Upgrade Nexus 5500 and 5600 NX-OS Software

Contents

Introduction

This document describes upgrade options and paths for the NX-OS software of a Cisco Nexus 5500 and 5600 series switch.

Prerequisites

Applicable Hardware

The information covered in this document applies to this hardware only:

- Cisco Nexus 5596UP
- Cisco Nexus 5596T
- Cisco Nexus 5548UP
- Cisco Nexus 5548P
- Cisco Nexus 5672UP
- Cisco Nexus 5648Q
- Cisco Nexus 5624Q
- Cisco Nexus 5696Q
- Cisco Nexus 56128

NX-OS Software

The NX-OS software for the Nexus 5500 and 5600 Series switches consists of the kickstart and system images . When updating the device's NX-OS software, ensure both images match the same version.

To obtain the required NX-OS images:

1. Navigate to the Software Download Center at https://software.cisco.com/download/home .
2. Look for the corresponding Nexus 5500 and 5600 platform that needs to be upgraded.
3. Download both, the system and kickstart image for the code that needs to be installed on the device.

Minimum Recommended Codes

For minimum information recommended NX-OS software releases for Cisco Nexus 5500 and 5600 Series switches, refer to one of these applicable documents:

Minimum Recommended Cisco NX-OS Releases for Cisco Nexus 5500 Series Switches

Minimum Recommended Cisco NX-OS Releases for Cisco Nexus 5600 Series Switches

Background Information

Cisco Nexus 5500 and 5600 Series switches provide two different options to update the software: In Service Software Upgrade (ISSU) and Non-ISSU. Each option can be leveraged depending on the environment, configuration applied, and downtime that can be permitted.

In-Service Software Upgrade (ISSU)

Cisco Nexus 5500 and 5600 Series switches support a single “supervisor” ISSU architecture and perform a stateful restart of the entire operating system upon execution, whilst leaving data plane forwarding intact. During this time, control plane functions of the switch undergoing ISSU are temporarily suspended for 80 seconds, and configuration changes are disallowed.

Considerations

- ISSU is only supported between compatible images. See the Supported Upgrade Paths section in this document.
- Any failures from the point where ISSU cannot be aborted gracefully can result in a disruptive upgrade (chassis reload). Common reasons for ISSU interruption are module insertions and removals or Spanning-Tree Topology Changes while the switch is undergoing ISSU.
- A successful ISSUdoes not cause any reload on the chassis or any connected FEXs.
- CLI and SNMP config change requests are denied during ISSU operations.

Prerequisites for ISSU

Here is a list of requirements that must be met for ISSU to be supported, failing to meet one of them is enough for ISSU to fail:

- The device must not run Layer 3 services. You must unconfigure all Layer 3 features, remove the L3 license, and reload the switch, to have a nondisruptive upgrade with an ISSU.
- Fast LACP timers (hello=1 sec, dead=3 sec) are not supported with ISSU. Default timers (hello=30 sec, dead=90 sec) must be configured on the switch and its LACP neighbors.
- STP-enabled switches cannot be present downstream to the switch undergoing an ISSU.
- The STP Bridge Assurance feature (**spanning-tree port type network**) cannot be configured on any interface except on the vPC peer link.
- No topology change must be active in any STP instance.

- There cannot be any interfaces in STP Designated Forwarding status except the VPC peer-link. If there are any interfaces in this state, and they are connected to devices that do not run STP, like servers, routers, firewalls, and others, you can configure `spanning-tree port type edge` on access ports and on trunk ports, to comply with the requirement. Do not use `spanning-tree port type edge` on interfaces connecting to switches running STP.
- In the case of a VPC set-up, all ISSU prerequisites must be met on both VPC peers simultaneously.

