

BIOS Protection

- Feature history for BIOS protection, on page 1
- BIOS protection, on page 1
- Primary ROMMON and golden ROMMON, on page 2
- Upgrade on standalone, high availability, and SVL devices, on page 2
- Capsule upgrade, on page 2
- LMS-signed bootloader, on page 3

Feature history for BIOS protection

This table provides release and platform support information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature name and description	Supported platform
Cisco IOS XE 26.2.1ea	BIOS protection: BIOS protection feature support has been introduced.	Cisco C9550 Series Smart Switches
Cisco IOS XE 26.1.1a	LMS-signed bootloader: The device supports secure boot process based on LMS PQC algorithm.	Cisco C9610 Series Smart Switches
Cisco IOS XE 17.18.1	BIOS protection: This feature provides write-protection for the golden ROMMON image and ensures that any upgrades to this image are performed securely.	Cisco C9350 Series Smart Switches Cisco C9610 Series Smart Switches

BIOS protection

The BIOS protection feature provides write-protection for the golden ROMMON image and ensures that any upgrades to this image are performed securely.

Without the BIOS protection feature, the golden ROMMON image is vulnerable to corruption by malicious code during software upgrades.

Primary ROMMON and golden ROMMON

ROMMON images are stored on the SPI flash device as both primary ROMMON and golden ROMMON.

The primary ROMMON is used to boot the device each time it is powered on or restarted. If the primary ROMMON becomes corrupted, the device automatically uses the golden ROMMON to boot the IOS XE software image.

When the device boots from the primary ROMMON, the golden ROMMON remains locked.

With the BIOS protection feature enabled, the golden ROMMON is write-protected and cannot be upgraded using the standard flash utility upgrade mechanism. Access policies for the golden ROMMON are enforced by the FPGA firmware, which blocks unauthorized operations such as write and erase commands on the golden ROMMON SPI flash device.



Note Golden ROMMON upgrade becomes available only after a secure boot FPGA upgrade.

Upgrade on standalone, high availability, and SVL devices

The upgrade process varies between standalone, high availability, and SVL devices. This table explains how the upgrade process works.

Table 1: Upgrade on standalone, high availability, and SVL devices

Device configuration	Upgrade process
Standalone device	When you upgrade in install mode, the primary ROMMON upgrades automatically when the device boots. To upgrade the golden ROMMON, use the capsule upgrade process.
High availability and StackWise Virtual devices	Perform an In-Service Software Upgrade (ISSU) for devices in a high availability setup. This ISSU process includes FPGA upgrades. If you upgrade in install mode with reload, reload one supervisor at a time. With the standby supervisor in the ROMMON state, boot the active supervisor first. After the ROMMON upgrade completes on the active supervisor, upgrade the FPGA and software image as well.

Capsule upgrade

The primary ROMMON, primary FPGA, and golden FPGA (secure-boot FPGA) are automatically upgraded when the device boots. In contrast, the golden ROMMON can only be upgraded using the capsule upgrade process, ensuring an additional layer of security for critical boot components.

In a capsule upgrade, a secure update capsule is created and digitally signed, and is used by the primary ROMMON to upgrade the golden ROMMON after authentication. This process requires a secure flash certificate, which is generated using the product key and included in the primary ROMMON image to verify the authenticity of the update capsule. The capsule itself is created using the secure flash certificate along with a secure boot 32 MB flash image on the Cisco C9350 Series Smart Switches and 64 MB flash image on the Cisco C9610 Series Smart Switches, and is then signed to ensure the integrity and authenticity of the upgrade.

When the device boots, the primary ROMMON initiates the capsule upgrade process for the golden ROMMON. To manually perform a capsule upgrade for the golden ROMMON, use the **upgrade rom-monitor capsule golden** command on a switch or the **upgrade rom-monitor capsule golden switch** command on a switch stack in privileged EXEC mode.

How Capsule Upgrade works

Workflow

This section explains what happens during a capsule upgrade.

1. The device checks if secure-boot FPGA upgrade is enabled. If secure-boot FPGA upgrade is not enabled, the upgrade stops.
2. The device checks if bootloader protection is enabled. If bootloader protection is not enabled, a one-time upgrade of primary ROMMON, golden ROMMON, and primary FPGA is initiated.
3. If bootloader protection is already active, Cisco IOS XE copies the secure update capsule to bootflash and the device reboots.
4. When the device reboots, the system selects the secure update capsule to perform the upgrade.

LMS-signed bootloader

The device supports secure boot process based on Leighton-Micali Signature (LMS) Post-Quantum Cryptography (PQC) algorithm which is approved by National Institute of Standards and Technology (NIST). When the device boots up, the microloader residing in secure boot FPGA loads the bootloader (ROMMON) after verifying its authenticity.



Note Use the **show module** command to view the hardware version.