd
Installing RNI lcnd ... done
Running mode is N9K-ToR ...done
Installing LC netdev container_id=0 is_standby=0 ... done
Installing psdev module ... done.
Installing veobc module ... done.
Clean up previous pcap files present in tmp directory
Checking SR card
Card Index is 21172
SR Card detected.
Inserting eMMC module ...
Inserting OBFL module ... 24.38: eMMC Device found.
24.38: card has mmc
done.
24.39: Making OBFL character devices for mmc
24.45: SR_START (2099200), size 3
mounting plog for N9k!
24.46: mounting plog for N9k!
24.49: Done..mounting plog for N9k!
Mounting OBFL for eMMC
grep: /bootflash/platform.inf: No such file or directory
Attach blkoops

25.03: Before mounting blkoops
25.81: After mounting blkoops
26.45: recreate_mmcfttrace_rr_device
COPY the image to ORIG_LC_FS_PATH

Adding system startup for /etc/init.d/cgroups-init.
tune2fs 1.46.5 (30-Dec-2021)
Setting reserved blocks percentage to 0% (0 blocks)
  KEXEC LXC ISSU bypass
Persistent log store is mounted successfully
Loading system software
kernel.core_pattern = |/bin/sparsecore.sh %p %h %P %E
  minicoredumper disabled for this platform..
Starting rpcbind daemon...pidof[8519]: can't read from 8511/stat

done.
Generating ssh keys...creating NFS state directory: done
starting 8 nfsd kernel threads: done
starting mountd: done
starting statd: done
Saving image for img-sync ...
exit code: 1
Installing local RPMS
Done ssh keys
Starting OpenBSD Secure Shell server: sshd ... done sshd.
Patch Repository Setup completed successfully
/logflash/stats_ssd/.ssd_overall_data file exist !!
moving /logflash/stats_ssd/.ssd_overall_data to /logflash/stats_ssd/.ssd_lastboot_data
Starting crond: OK
TOR ISSU is TRUE. Touching /isan-upgrade/isan.bin at Tue Mar 24 10:11:08 PDT 2026
TOR ISSU is TRUE. /mnt/pss/upgrade/ present at Tue Mar 24 10:11:08 PDT 2026
touched /share/vmm/lxc_fallback at Tue Mar 24 10:11:08 PDT 2026
Creating /dev/mcelog
Starting mcelog daemon

```

```

Stopping crond: OK
fastboot or torissu
Starting crond: OK
N9K CPA setup done
N9K TOR LC CPA setup done
Remove pltfm_config from eltm.conf for SONE cards
INIT: Entering runlevel: 3
Replacement complete. All system shutdown binaries now point to /sbin/rep_file.
Running S93thirdparty-script...
vlc_card_index 0
S26: sw_id 21172 vp 0
S26 B: sw_id 21172, Moving libcrdcfgdata_tah_tor.so to libcrdcfgdata.so
packagegroup-nxos-optional-rpms_pkg_list

Starting lem_drv driver
done
Netbroker support IS present in the kernel.
done
Disabling cisco netbroker hooks ... done
Skipping EMON in TOR ...
Executing Prune clis.
Removing exusd cli files if it is not exbl_card in prune_clis
ethernet switching mode Tue Mar 24 10:11:17 PDT 2026
prepare span CLI

System is coming up ... Please wait ...
2026 Mar 24 10:12:28 switch %$ VDC-1 %$ %NVE-5-VDC_MAC_G_STATUS: Attempting to get router-mac,
current value N/A
2026 Mar 24 10:12:28 switch %$ VDC-1 %$ %ASCII-CFG-2-CONFIG_REPLAY_STATUS: Bootstrap Replay
Started.
2026 Mar 24 10:12:28 switch %$ VDC-1 %$ %USER-0-SYSTEM_MSG: Recover l3vm state - l3vm
2026 Mar 24 10:12:28 switch %$ VDC-1 %$ %ASCII-CFG-2-CONFIG_REPLAY_STATUS: Bootstrap Replay
Done.
2026 Mar 24 10:12:28 switch %$ VDC-1 %$ %NETSTACK-0-IP_EMERG_LOG: netstack [18083] Recovery
restart: Stateful Restart: init_iftype, Reset im_ext share memory intact FALSE
2026 Mar 24 10:12:31 switch %$ VDC-1 %$ %NETSTACK-0-IP_EMERG_LOG: netstack [18083] Recovery
restart: ip_ha_recover_if_restart: ip_recover_iftype_all
.