Management Services during ISSU

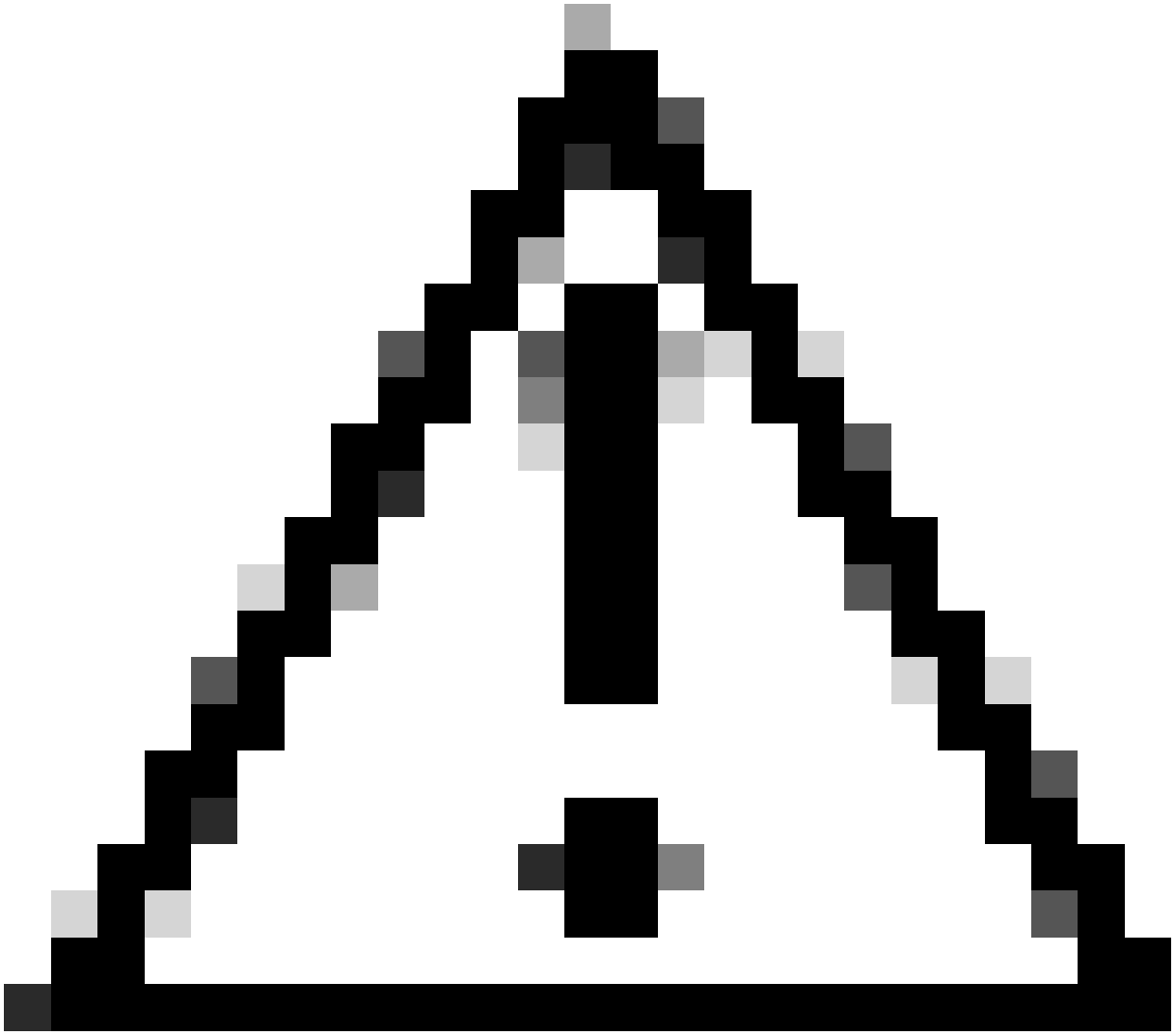
Before the switch is reset for ISSU (control plane goes down for ~80sec), `inband and management connections are brought down, and are brought back up after ISSU completes`**.** Services that depend on inband and management ports are impacted during this time, for example: Telnet, SSH, AAA, RADIUS, HTTP, and NTP sessions to and from the switch are disrupted during ISSU control plane reboot. For this reason, it is recommended to have console access during the ISSU process, so the user can still observe the ISSU progress while the management connections come back.

Non-In-Service Software Upgrade (Non-ISSU)

