Upgrade Software on Catalyst 8000 Edge Platforms: A Quick Start Guide

Contents

Introduction

Background Information

Catalyst 8200/8300

- ROMMON Compatability Matrix 17.9.x Version
- ROMMON Compatability Matrix 17.12.x Version
- ROMMON Compatability Matrix 17.15.x and 17.18.x Version

Catalyst 8500

- ROMMON Compatability Matrix

Catalyst C8500L

- ROMMON Compatability Matrix

Catalyst 8000V

Catalyst 8000 Edge Platforms - Upgrade Steps

Cisco IOS XE Upgrade Steps

- Install Mode
  - One-Step Upgrade Process
  - Three-Step Upgrade Process
- ROMMON Manual Upgrade Steps
  - Dual-ROMMON Upgrade
- Important Notes
  - Weak ciphers deprecation

Introduction

This document describes the key considerations, known issues, and best practices when upgrading software on Cisco Catalyst 8000 Edge routers.

Background Information

This document includes specific ROMMON compatibility requirements for different versions of Cisco IOS® XE and step-by-step instructions for upgrading in both bundle and install mode.

Catalyst 8200/8300

On Catalyst 8200/8300 Edge series platforms the ROMMON package is integrated with Cisco IOS XE

software image.
During Cisco IOS XE upgrade process the ROMMON version check is performed and the **ROMMON image is automatically upgraded to the recommended version**, if needed.

ROMMON Compatability Matrix 17.9.x Version

Platforms	Cisco IOS XE	Minimum ROMMON	Recommended ROMMON
Catalyst 8300 Series			
C8300-1N1S-4T2X/6T	17.9.4+	17.3(1r)	17.6(6r)
C8300-2N2S-4T2X/6T	17.9.4+	17.3(1.2r)	17.7(1r)
Catalyst 8200 Series			
C8200-1N-4T	17.9.4+	17.4(1r)	17.6(6r)
C8200L-1N-4T	17.9.4+	17.5(1.1r)	17.6(6r)

ROMMON Compatability Matrix 17.12.x Version

Platforms	Cisco IOS XE	Minimum ROMMON	Recommended ROMMON
Catalyst 8300 Series			
C8300-1N1S-4T2X/6T	17.12.x	17.3(1r)	17.6(6r)
C8300-2N2S-4T2X/6T	17.12.x	17.3(1.2r)	17.7(1r)
Catalyst 8200 Series			
C8200-1N-4T	17.12.x	17.4(1r)	17.6(8.1r)

Platforms	Cisco IOS XE	Minimum ROMMON	Recommended ROMMON
C8200L-1N-4T	17.12.x	17.5(1.1r)	17.6(8.1r)

ROMMON Compatability Matrix 17.15.x and 17.18.x Version

Platforms	Cisco IOS XE	Minimum ROMMON	Recommended ROMMON
Catalyst 8300 Series			
C8300-1N1S-4T2X/6T	17.15.x | 17.18.x	17.3(4.2r)	17.9(7r) or 26.1(1r) for latest IOS XE versions
C8300-2N2S-4T2X/6T	17.15.x | 17.18.x	17.3(4.1r)	17.7(1r) or 26.1(1r) for latest IOS XE versions
Catalyst 8200 Series			
C8200-1N-4T	17.15.x | 17.18.x	17.6(8.1r)	17.6(8.1r) or 26.1(1r) for latest IOS XE versions
C8200L-1N-4T	17.15.x | 17.18.x	17.6(8.1r)	17.6(8.1r) or 26.1(1r) for latest IOS XE versions

---



Caution: For Cisco Catalyst 8200 and 8200L Series Edge platforms, if your ROMMON is at a version lower than 17.6(8.1r), the direct upgrade to Cisco IOS XE 17.15.x or 17.18.x is not recommended.

On Cisco Catalyst 8200 and 8200L Series Edge platforms you can upgrade the device to Cisco IOS XE 17.15.x or 17.18.x using any of the available methods:

- Bundle Mode:
    - Manually upgrade the device to Cisco IOS XE 17.12.5 or later rebuild. This triggers auto-upgrade of ROMMON to 17.6(8.1r). You can then upgrade the device to Cisco IOS XE 17.15.x or 17.18.x.
      Or
    - Manually upgrade the ROMMON to 17.6(8.1r). Then upgrade the device to Cisco IOS XE

17.15.x or 17.18.x.