2026 Mar 24 10:12:34 switch %$ VDC-1 %$ %NETSTACK-0-IP_EMERG_LOG: netstack [18083]
Registration with clis server complete
Continuing with installation process, please wait.
The login will be disabled until the installation is completed.

Status for linecard upgrade.

[#####] 100% -- SUCCESS

Performing supervisor state verification.

[#####] 100% -- SUCCESS

Supervisor non-disruptive upgrade successful

Install has been successful.

User Access Verification

Login incorrect
User Access Verification

```

## Examples of upgrade types

```
switch login: admin
Password:
```

**Min-Disruptive ISSU Silicon One TOR**

```
=====
```

```
switch# install all nxos bootflash:nxos64-s1.10.6.2.F.bin.upg.tmp min-disruptive
non-interruptive
Installer will perform compatibility check first. Please wait.

Verifying image bootflash:/nxos64-s1.10.6.2.F.bin.upg.tmp for boot variable "nxos".
[#####] 100% -- SUCCESS

Verifying EPLD/FPGA image //bootflash/nxos64-s1.10.6.2.F.bin.upg.tmp.
[#####] 100% -- SUCCESS

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

Preparing "nxos" version info using image bootflash:/nxos64-s1.10.6.2.F.bin.upg.tmp.
[#####] 100% -- SUCCESS

Preparing "bios" version info using image bootflash:/nxos64-s1.10.6.2.F.bin.upg.tmp.
[#####] 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	min-disruptive	rolling	
27	yes	min-disruptive	reset	

Images will be upgraded according to following table:

Module	Image	Running-Version (pri:alt)	New-Version
1	lcn9k	10.6 (3)	10.6 (3u) I9 (1u)
yes			
27	nxos	10.6 (3)	10.6 (3u) I9 (1u)
yes			
27	bios	v01.10 (03/06/2025) :v01.08 (01/22/2025)	v01.10 (03/06/2025)
no			

FPGA microcode will be upgraded according to following table:

Module	Type	EPLD	Running-Version	Flashed-Version*	New-Version	Upg-Required
27	SUP	MI FPGA	0x1000a	0x1000a	0x1000a	
No						
27	SUP	IO FPGA	0x1000d	0x1000d	0x1000d	
No						
27	SUP	IO FPGA (TAM)	0x70016	0x70016	0x70016	

```
No
  27  SUP  IO FPGA(FB)          0x1000d          0x1000d          0x1000d
No
```

\* If Running-Version and Flashed-Version are different it implies that the system has not yet been reloaded for the new version to take effect

Additional info for this installation:  
-----

Estimated traffic outage time for current upgrade : about 65 ms

Install is in progress, please wait.

```
[#           ] 0%
```

Notifying services about the upgrade.

Setting boot variables.

```
[#           ] 0%
```

Setting boot variables.

```
[#####] 100% -- SUCCESS
```

Performing configuration copy.

```
[#####] 100%
```

Performing configuration copy.

```
[#####] 100% -- SUCCESS
```

Module 1: Upgrading bios/loader/bootrom.

Warning: please do not remove or power off the module at this time.

```
[#           ] 0%
```

Module 1: Upgrading bios/loader/bootrom.

Warning: please do not remove or power off the module at this time.

```
[#####] 100% -- SUCCESS
```

Module 27: Upgrading bios/loader/bootrom.

Warning: please do not remove or power off the module at this time.

```
[#           ] 0%
```

Module 27: Upgrading bios/loader/bootrom.

Warning: please do not remove or power off the module at this time.

```
[#####] 100% -- SUCCESS
```

```
[#           ] 0%
```

```
[#####] 100% -- SUCCESS
```

All EPLD/FPGAs are up to date

Upgrade can no longer be aborted, any failure will result in a disruptive upgrade

```
[#           ] 0%
```

Freeing memory in the file system.

Loading images into memory.

```
[##        ] 5%
```

Loading images into memory.

```
[#####] 100% -- SUCCESS
```

Saving linecard runtime state.

Saving linecard runtime state.

Saving supervisor runtime state.

Saving supervisor runtime state.

Saving mts state.