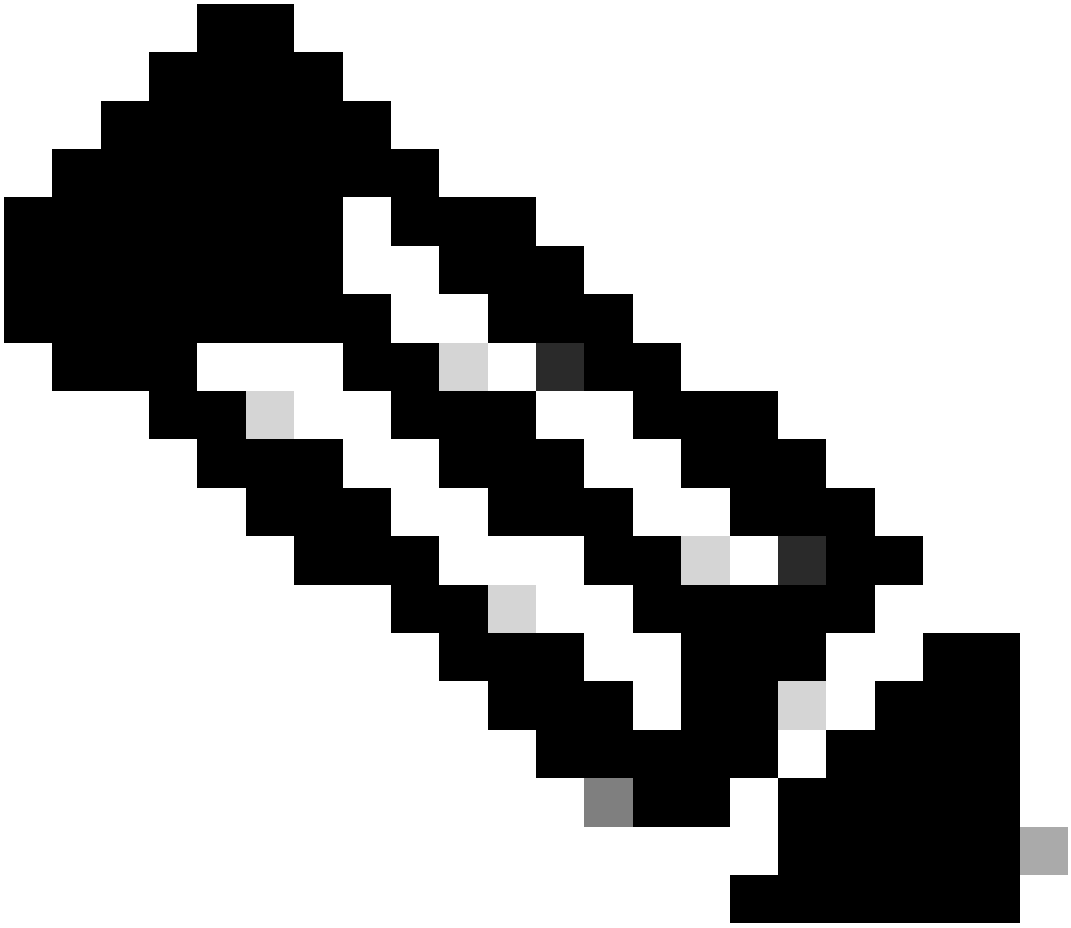
Cisco Nexus 5500 and 5600 Series switches also support a non-ISSU option, commonly known as a disruptive upgrade, which allows a new image to be loaded by reloading the device.

Reasons for Disruptive Upgrade

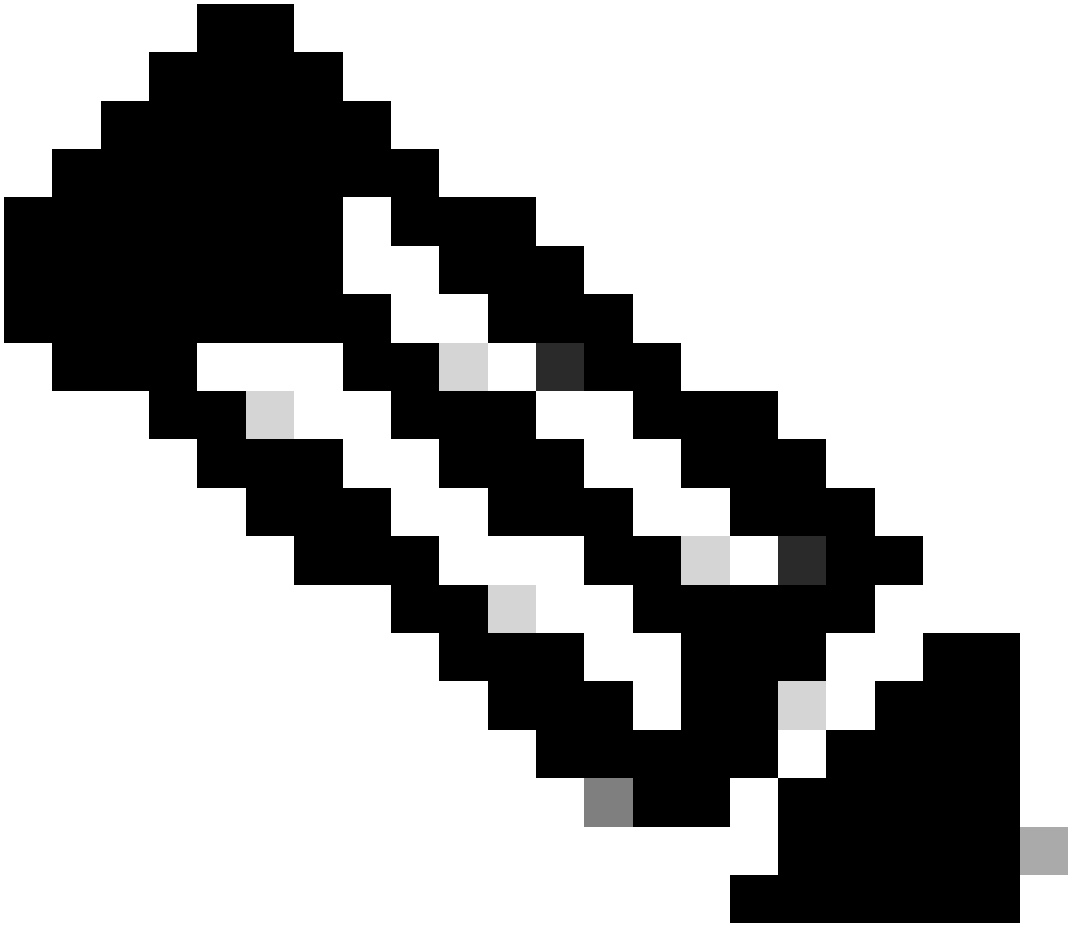
- Disruptive upgrade is the only method to upgrade if one of the ISSU conditions is not met.
- With a disruptive upgrade, all the connected FEXs are upgraded simultaneously, so a maintenance window can be shorter.
- Disruptive upgrades can be performed between incompatible images, which can help avoid multiple upgrade jumps that are required by the ISSU option.