- Install Mode:
  Upgrade the device to Cisco IOS XE 17.15.x or 17.18.x; the ROMMON is auto-upgraded to the recommended version when the device boots.

On Cisco Catalyst 8300 Series Edge platforms, if your ROMMON is at a version lower than the minimum supported version, manually upgrade the device first to Cisco IOS XE 17.12.5 or later rebuild. This triggers auto-upgrade of ROMMON to the recommended version. You can then upgrade the device to Cisco IOS XE 17.15.x or 17.18.x.

Catalyst 8500

On Catalyst 8500 Edge platforms, the ROMMON package is available for download and must be installed manually. **As opposed to other Catalyst 8000 Edge series platforms the ROMMON upgrade does not get triggered automatically when Cisco IOS XE upgrade is peformed.**

This is the example command to perform ROMMON upgrade:

upgrade rom-monitor filename bootflash:c8000aep-rommon.1711-1r.SPA.pkg

ROMMON Compatability Matrix

Platforms	Cisco IOS XE	DRAM	Minimum ROMMON	Recommended ROMMON
C8500-12X4QC C8500-12X	17.9.x/17.12.x/17.15.x/17.18.x	16GB (default) 32GB	17.2(1r)	17.11(1r)
C8500-12X4QC C8500-12X	17.9.x/17.12.x/17.15.x/17.18.x	64GB	17.3(2r)	17.11(1r)
C8500-20X6C	17.9.x/17.12.x/17.15.x/17.18.x	All variants	17.10(1r)	17.15(1r) Important: After installing ROMMON 17.15.(1r) downgrading to a lower ROMMON version is not supported.

Note: Cisco IOS XE 17.12.5a introduces support to update FPGA software for C8500-20x6C devices that use WAN MACsec for encrypting traffic across WAN networks. For information on how to upgrade FPGA for C8500-20x6C consult the reference link.

Note: ROMMON 17.15(1r) has minor fixes that do not affect functionality. It is programmed by default on newer C8500-20X6C systems shipped from factory. Existing systems can be updated but it is not mandatory.

Note: ROMMON 17.15(1r) cannot be downgraded to earlier versions.

Catalyst C8500L

On Catalyst 8500L Edge series platforms the ROMMON package is integrated with Cisco IOS XE software bundle.
During Cisco IOS XE upgrade process the ROMMON version check is performed and the **ROMMON image is automatically upgraded to the recommended version, if needed.**

ROMMON Compatability Matrix

Platforms	Cisco IOS XE	Minimum ROMMON	Recommended ROMMON
C8500L-8S4X	17.9.x/17.12.x	17.10(1r)	17.10(1r)
C8500L-8S4X	17.15.x/17.18.x	17.10(1r)	17.14(1r)

Note: ROMMON 17.14(1r) is only available from Cisco IOS XE 17.15.1a onwards. It provides software fixes for Cisco bug IDs CSCwf98337 and CSCwe21026.

Catalyst 8000V

Although the upgrade process regarding physical and virtual appliances is very similar, there are a few aspects that must be taken into account before proceeding. The primary distinction arises from the fact that C8000V operates within a virtual environment and does not depend on hardware-based ROMMON which means that this component does not need to be factored into the upgrade process. However, there are certain

prerequisites and restrictions that have been captured in the product documentation:

Prerequisites and restrictions for upgrading Cisco Catalyst 8000V

Catalyst 8000 Edge Platforms - Upgrade Steps

The upgrade steps depend on whether the device is supposed to operate in Install or Bundle mode.

In bundle mode, the device is booted from a consolidated **.bin** image.

In Install mode, the system expands the **.bin** into individual package files and boots from a single **packages.conf** file. This allows for:
– Faster reload
– More optimal memory usage
– Automatic image-sync of newly inserted FRU modules
– Activation/deactivation of Software Maintenance Upgrade (SMU) or security hot-patches without a full software upgrade

From Cisco IOS XE Cupertino 17.7.1a, Cisco Catalyst 8000 Edge platforms are shipped in install mode by default. Users can boot the platform, and upgrade or downgrade to Cisco IOS XE software versions using a set of install commands.

In the upcoming Cisco IOS XE versions, Bundle mode is going to be discontinued (see: https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-xe-17/ios-xe-bundle-boot-pb.html).

Therefore:

1. If upgrading from Cisco IOS XE 17.6 and earlier, use Bundle mode.
2. If upgrading from Cisco IOS XE 17.7 onwards, it is recommened that you use Install mode.

