

# Upgrading Catalyst 9400 Switches

## Contents

---

### [Introduction](#)

### [Prerequisites](#)

[Requirements](#)

[Components Used](#)

### [Background Information](#)

### [Recommended Releases](#)

### [Software Download](#)

### [Essential Criteria for Upgrade](#)

### [Common Upgrade OR Bootloader Upgrade](#)

### [CPLD Upgrade](#)

### [Upgrade Methods](#)

[Install Mode](#)

[Bundle Mode](#)

[In Service Software Upgrade \(ISSU\)](#)

[Prerequisites for ISSU](#)

[Steps To Upgrade](#)

[ISSU Validation Steps](#)

[Steps to Recover from ISSU Failure](#)

[Abort ISSU](#)

[Clean ISSU State](#)

---

## Introduction

This document describes the methods for upgrading Catalyst 9400 switches.

## Prerequisites

### Requirements

There are no specific requirements for this document.

### Components Used

The information in this document is based on C9400.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

## Background Information

This document covers upgrade procedures for Catalyst 9400 switches that use either BUNDLE or INSTALL

modes. ISSU is supported for C9400 High Availability Setup.

## Recommended Releases

For the recommended software versions based on the downloads page, please consult the following link:

[Recommended Releases for Catalyst 9000 Switches](#)

## Software Download

To download the software, please visit <https://software.cisco.com/download/home> and select your product.

## Essential Criteria for Upgrade

- A maintenance window of 2-3 hours should be sufficient for upgrading to the target version or rolling back to the previous version if any issues arise.
- Ensure you have a 4GB or 8GB USB drive with the .bin files of both the current and target IOS versions. The USB drive should be formatted in FAT32 to copy the IOS image.
- Verify that TFTP is set up with both the current and target IOS versions and is reachable to download these versions to the switch if needed.
- Confirm that console access to the device is available in case any issues occur.
- Ensure there is at least 1GB to 1.5GB of available space in the flash memory for the expansion of the new image. If there is insufficient space, remove old installation files.

## ROMMON Upgrade OR Bootloader Upgrade

ROMMON, also known as the boot loader, is firmware that runs when the device is powered up or reset. It initializes the processor hardware and boots the operating system software (Cisco IOS XE software image). The ROMMON is stored on the following Serial Peripheral Interface (SPI) flash devices on your switch:

- Primary: The ROMMON stored here is the one the system boots every time the device is powered-on or reset.
- Golden: The ROMMON stored here is a backup copy. If the one in the primary is corrupted, the system automatically boots the ROMMON in the golden SPI flash device.

ROMMON upgrades may be required to resolve firmware defects or to support new features, but there may not be new versions with every release.

To know the ROMMON or bootloader version that applies to every major and maintenance release, see these links.

[ROMMON and CPLD Versions for 17. x.x](#)

[ROMMON and CPLD Versions for 16. x.x](#)

You can upgrade the ROMMON before, or, after upgrading the software version. If a new ROMMON version is available for the software version you are upgrading to, proceed as follows:

- Upgrading the ROMMON in the primary SPI flash device

This ROMMON is upgraded automatically. When you upgrade from an existing release on your switch to a later or newer release for the first time, and there is a new ROMMON version in the new release, the system automatically upgrades the ROMMON in the primary SPI flash device, based on the hardware version of the switch.

- Upgrading the ROMMON in the golden SPI flash device

You must manually upgrade this ROMMON. Enter the `upgrade rom-monitor capsule golden switch` command in privileged EXEC mode.

#### Note:

- Golden ROMMON upgrade is only applicable to Cisco IOS XE Amsterdam 17.3.5 and later releases.
- Golden ROMMON upgrade will fail if the FPGA version is 17101705 or older. To upgrade the FPGA version, see [Upgrading the Complex Programmable Logic Device Version](#).
- In case of a Cisco StackWise Virtual setup, upgrade the active and standby supervisor modules.
- In case of a High Availability set up, upgrade the active and standby supervisor modules.

After the ROMMON is upgraded, it will take effect on the next reload. If you go back to an older release after this, the ROMMON is not downgraded. The updated ROMMON supports all previous releases.