Caution: Running an upgrade between incompatible images can result in certain configuration loss. See Cisco bug ID CSCul22703 for details. A decision must be made on whether losing part of the configuration and restoring it after the upgrade is acceptable, or if it is preferred to retain all configuration by using a supported upgrade path.



Note: If upgrading from any 7. x release to a release which has a fix of Cisco bug ID CSCva49522, binary configuration replay is used and loss of configuration is not expected.



Note: Nexus 5596 switches fail to boot up after a reload or a NX-OS upgrade if power controller settings have not been updated. See Cisco bug ID CSCun66310 for details.

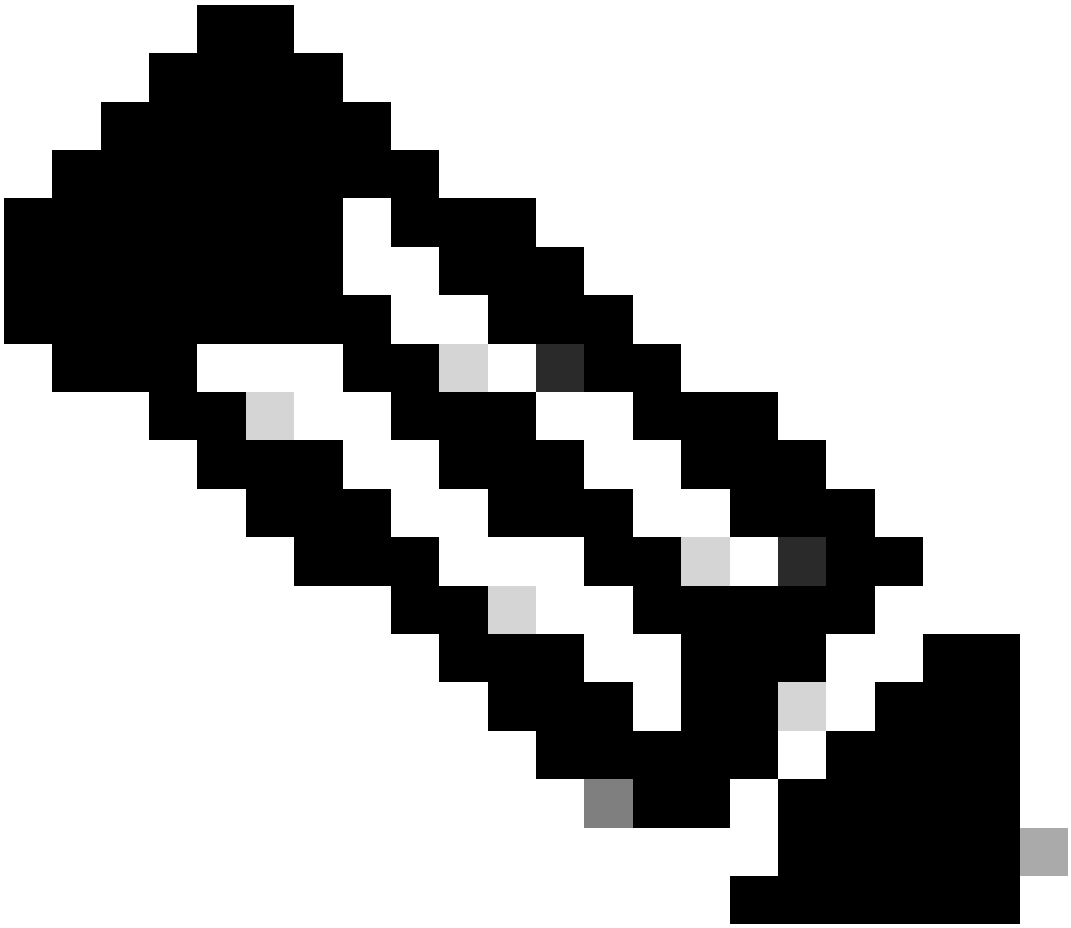
Supported Upgrade Paths

Refer to Table 1. for the supported upgrade paths to Cisco NX-OS Release 7.3(13)N1(1) and 7.3(14)N1(1) on Nexus 5500.

