



Hardware Features

- [BIOS Protection on the Controller, on page 1](#)
- [USB disablement, on page 2](#)

BIOS Protection on the Controller

BIOS Protection enables you to protect and securely update BIOS flash for Intel-based platforms. If BIOS Protection is not used, the flash utility that stores the BIOS for an Intel platform is not write-protected. As a result, when BIOS updates are applied, malicious code also makes its way through.

By default, BIOS Protection works by bundling the flash containing the BIOS image, and by accepting updates only through the BIOS capsules that enable writing on the BIOS Flash.

BIOS or ROMMON Upgrade with BIOS Protection

To upgrade BIOS or ROMMON use the BIOS Protection feature as follows:

1. The new BIOS image capsule bundled together with the ROMMON binary is inserted into the media of the Cisco device by the ROMMON upgrade scripts.
2. The Cisco device is then reset for the new BIOS/ROMMON upgrade to take place.
3. On reset, the original BIOS detects the updated capsule and determines if the updated BIOS is available.
4. The original BIOS then verifies the digital signature of the BIOS capsule. If the signature is valid, the original BIOS will remove write-protection from the flash utility and update the SPI flash with the new BIOS image. If the BIOS capsule is invalid, the SPI flash is not updated.
5. After the new BIOS/ROMMON image is written to the SPI flash, the required regions of the SPI flash are once again write-protected.
6. After the card is reset, the updated BIOS is rebooted.
7. The capsule is deleted by BIOS.

Upgrading BIOS

Procedure

Use the **upgrade rom-monitor filename** command to update the BIOS capsule.

Example:

```
upgrade rom-monitor filename bootflash:capsule.pkg <slot>
```

Example

The following example shows you how to verify a BIOS Protection upgrade:

```
Device# upgrade rom-monitor filename bootflash:qwlc-rommon-capsule-p106.pkg all
Verifying the code signature of the ROMMON package...
Chassis model AIR-CT5540-K9 has a single rom-monitor.

Upgrade rom-monitor

Target copying rom-monitor image file

Secure update of the ROMMON image will occur after a reload.

8388608+0 records in
8388608 records out
8388608 bytes (8.4 MB, 8.0 MiB) copied, 11.9671 s, 701 kB/s
131072+0 records in
131072 records out
131072 bytes (131 kB, 128 KiB) copied, 0.414327 s, 316 kB/s
Copying ROMMON environment
8388608+0 records in
8388608 records out
8388608 bytes (8.4 MB, 8.0 MiB) copied, 31.1199 s, 270 kB/s
131072+0 records in
131072 records out
131072 bytes (131 kB, 128 KiB) copied, 2.44015 s, 53.7 kB/s
131072+0 records in
131072 records out
131072 bytes (131 kB, 128 KiB) copied, 2.43394 s, 53.9 kB/s
ROMMON upgrade complete.
To make the new ROMMON permanent, you must restart the RP.
Device#reload
```

USB disablement

USB ports are hardware interfaces on standalone or stacked devices that:

- can be disabled together using the `platform usb disable` command
- can be reenabled using the `no platform usb disable` command, and
- do not generate system messages when a USB device is inserted while the ports are disabled.

The `platform usb disable` command disables USB ports on the device, but it does not disable Bluetooth dongles connected to USB ports.

Disable USB (CLI)

Disable all USB ports on a standalone or stacked device.

Use this task when you want to prevent USB devices from being used on the device. When USB ports are disabled, the device does not generate system messages if a USB device is inserted.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Disable all the USB ports on the device.

Example:

```
Device(config)# [no] platform usb disable
```

Use the **no platform usb disable** command to reenable the USB ports.

All USB ports on the device are disabled. The device will not recognize or generate system messages for connected USB peripherals.