## CPLD Upgrade

CPLD refers to hardware-programmable firmware. CPLD upgrades may be required to resolve firmware defects or to support new features, but there may not be new versions with every release. The CPLD version upgrade process must be completed after upgrading the software image.

The following links provide ROMMON and CPLD version information for the Cisco Catalyst 9400 Series Supervisor Modules.

[ROMMON and CPLD Versions for 17. x.x](#)

[ROMMON and CPLD Versions for 16. x.x](#)

You can trigger a CPLD version upgrade after upgrading the software image. During the CPLD upgrade, the supervisor module automatically power cycles. This completes the CPLD upgrade process for the supervisor module but also causes traffic disruption. Therefore, auto-upgrade of CPLD is not supported. You must manually perform CPLD upgrade.

[Upgrading the CPLD Version: High Availability Setup](#)

[Upgrading the CPLD Version: Cisco StackWise Virtual Setup](#)

[Upgrading the CPLD Version: Single Supervisor Module Setup](#)

## Upgrade Methods

This document covers upgrade procedures for the Catalyst 9400 switch that uses either BUNDLE or INSTALL modes.

## Install Mode

An install mode upgrade on a Cisco Catalyst 9400 switch is a method of upgrading the switch's software that involves using individual software packages rather than a single monolithic image file.

When upgrading to any newer version in INSTALL mode, the "install" commands are utilized.

Please follow the outlined steps for an upgrade in Install mode.

### 1. Cleanup

Remove any inactive installations with the command:

```
Switch#install remove inactive
```

### 2. Copying the New Image

Transfer the new .bin image file to the active switch's flash storage using one of the following methods:

Via TFTP:

```
Switch#copy tftp://Location/directory/<file_name> flash:
```

Via USB:

```
Switch#copy usbflash0:<file_name> flash:
```

Confirm the available file systems with:

```
Switch#show file systems
```

### 3. Verification

After transferring the IOS to the active switch, check if the image is correctly copied with:

```
Switch#dir flash:
```

(Optional) To verify the MD5 checksum, use the command:

```
Switch#verify /md5 flash:<file_name>
```

Make sure this checksum matches the one provided on the Software Download page.

#### 4. Setting the Boot Variable

Set the boot variable to point to the packages.conf file with the following commands:

```
Switch#configure terminal
```

```
Switch(config)#no boot system
```

```
Switch(config)#boot system flash:packages.conf
```

```
Switch(config)#end
```

#### 5. Autoboot Configuration

Configure the switch to autoboot by executing:

```
Switch#configure terminal
```

```
Switch(config)#no boot manual
```

```
Switch(config)#end
```

#### 6. Saving Configuration

Save your current configuration with:

```
Switch#write memory
```

Confirm the boot settings with the command:

```
Switch#show boot
```

#### 7. Installation of the Image

To install the image, use the command:

```
Switch#install add file flash:<file_name> activate commit
```