Table 1. Supported Upgrade Paths for the Cisco Nexus 5500

Current Release	Intermediate Releases	Target Release
Any release on Cisco NX-OS 7.3	Direct upgrade is supported	7.3(13)N1(1) 7.3(14)N1(1)
Any release on Cisco NX-OS	7.3(2)N1(1)	

7.2		
NX-OX 7.1(4) or 7.1(5)	Direct upgrade is supported	
NX-OX 7.1 before 7.1(4)	7.1(4)N1(1) or 7.1(5)N1(1)	
NX-OX 7.0(4) or higher	7.1(4)N1(1) or 7.1(5)N1(1)	
NX-OX 7.0 before 7.0(4)	Two jumps: First 7.0(8)N1(1), then 7.1(4)N1(1)	
NX-OX 5.2 or 6.0	Two jumps: First 7.0(4)N1(1), then to 7.1(4)N1(1)	



Note: You cannot upgrade non-disruptively to Cisco NX-OS Release 7.3(13)N1(1) from Cisco NX-OS Release 7.3(7)N1(1) because of the issue due to Cisco bug ID CSCvt58479.

See Table 2. for the supported upgrade paths to Cisco NX-OS Release 7.3(13)N1(1) and 7.3(14)N1(1) on Nexus 5600.

Table 2. Supported Upgrade Paths for the Cisco Nexus 5600 Series Switches

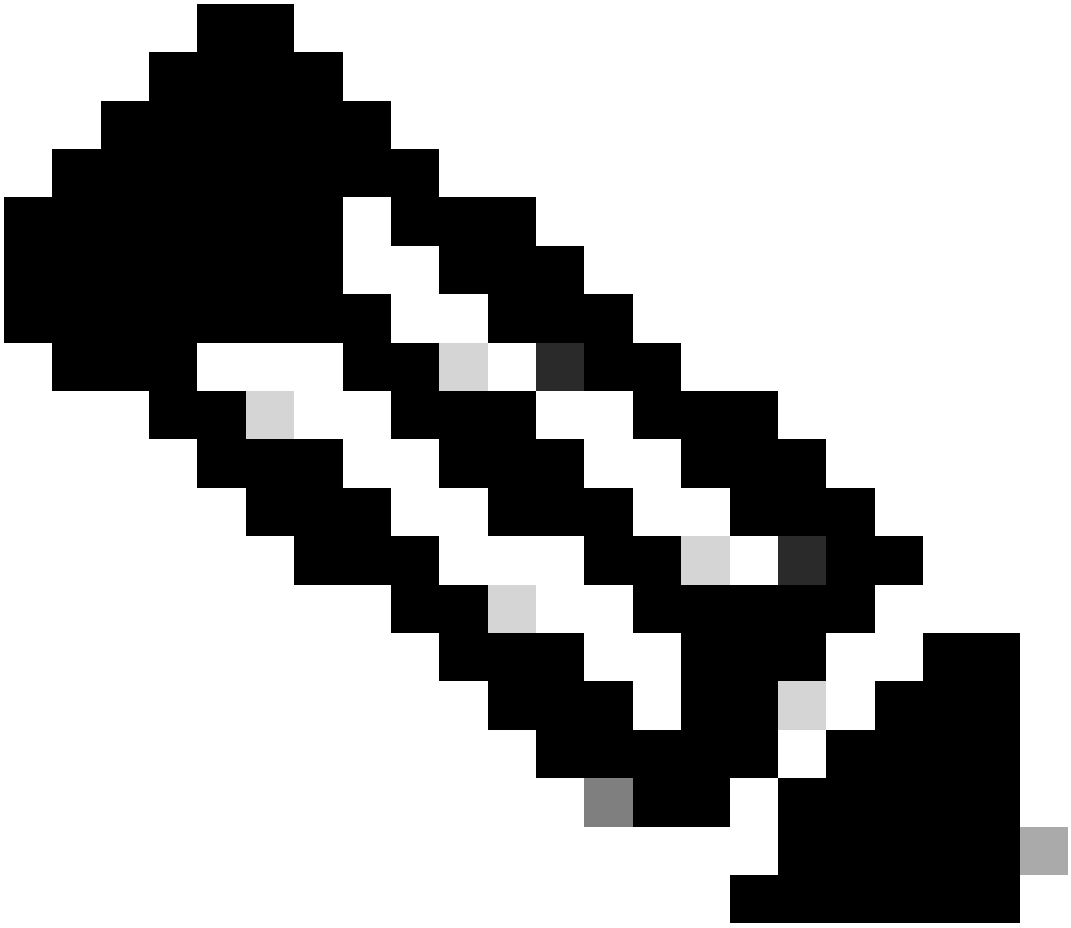
Current Release	Intermediate Releases	Target Release
Any release higher than 7.3(8)N1(1)	Direct upgrade is supported	7.3(13)N1(1) 7.3(14)N1(1)
NX-OS 7.2(1)N1(1)	Two jumps: First 7.3(2)N1(1), then 7.3(8)N1(1)	
NX-OS 7.2(0)N1(1)	Three jumps: First 7.2(1)N1(1), then 7.3(2)N1(1), then 7.3(8)N1(1)	
NX-OX 7.1(4) or 7.1(5)	7.3(8)N1(1)	
NX-OX 7.1 before 7.1(4)	7.1(4)N1(1) or 7.1(5)N1(1)	
NX-OX 7.0(4) or higher	7.1(4)N1(1) or 7.1(5)N1(1)	
NX-OX 7.0 before 7.0(4)	Two jumps: First 7.0(8)N1(1), then 7.1(4)N1(1)	

