BIOS Protection

- BIOS protection, on page 1
- Primary ROMMON and golden ROMMON, on page 1
- Upgrade on standalone, high availability, and SVL devices, on page 2
- Capsule upgrade, on page 2

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 is not enabled without secure-boot FPGA upgrade.

Upgrade on standalone, high availability, and SVL devices

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

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

Device configuration	Upgrade process
Standalone device	Upgrading in install mode automatically upgrades the primary ROMMON when the device boots. The golden ROMMON, however, can only be upgraded using the capsule upgrade process.
High availability and StackWise Virtual devices	It is recommended to perform an In-Service Software Upgrade (ISSU) for devices configured in a high availability setup, as FPGA upgrades are included as part of the ISSU process. If you are upgrading in install mode with reload, avoid reloading both supervisors simultaneously. Instead, while the standby supervisor is in the ROMMON state, boot the active supervisor first. Once the ROMMON upgrade is completed on each supervisor, the FPGA and software image are also upgraded. Afterward, boot the standby supervisor and allow it to complete its upgrade and reach the standby hot state

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 16 MB flash image, 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 switch in privileged EXEC mode.

How Capsule Upgrade works

Workflow

The following details the process that occurs in a capsule upgrade:

1. The device checks if secure-boot FPGA upgrade is enabled. If not, the process exits.

2. The device checks if bootloader protection is enabled. If not, a one-time upgrade of primary ROMMON, golden ROMMON, and primary FPGA is initiated.
3. If bootloader protection is already active, IOS copies the secure update capsule to bootflash and the device reboots.
4. When the device reboots, secure update capsule is picked for performing the upgrade.