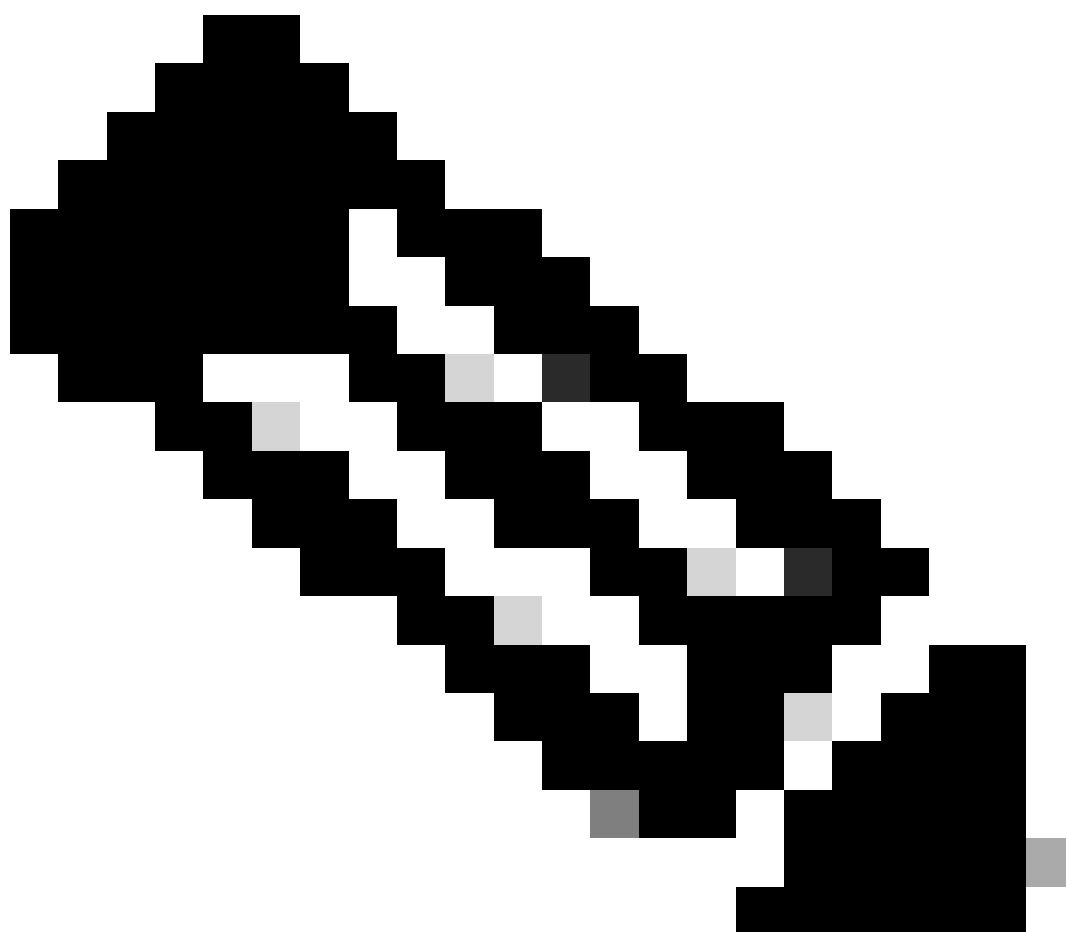
When prompted with "This operation requires a reload of the system. Do you want to proceed? [y/n]," respond with "y" to proceed.

## 8. Verification of the successful upgrade

```
Switch#show version
```

```
Switch#show redundancy (in case of High Availability setup)
```

---



**Note:** Replace with the actual name of your IOS image file throughout the steps.

---

## Bundle Mode

A bundle mode upgrade on a Cisco Catalyst 9400 switch refers to a method of upgrading the switch's software where the entire software image is bundled into a single file. This file includes all the necessary

components such as the operating system, device drivers, and other essential software required for the switch to operate. The upgrade involves a single software image file, typically with a .bin extension. This contrasts with other methods, such as install mode, which may involve multiple files and packages.

Please follow the outlined steps for an upgrade in Bundle mode.

1. Transfer the new image (.bin file) to the flash memory of each supervisor module installed (in case of dual sup or SVL) in the switch using one of these methods

•Via TFTP:

```
Switch#copy tftp://Location/directory/<file_name> bootflash:
```

```
Switch#copy tftp://Location/directory/<file_name> stby-bootflash:
```

Via USB:

```
Switch#copy usbflash0:<file_name> bootflash:
```

```
Switch#copy usbflash0:<file_name> stby-bootflash:
```

2. Confirm the available file systems by using the command

```
Switch#show file systems
```

3. After copying the IOS to all member switches, verify that the image has been correctly copied with

```
Switch#dir bootflash:
```

```
Switch#dir stby-bootflash:
```

4. (Optional) Verify the MD5 checksum with the command

```
Switch#verify /md5 bootflash:<file_name>
```

```
Switch#verify /md5 stby-bootflash:<file_name>
```

Ensure that the output matches the MD5 checksum value provided on the Software Download page.