Supported Methods to Upgrade

ISSU (Non-Disruptive)

To trigger an ISSU upgrade, the install all command must be used between compatible images:

```
switch# install all kickstart bootflash:[kickstart-image.bin] system bootflash:[system-image.bin]
```



Note: For additional information about upgrade steps on Cisco Nexus 5500 and 5600 Series switches select the corresponding upgrade guide from Cisco Nexus 5X00 Series NX-OS Software Upgrade and Downgrade Guide and review the section **Upgrading Procedures**.

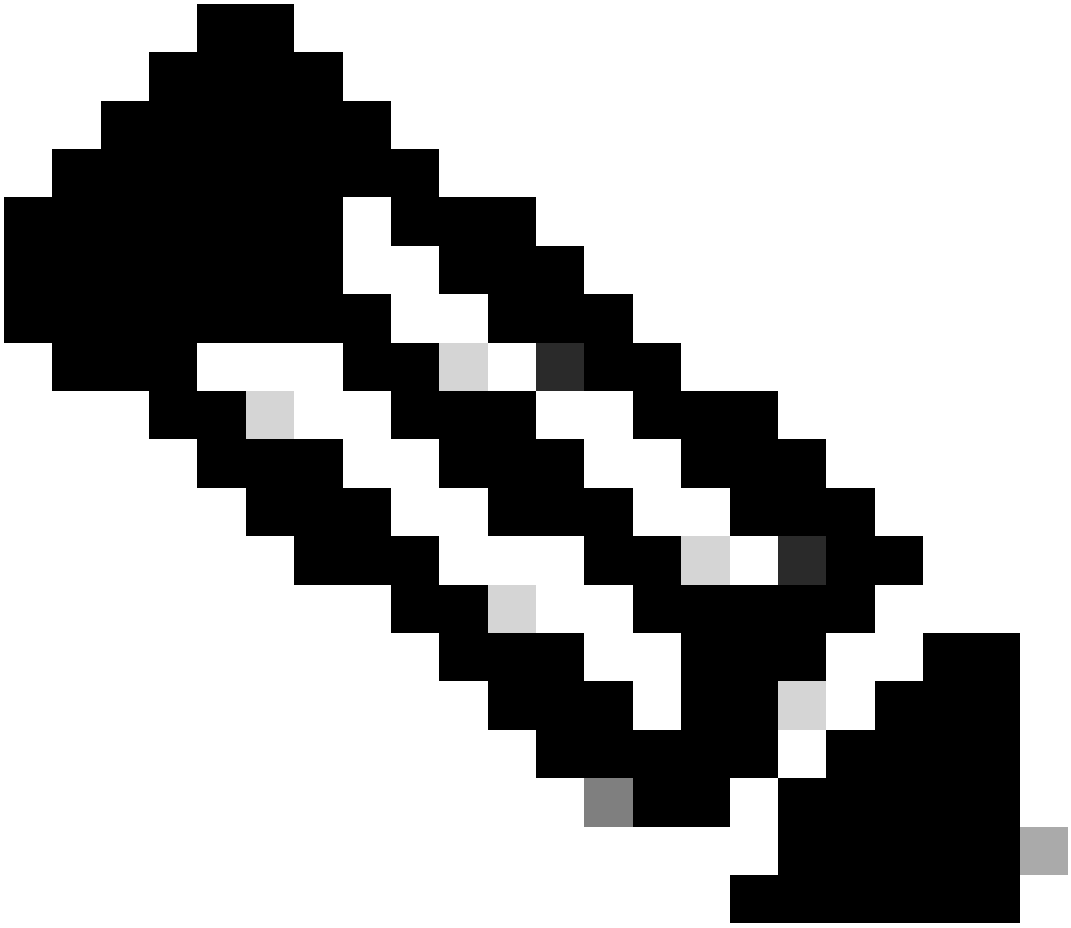
Non-ISSU (Disruptive)