Saving mts state.

```
Rebooting the switch to proceed with the upgrade.
All telnet and ssh connections will now be temporarily terminated.
switch# incroncd[18252]: stopping service
71+1 records in
71+1 records out
300548096 bytes (301 MB, 287 MiB) copied, 0.155314 s, 1.9 GB/s
mount: overlay mounted on /newroot/usr.
Installing klm_card_index
done
Linking n9k mando SSD partition...
creating flash devices BOOT_DEV= sda
Replacing inittab for node - host
INIT: version 3.04 booting
Setting up sysV scripts for host node
Installing ata_piix module ... done.
Unsquashing rootfs ...
is_lxc:1 is_titan_eor: is_stby: suffix: klm_ftrace: /isanboot/lib/modules/klm_ftrace.o
Installing ftrace in lxc 0 mode done
      Model Number:      Micron_5400_MTFDDAV480TGA
      Serial Number:     MSY28450C90
      Firmware Revision: D4CN005
```

```
Checking all filesystems.cgroups initialized
System is at the expected SSD partitioning format
Generating ssh keys...Done ssh keys
Starting OpenBSD Secure Shell server: sshd ... done sshd.
Checking rpmstore swap in host context.
tune2fs 1.47.0 (5-Feb-2023)
Setting reserved blocks percentage to 0% (0 blocks)
Installing kheaders module ... done.
INIT: Entering runlevel: 3
```

```
mount: overlay mounted on /usr.
Linking n9k mando SSD partition...
creating flash devices BOOT_DEV= sda
Replacing inittab for node - vsup
INIT: version 3.04 booting
Unsquashing rootfs ...
No TOR virtual chassis
skip untra_klms
Enabling 8250 serial driver spurious INTs workaround
Installing isan procfs isan_proc_name=isan26... done.
Installing SSE module with card index 21267 and vslot ID 26 ... done.
Creating SSE device node 240 ... done.
cg controllers already mounted at /var/cgroup
Inserting kernel_services module ... done.
Making kernel_services character devices
is_lxc:1 is_titan_eor: is_stby:0 suffix: klm_ftrace: /isanboot/lib/modules/klm_ftrace.o
klm_ftrace already loaded. skip.
      Model Number:      Micron_5400_MTFDDAV480TGA
      Serial Number:     MSY28450C90
      Firmware Revision: D4CN005
26.81: card_index: 21267, card_type: 152
Loading I2C driver ... done.
Installing CTRL driver for card_type 152 in vslot ID 26 without NEED_GEM ... done.
26.88: Interrupt throttling disabled. No ctrl irq detected.
Loading IGB driver ...
Checking all filesystems.
```

```

Quick rpm extraction...
done.
Segment 6 already extracted! Continuing...
Segment 7 already extracted! Continuing...
Modify INotify fd
128
fs.inotify.max_user_instances = 2048
2048
Installing SPROM driver ... 21267 IS_N9K done.
Installing pfmsvcs module ...done.
Installing nvram module ... done.
Installing if_index module with port mode 6 ... done.
Calling install_tor for TOR
copying common rpm to ftp
Installing fcfwd
Installing RNI lcnd ... done
Running mode is N9K-ToR ...done
Installing LC netdev container_id=0 is_standby=0 ... done
Installing psdev module ... done.
Installing veobc module ... done.
Clean up previous pcap files present in tmp directory
Checking SR card
Card Index is 21267
old data: 9f000000 new data: 9f000000
old data: 0 new data: 0
old data: a0901406 new data: a0901406
33.23: Inserting obfl & mtd spi driver ...
[ 33.245002] fpga_setup_probe
[ 33.248280] Probe called for devide 0x17a
33.32: Done..Inserting obfl & mtd spi driver ...
Making OBFL character devices
old data: 9f000000 new data: 9f000000
old data: 0 new data: 0
old data: a0901406 new data: a0901406
mounting plog for N9k!
33.38: mounting plog for N9k!
33.42: Done..mounting plog for N9k!
mounting recovery for N9k!
33.44: mounting recovery for N9k!
Mounting OBFL pstore for mtd
System is at the expected SSD partitioning format
COPY the image to ORIG_LC_FS_PATH
/isanboot/bin/images/sl_gr2_xc_sdk.bin
/isanboot/bin/images/slhal_n9000.bin
tune2fs 1.47.0 (5-Feb-2023)
Setting reserved blocks percentage to 0% (0 blocks)
KEXEC LXC ISSU bypass
Persistent log store is mounted successfully
Loading system software
kernel.core_pattern = /bin/sparsecore.sh %p %h %P %E
minicoredumper disabled for this platform...
Starting rpcbind daemon...Generating ssh keys...done.
Saving image for img-sync ...
creating NFS state directory: done
starting 8 nfsd kernel threads: done
starting mountd: done
starting statd: done
exit code: 1
Installing local RPMS
Done ssh keys
Starting OpenBSD Secure Shell server: sshd ... done sshd.
Patch Repository Setup completed successfully
/logflash/stats_ssd/.ssd_overall_data file exist !!
moving /logflash/stats_ssd/.ssd_overall_data to /logflash/stats_ssd/.ssd_lastboot_data