5. Configure the boot variable to point to the new image file with these commands

```
Switch#configure terminal
```

```
Switch(config)#no boot system
```

```
Switch(config)#boot system bootflash:<file_name>.bin
```

```
Switch(config)#end
```

## 6. Save the configuration

```
Switch#write memory
```

## 7. Verify the boot settings using

```
Switch#show boot
```

## 8. Reload the switch to apply the new IOS

```
Switch#reload
```

## 9. Verification of the successful upgrade

```
Switch#show version
```

```
Switch#show redundancy (in case of High Availability setup)
```





**Note:** Replace with the actual name of your IOS image file throughout the steps.

---

## **In Service Software Upgrade (ISSU)**

In-Service Software Upgrade is a process that upgrades an image to another image on a device while the network continues to forward packets. ISSU helps network administrators avoid a network outage when they perform a software upgrade. The images are upgraded in install mode, wherein, each package is upgraded individually.

ISSU is supported on 9400 Stackwise-Virtual and also on 9400 stand-alone chassis with dual supervisors.

- For Catalyst 9400 with StackWise Virtual, ISSU support starts from Cisco IOS XE Fuji 16.9.2.
- For Catalyst 9400 in dual supervisor module configuration, ISSU support starts from Cisco IOS XE Fuji 16.9.1.

Please ensure the current SW version and Target SW version is suitable for ISSU upgrade using the link below :

[Compatibility Matrix](#)



**Note:** All upgrades from 16.9.x up to 16.9.5 in the 16.9 release train, and up to 16.12.2 in the 16.12 release train, require the installation of Software Maintenance Upgrade (SMU) packages. Upgrades from 16.9.5 and 16.12.2 to later releases do not require the installation of SMU packages.

---

## Prerequisites for ISSU

### 1. Check the Current Code Version

```
C9400#show version | include IOS XE
```

### 2. Check the Boot Mode

ISSU is supported only if both the switches in StackWise Virtual are booted in Install mode.

### 3. Check if There is Sufficient Available Memory on the Flash

```
C9400#dir flash: | include free
10527629312 bytes total (7523303424 bytes free)
```

```
C9400#dir stby-bootflash: | include free
11250098176 bytes total (8191942656 bytes free)
```

#### 4. Check if Switches are in SSO Mode

```
<#root>
```

```
C9400#show redundancy
Redundant System Information :
-----
Available system uptime = 4 hours, 29 minutes
Switchovers system experienced = 0
Standby failures = 0
Last switchover reason = none
```

```
Hardware Mode = Duplex
Configured Redundancy Mode = sso
Operating Redundancy Mode = sso
Maintenance Mode = Disabled
Communications = Up
```

```
Current Processor Information :
-----
Active Location = slot 1
Current Software state =
```

**ACTIVE**

```
<-----
```

```
Uptime in current state = 4 hours, 29 minutes
Image Version = Cisco IOS Software [Fuji], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 16.9.1, R
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Tue 17-Jul-18 17:00 by mcpre
BOOT = flash:packages.conf;
CONFIG_FILE =
Configuration register = 0x102
```

```
Peer Processor Information :
-----
Standby Location = slot 2
Current Software state =
```

**STANDBY HOT <-----**

```
Uptime in current state = 4 hours, 25 minutes
Image Version = Cisco IOS Software [Fuji], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 16.9.1, R
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Tue 17-Jul-18 17:00 by mcpre
BOOT = flash:packages.conf;
CONFIG_FILE =
Configuration register = 0x102
```

## 5. Check if Auto-Boot is Enabled

<#root>

```
C9400#show boot
BOOT variable = flash:packages.conf;
Configuration Register is 0x102
```

```
MANUAL_BOOT variable = no <-----
```

```
BAUD variable = 9600
ENABLE_BREAK variable = yes
BOOTMODE variable does not exist
IPXE_TIMEOUT variable does not exist
CONFIG_FILE variable =
```

```
Standby BOOT variable = flash:packages.conf;
Standby Configuration Register is 0x102
```

```
standby MANUAL_BOOT variable = no <-----
```

```
Standby BAUD variable = 9600
Standby ENABLE_BREAK variable = yes
Standby BOOTMODE variable does not exist
Standby IPXE_TIMEOUT variable does not exist
Standby CONFIG_FILE variable =
```