To trigger a Non-ISSU upgrade, the install all command must be used between compatible or incompatible images:

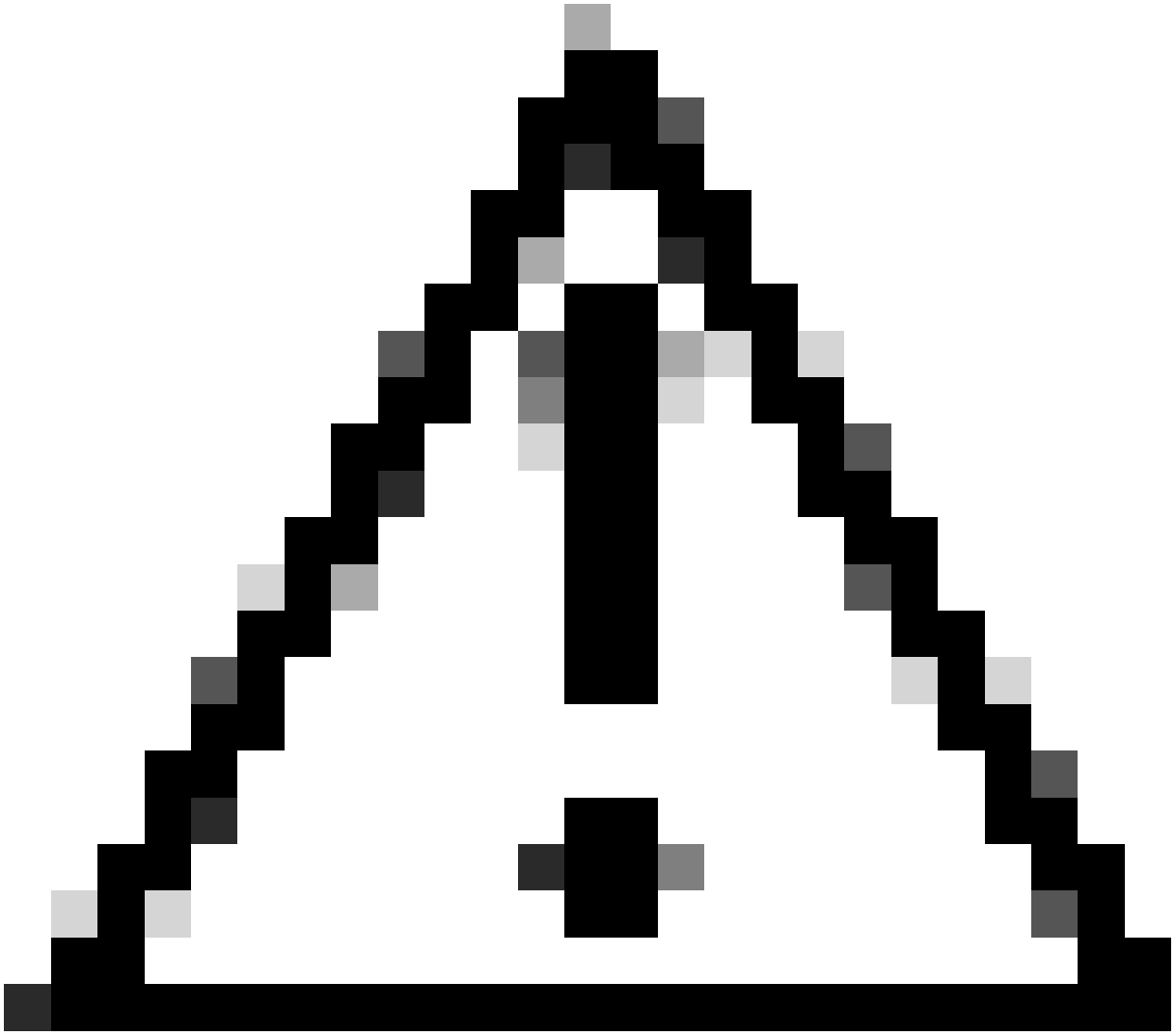
```
switch# install all kickstart bootflash:[kickstart-image.bin] system bootflash:[system-image.bin]
```