```

```

Starting crond: OK
TOR ISSU is TRUE. Touching /isan-upgrade/isan.bin at Thu Mar 19 09:47:17 PDT 2026
TOR ISSU is TRUE. /mnt/pss/upgrade/ present at Thu Mar 19 09:47:17 PDT 2026
touched /share/vmm/lxc_fallback at Thu Mar 19 09:47:17 PDT 2026
Creating /dev/mcelog
Starting mcelog daemon
Stopping crond: OK
Remove pltfm_config from eltm.conf for SONE cards
INIT: Entering runlevel: 3
Replacement complete. All system shutdown binaries now point to /sbin/rep_file.
Starting crond: OK
Deleting /usr/bin/xr_cpa
Deleting /usr/lib64/xr_cpa
Deleting /usr/local/etc/xr-cpa-data
Deleting /usr/lib64/dummy_libs
Deleting /usr/lib64/r78x_27.tar.gz
Run dc3_sensor as root
ASIC_GIBRALTAR is
ASIC_IRON is
Running S93thirdparty-script...
vlc_card_index 0
S26: sw_id 21267 vp 0
S26 B: sw_id 21267, Retaining libcrdcfgdata.so as is
packagegroup-nxos-optional-rpms_pkg_list

Starting lem_drv driver
Netbroker support IS present in the kernel.
done
done
Disabling cisco netbroker hooks ... done
Skipping EMON in TOR ...
Executing Prune clis.
Removing exusd cli files if it is not exbl_card in prune_clis
ethernet switching mode Thu Mar 19 09:47:24 PDT 2026
prepare span CLI

Continuing with installation process, please wait.
The login will be disabled until the installation is completed.

Status for linecard upgrade.
[#####] 100% -- SUCCESS

Performing supervisor state verification.
[#####] 100% -- SUCCESS

Supervisor min-disruptive upgrade successful

Install has been successful.

User Access Verification
switch login: admin
Password:

Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2026, Cisco and/or its affiliates.
All rights reserved.

```

## Prerequisites for NX-OS software downgrade

The prerequisites for downgrading the NX-OS software include

- Before downgrading from a NX-OS release that supports the Control Plane Policing (CoPP) feature to an earlier release that does not support the CoPP feature, verify compatibility using the **show incompatibility nxos bootflash:filename** command. If incompatibility exists, disable any features that are incompatible with the downgrade image before downgrading the software.
- Save, commit, or discard any active configuration sessions before downgrading the NX-OS software image on your device.

## NX-OS software downgrade guidelines

Read and follow these guidelines and limitations listed in this section before downgrading your NX-OS software from the current release to an earlier release.

- The only supported method of downgrading a Nexus 9000 Series switch is to utilize the **install all** command. Changing the boot variables, saving the configuration, and reloading the switch is not a supported method to downgrade the switch.

Disable the Guest Shell if you need to downgrade from NX-OS Release 9.3(x) to an earlier release.

- Performing an ISSU downgrade from NX-OS Release 9.3(x) to Release 7.0(3)I4(1) with an FCoE (Fiber Channel over Ethernet) NPV (N-port Virtualization) configuration causes the port channel to crash with a core file:

```
[##### ] 38%2016 Apr 18 20:52:35 n93-ns1 %$ VDC-1 %$ %SYSMGR-2-
SERVICE_CRASHED: Service "port-channel" (PID 14976) hasn't caught signal 11 (core
will be saved)
```

- ISSU (non-disruptive) downgrade is not supported
- On Nexus 9500 switches with N9508-E2 Fabric module, downgrade from any 9.x or 10.x supported releases to any unsupported releases of 7.x is not supported.
- When downgrading from the NX-OS Release 9.3(x) to earlier releases, any ACL with the statistics per-entry command enabled and applied as RACL needs the statistics per-entry command removed from the running configuration before downgrading. Otherwise, the interfaces on which this ACL is applied as a RACL will be error disabled after the downgrade.
- Prior to downgrading a Nexus 9500-series switch, with -FX or -FX+EX line cards, from NX-OS Release 10.1(x) to earlier releases (9.2(x) or 7.x), the TCAM region that applies to NetFlow (ing-netflow) should be carved to zero (0) using the following command:

### **hardware access-list tcam region ing-netflow 0**

The configuration change is required because the default ing-netflow TCAM region in 9.3(1) and onwards is 512 while the default in 9.2(x) and earlier is 0.