Cisco IOS XE Upgrade Steps

Bundle Mode

Step 1. Execute the copy command on your device in order to create a backup of the configuration:

```
Device# copy running-config bootflash:backup
```

Step 2. Proceed with upgrading the Cisco IOS XE version of the device:

```
Device(config)# no boot system
Device(config)# boot system flash location:[new_image_file.bin]
Device(config)# boot system flash location:[old_image_file.bin]     // this works as a backup
```

Step 3. Once finished, save changes, and reload the router:

```
Device# write memory
Device# reload
```

Step 4. After reloading the device verify the new Cisco IOS XE version was loaded:

```
Device# show version
```

Install Mode

If the platform is working in bundle mode, the one-step install procedure must be used to initially convert the platform from bundle mode to install mode. Subsequent installs and upgrades on the platform can be done with either one-step or three-step variants.

One-Step Upgrade Process

The software install package is copied from a local or remote location to the platform and the individual components of the **.package** file are extracted into subpackages and **packages.conf** files. The system also performs a validation and compatibility check for the platform and image versions, activates the package, and commits the package to make it persistent across reloads.

```
Device# install add file [location]:[new_image_file.bin] activate commit
```

Three-Step Upgrade Process

1. Execute the install add command.

```
Device# install add file [location]:[new_image_file.bin]
```

The system prompts a question regarding saving the configuration.

2. Execute the install activate command.

```
Device# install activate [auto-abort-timer {time}]
```

The system prompts a questions regarding reloading the system. The system then reloads. The install activate command performs the required validations and provisions the packages added earlier using the **install add** command. It also triggers a system reload. The auto-abort-timer starts automatically with the **install activate** command; the default for the timer is 120 minutes. If the **install commit** command is not run before the timer expires, the install process is automatically terminated. The platform reloads and boots up with the last committed version.

3. (Optional) If necessary, terminate the software install activation and return the platform to the last committed version. Use this command only when the image is in the activated state and not when the image is in the committed state.

```
Device# install abort
```

4. After the device reboots, execute the final command. The **install commit** command confirms the packages activated earlier using the **install activate** command, and makes the updates persistent over reloads.

```
Device# install commit
```

5. (Optional) If required, roll back the platform to the last committed state.

```
Device# install rollback to commited
```

6. (Optional) Display the information about the current state of the system.

```
Device# show install summary
```

ROMMON Manual Upgrade Steps

In specific cases where you need to upgrade the ROMMON to a specific version rather than the one already

bundled with the Cisco IOS XE image, these are the steps to observe:

1. Check the existing version of ROMMON. If you are installing Cisco IOS XE software on a new device, skip this step.

```
Device# show rom-monitor r0
```

2. Review minimum and recommended ROMMON releases in order to identify the recommended version of ROMMON software for the device you plan to upgrade.

3. Navigate to Cisco Software Download Page and download the ROMMON package file.

4. Copy the ROMMON file to the device.

5. Upgrade ROMMON package using the command:

```
Device# upgrade rom-monitor filename bootflash:[rommon-package-name] all
```

6. Reload the device to complete the ROMMON upgrade process.

7. Ensure the ROMMON software is upgraded.

```
Device# show rom-monitor r0
```

Dual-ROMMON Upgrade

Certain platforms are equipped with two ROMMON partitions. In such cases, the routers utilize a 'ping-pong' upgrade mechanism. During this process, the device first upgrades the active ROMMON partition. Once the upgrade is successfully completed, the system designates the other ROMMON partition as active. This change is then stored in NVRAM after the device successfully boots into the Cisco IOS.

After the device has fully booted, the upgrade process must be repeated to update the second ROMMON partition. This ensures that the ROMMON partition upgraded earlier can once again be set as the active partition, completing the upgrade cycle for both partitions.

Important Notes

Weak ciphers deprecation

Starting with Cisco IOS XE 17.11.1a, as part of security hardening and deprecation of weak ciphers, the options to configure DES, 3DES, MD5, and Diffie-Hellman (DH) groups 1, 2, and 5 are deprecated and are no longer supported. Instead, use AES, SHA, and DH Groups 14 or higher. Additionally, the esp-gmac transforms are also deprecated.

If you want to continue using the weak ciphers until migration to the more secure setting is performed, disable CSDL compliance on the device using the ***crypto engine compliance shield disable*** command and reboot.