To force a disruptive upgrade even if an ISSU can be leveraged use install all command with the force option:

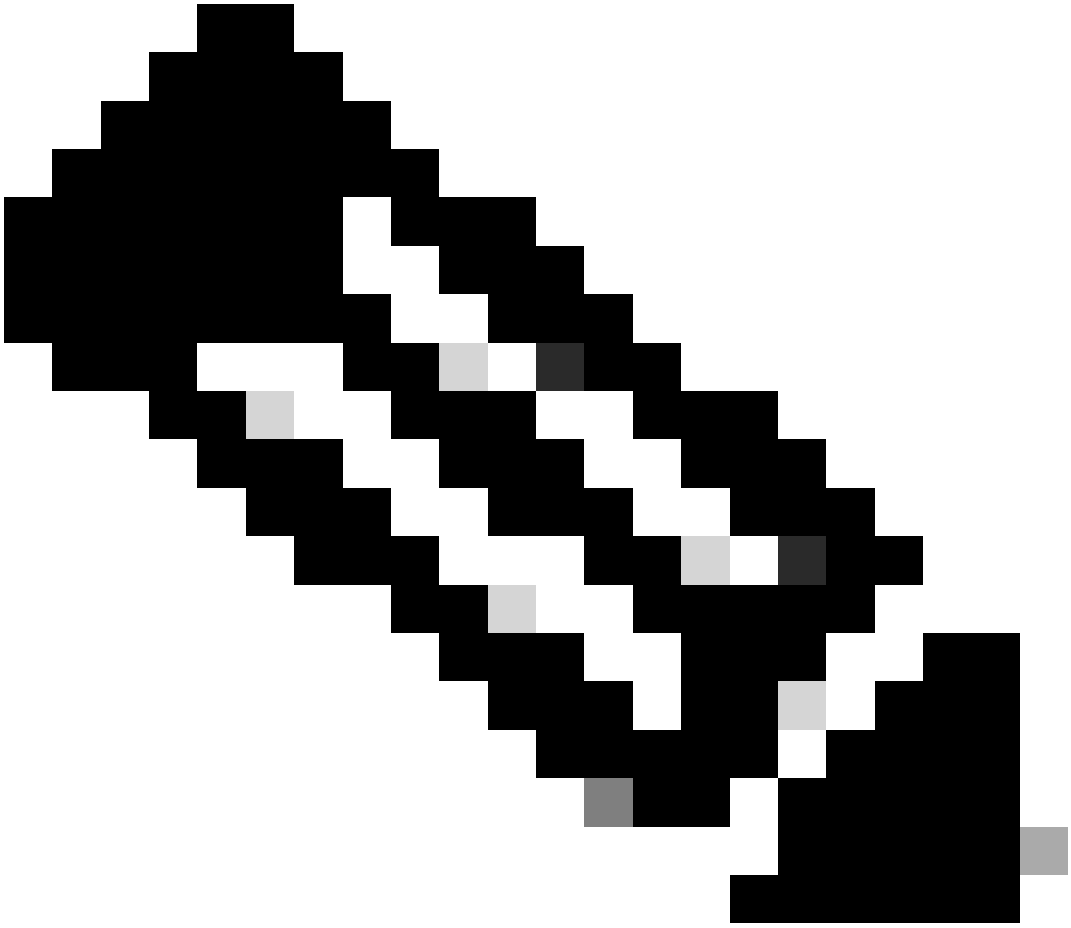
```
switch# install all force kickstart bootflash:[kickstart-image.bin] system bootflash:[system-image.bin]
```



Note: After the install all command completes its pre-checks, a Disruptive Upgrade is alerted with this message: Switch will be reloaded for disruptive upgrade. Do you want to continue with the installation (y/n)? [n]here type 'y' for the upgrade to continue.



Caution: Changing the boot variable is not a recommended way to upgrade or downgrade Cisco NX-OS, doing so can cause loss of configuration and system instability.



Note: For additional information about upgrade steps on Cisco Nexus 5500 and 5600 Series switches select the corresponding upgrade guide from Cisco Nexus 5X00 Series NX-OS Software Upgrade and Downgrade Guide and review the section **Upgrading Procedures.**

Related Documentation

Documentation for the Cisco Nexus 5500 and 5600 Series Switch is available at Cisco Nexus 5000 Series Switches.

The documentation set is divided into these categories:

- Release Notes
- Installation and Upgrade Guides
- Command References
- Configuration Guides
- Error and System Messages