- When downgrading from the NX-OS Release 10.1(x) to a release prior to 9.3(x), make sure that the ACL TCAM usage for ingress features does not exceed the allocated TCAM space in the absence of the label sharing feature. Label sharing is a new feature in NX-OS Release 9.3(x). Otherwise, interfaces with RACLs that could not fit in the TCAM will be disabled after the downgrade.

- Software downgrades should be performed using the **install all** command. Changing the boot variables, saving the configuration, and reloading the switch is not a supported method to downgrade the switch.
- This limitation applies to Nexus platform switches that support Trust Anchor Module (TAM):  
The TACACS global key cannot be restored when downgrading from NX-OS Release 9.3(3) and higher to any earlier version. TAM was updated to version-7 in 9.3(3), but earlier NX-OS versions used TAM version-3.
- iCAM must be disabled before downgrading from Release 9.2(x) or Release 9.3(x) → 7.0(3)I7(1). Only Release 9.3(1) → Release 9.2(4) can be performed if iCAM is enabled.
- Beginning with NX-OS Release 9.3(3), new configuration commands exist for SRAPP (with sub-mode options for MPLS and SRTE). The SRAPP configuration on the switch running release 9.3(3) (or later) will not be present if the switch is downgraded to an earlier release.
- 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. For more information about your specific chassis, see the relevant [Hardware Installation Guide](#).
- NX-OS automatically installs and enables the guest shell by default. However, if the device is reloaded with a 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 NX-OS image.
- You must delete the switch profile (if configured) when downgrading from a NX-OS release that supports switch profiles to a release that does not. For more information, see the [Cisco Nexus 9000 Series NX-OS System Management Configuration Guide](#).
- Software downgrades are disruptive. In-service software downgrades (ISSDs), also known as non-disruptive downgrades, are not supported.
- While downgrading from the NX-OS Release 10.2(1)F or higher to an earlier release, the **install all** command is blocked when the delay config is present in track list Boolean/weight.
- While performing ISSD from NX-OS Release 10.2(3)F to NX-OS Release 10.2(2)F with **epbr L2** applied on interfaces, remove the policies from interfaces before performing ISSD to avoid the duplicate tracks issue.
- Beginning with NX-OS Release 10.2(3)F, if you have configured the **lldp chassis-id switch** command, then you must disable the command before performing ISSD.
- Beginning with 10.2(3)F, although application of ePBR policy to access ports is supported, downgrading with this configuration is not recommended.
- When feature ngmvpn is enabled and a disruptive downgrade is performed from NX-OS Release 10.3(2)F to NX-OS Release 10.3(1)F, although a few VRFs are missing from the show run output, this is only a display issue, and has no functional impact.
- When a switch is downgraded from NX-OS Release 10.3(3)F or 10.4(1)F to a version that supports both Native and LXC modes, the switch always goes to Native mode even if the upgrade was done from LXC mode. To keep the mode persistent after a downgrade, ensure that you perform the downgrade in the following sequence:

**Note**

- The following sections are applicable only to Nexus 9300-FX3 and 9300-GX platform switches.
- When system comes up in native mode on downgrade, boot mode lxc is removed from configuration.

- 
- LXC mode upgrade/downgrade: For example,
    1. The switch is running on NX-OS Release 10.3(2)F in LXC mode.
    2. Upgrade the version to NX-OS Release 10.3(3)F (LXC mode).
    3. Downgrade the version to NX-OS Release 10.3(2)F to the Native mode.
    4. Execute the boot mode lxc configuration command, save the configuration, and reload the switch.
    5. The switch comes up in NX-OS Release 10.3(2)F LXC mode.

- Native mode upgrade/downgrade:

## Example 1

1. The switch (9300-FX3 or 9300-GX) is running on NX-OS Release 10.3(2)F in the Native mode.
2. Upgrade the version to NX-OS Release 10.3(3)F (LXC mode), as these (9300-FX3 or 9300-GX) switches support only LXC mode.
3. Downgrade to any earlier NX-OS Release [for example, 10.3(2)].
4. The switch comes up in NX-OS Release 10.3(2)F in Native mode.

## Example 2

1. The switch (Nexus 9300-FX or 9300-FX2) is running on NX-OS Release 10.3(2)F in the Native mode.
2. Upgrade the version to NX-OS Release 10.4(1)F (LXC mode), as these switches support only LXC mode.
3. Downgrade to any earlier NX-OS Release [for example, 10.3(2)].
4. The switch comes up in NX-OS Release 10.3(2)F in Native mode.