If Auto-Boot is not enabled, this can be changed as shown

```
C9400(config)#no boot manual
```

## 6. Check the Current ISSU and Install States

<#root>

```
C9400#show issu state detail
--- Starting local lock acquisition on chassis 1 ---
Finished local lock acquisition on chassis 1
```

```
No ISSU operation is in progress
```

```
<----- If anything else, abort ISSU before proceeding.
```

```
C9400#show install summary
[ Chassis 1 2 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
```

C - Activated & Committed

, D - Deactivated & Uncommitted

-----  
Type St Filename/Version  
-----

IMG C 16.9.1.0.70

<----- State should be Activated & Committed for current version alone. If not clear install state bef

-----  
Auto abort timer: inactive  
-----

## Steps To Upgrade

Please follow the outlined steps to perform an In-Service Software Upgrade (ISSU) upgrade.

### 1. Cleanup

Remove any inactive installations with the command:

```
Switch#install remove inactive
```

### 2. Copying the New Image

- Transfer the new .bin image file to the active supervisor's flash storage using one of the following methods:

- Via TFTP:

```
Switch#copy tftp://Location/directory/<file_name> flash:
```

- Via USB:

```
Switch#copy usbflash0:<file_name> flash:
```

- Confirm the available file systems with show file systems

### 3. Verification

After transferring the IOS to the active supervisor's flash, check if the image is correctly copied with:

```
Switch#dir flash:
```

(Optional) To verify the MD5 checksum, use the command:

```
Switch#verify /md5 flash:<File_name>
```

Make sure this checksum matches the one provided on the Software Download page.

#### 4. Setting the Boot Variable

Set the boot variable to point to the packages.conf file with the following commands:

```
Switch#configure terminal
Switch(config)#no boot system
Switch(config)#boot system flash:packages.conf
Switch(config)#end
```

#### 5. Autoboot Configuration

Configure the switch to autoboot by executing:

```
Switch#configure terminal
Switch(config)#no boot manual
Switch(config)#end
```

#### 6. Saving Configuration

Save your current configuration with:

```
Switch#write memory
```

Confirm the boot settings with the command:

```
Switch#show boot
```

#### 7. Installation of the Image

To install the image, use the command:

```
Switch#install add file flash:<file_name> activate issu commit
```

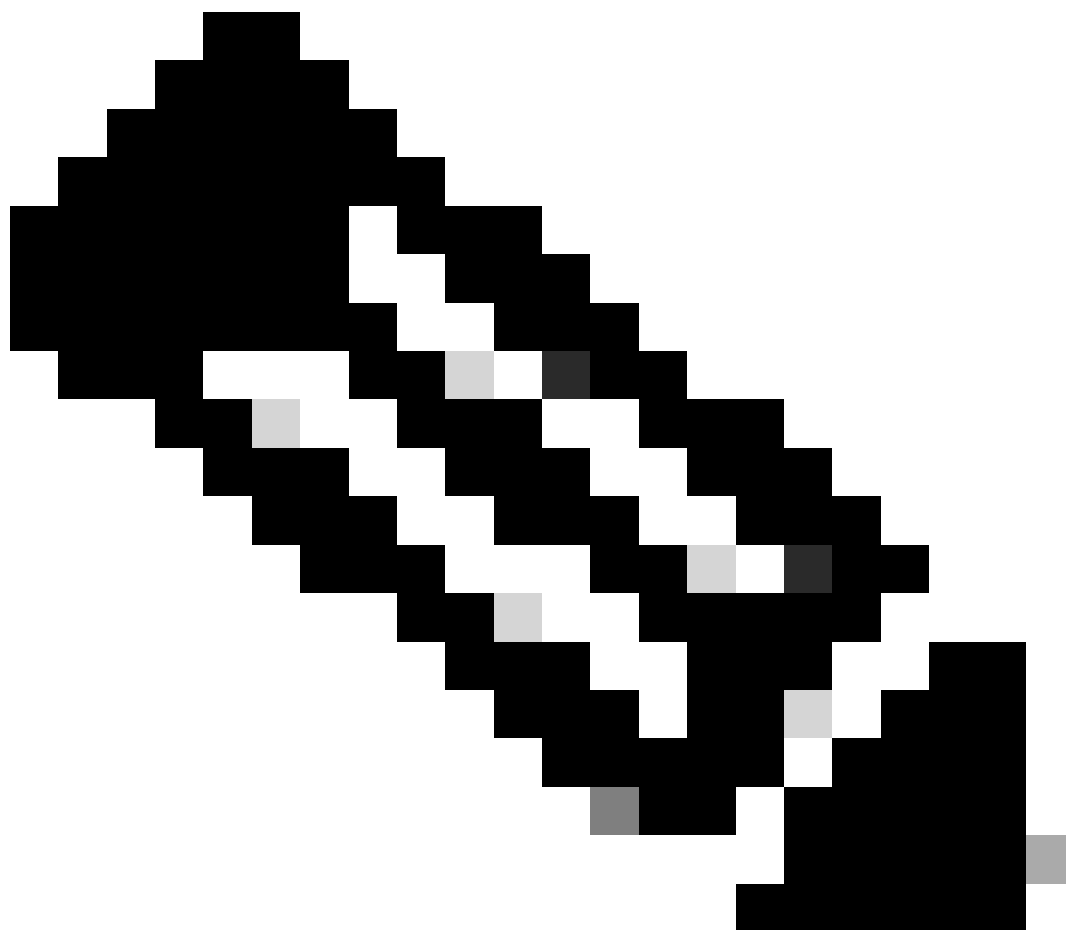
## 8. Verification of the successful upgrade

```
Switch#show version
```

```
Switch#show redundancy
```