- When you downgrade from NX-OS Release 10.4(2)F to any earlier releases until 10.3(2)F (included), N9K-C9400-SW-GX2A Sup card ports 2xSFP Eth10/1-2 are not supported.
- When Nexus 9400 has feature security-group enabled, then downgrade from 10.5(1)F release to a lower release is not possible as feature security-group is not supported on 9400 in 10.4(3)F release and earlier.
- Downgrade of Nexus 9800 switches that have s1 image format from NX-OS Release 10.5(1)F to earlier releases that have cs image format is supported. However, as the s1 image is not present in earlier releases, the downgrade should be done to the cs image from the corresponding release.

- If you are on NX-OS Release 10.5(2)F, where DSVNI with IPv6 underlay feature is supported, and downgrade to a release that does not support this feature, then this leads to traffic loss for DSVNI VLANs. To avoid this, ensure that you remove the IPv6 underlay with downstream VNI configuration before downgrading.
- During downgrade, where both source and target images support Type-6 encryption, while performing device reload, if ASCII replay is triggered without binary restore, primary key gets lost. The primary key must be reconfigured after device reload. Use the **key config-key ascii** command to reconfigure the primary key and avoid encryption issues. However, downgrade with binary restore retains the primary key after the reboot, provided both source and target images support Type-6 encryption.

If you downgrade the system from an image that supports Type-6 encryption to an image that does not support Type-6 encryption, compatibility check fails.

- When a switch is downgraded from NX-OS Release 10.6(1)F to any lower releases, the **allow feature-set fex** configuration gets added to the running configuration file.

## Downgrade to an earlier software release

The downgrade of Nexus 9000 switches involves using the supported **install all** command to revert to an earlier NX-OS software release, ensuring compatibility by checking for software and hardware incompatibilities, disabling unsupported features, and following a structured procedure including saving configurations and reloading the switch.

Downgrade on Nexus switches is always disruptive.




---

**Note** Downgrade from releases 10.5(1)F, 10.5(2)F, or 10.5(3)F to 10.4(6)F and later 10.4(x) releases are not supported and can result in configuration corruption. If downgrade is needed, upgrade first to 10.5(4)M or later releases and then downgrade to 10.4(6)F and later 10.4(x) releases. See [CSCwr21007](#) in the [Cisco Nexus 9000 Series NX-OS Release Notes, Release 10.4\(6\)M](#).

---




---

**Note** If an error message appears during the downgrade, the downgrade fails due to the indicated reason. See the appropriate version of the [Cisco Nexus 9000 Series NX-OS Troubleshooting Guide](#) for a list of possible causes and solutions.

---

### Before you begin

Read the release notes for the software image file for any exceptions to this downgrade procedure. For information about software image file, see the appropriate version of the [Cisco Nexus 9000 Series NX-OS Release Notes](#).

### Procedure

---

- Step 1** Log in to the device on the console port connection.
- Step 2** Verify the software image file and copy it to the active supervisor module.

- a) Verify that the image file for the downgrade is present on the active supervisor module bootflash.

**Example:**

```
switch# dir bootflash:
```

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

**Note**

If you need more space on the active or standby supervisor module bootflash, use the **delete** command to remove unnecessary files.

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

**Example:**

```
switch# copy scp://user@scpserver.cisco.com/download/nxos.9.2.1.bin
bootflash:nxos.9.2.1.bin
```

**Step 3** Check for any incompatibilities.

- a) Check for any software incompatibilities.

**Example:**

```
switch# show incompatibility-all nxos bootflash:nxos.9.2.1.bin
Checking incompatible configuration(s)
No incompatible configurations
```

The resulting output displays any incompatibilities and remedies.

- b) Check for any hardware incompatibilities.

**Example:**

```
switch# show install all impact nxos bootflash:nxos.9.2.1.bin
```

**Step 4** Mitigate incompatibilities.

- a) Disable any features that are incompatible with the downgrade image.  
b) Power off any unsupported modules.

**Example:**

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

**Step 5** Save the running configuration to the startup configuration.**Example:**

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

**Step 6** Downgrade the NX-OS software using the **install all nxos bootflash** *<nxos\_image\_to\_downgrade>* command.**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 7** (Optional) Display the entire downgrade process.**Example:**

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

**Step 8** (Optional) Log in and verify that the device is running the required software version.

**Example:**

```
switch# show version
```

---