Once you run the command noted here, the process starts and reloads sup automatically. Do not run the command until you are ready for sups to start to reboot. Unlike the normal upgrade process, it does not ask for confirmation from you before the reload happens.

Once you run this command, the ISSU process extracts the files, reloads the standby sup, waits for it to get back to SSO then failover reloads the active.



**Note:** Replace with the actual name of your IOS image file throughout the steps.

---

## ISSU Validation Steps

Once ISSU is completed,

- Check if both switches run on the new software.
- Check show issu state detail output to be clean and not showing any ISSU in progress.
- Check show install issu history output to ensure successful ISSU operation (Command available only with 16.10.1 release and later).

## Steps to Recover from ISSU Failure

- If ISSU fails, it is expected that auto-abort can recover the system back to its initial state (older image). However, if this fails as well, manual recovery of the chassis is expected.
- During manual recovery, check if both active and standby run the older image (if not, recover the individual chassis).
- After you ensure both chassis run the old image, run **install remove inactive** to remove any unused image packages.
- Once both chassis run the old software, manually clean all the internal states of ISSU operation. (Refer here on how to clean the internal ISSU states).

## Abort ISSU

In the 3-Step Work Flow, during the activate ISSU process, the system can auto-abort to the older image if the abort-timer expires. Manual abort is required if the standby does not reach SSO during abort. Also, if for any reason you wish to abort the ISSU in between, manual abort is required.

```
C9400#install abort issu
```

## Clean ISSU State

If ISSU upgrade/downgrade/abort/auto-abort is not successful, manual clean-up of ISSU internal states is required.

**\*\*Enable service internal before running the following command**

```
C9400#configure terminal
C9400(config)#service internal
C9400(config)#end
```

```
C9400#clear install state
clear_install_state: START Thu Jul 25 15:03:58 UTC 2024
```

This command will remove all the provisioned SMUs, and rollback points. Use this command with caution. A reload is required for this process. Press y to continue [y/n]y

```
--- Starting clear_install_state ---
Performing clear_install_state on all members
```

```
[1] clear_install_state package(s) on chassis 1
[1] Finished clear_install_state on chassis 1
[2] clear_install_state package(s) on chassis 2
```



```
[2] Finished clear_install_state on chassis 2  
Checking status of clear_install_state on [1 2]  
clear_install_state: Passed on [1 2]  
Finished clear_install_state
```

Install will reload the system now!