Cisco IMC Firmware Management

This chapter includes the following sections:

Overview of Firmware

C-Series servers use Cisco-certified firmware that is specific to the C-Series server model that you are using. You can download new releases of the firmware for all supported server models from Cisco.com.

> ⚠️
>
> **Caution**   When you install the new BIOS firmware, it must be from the same software release as the Cisco IMC firmware that is running on the server. Do not install the new BIOS firmware until after you have activated the matching Cisco IMC firmware or the server will not boot.

To avoid potential problems, we strongly recommend that you use the Cisco Host Upgrade Utility (HUU), which upgrades the BIOS, Cisco IMC, and other firmware to compatible levels. For detailed information about this utility, see the *Cisco Host Upgrade Utility Guide* for the version of the HUU that goes with the Cisco IMC software release that you want to install. The HUU guides are available at the following URL: http://www.cisco.com/en/US/products/ps10493/products_user_guide_list.html.

If you want to update the firmware manually, you must update the Cisco IMC firmware first. The Cisco IMC firmware update process is divided into the following stages to minimize the amount of time that the server is offline:

- Installation—During this stage, Cisco IMC installs the selected Cisco IMC firmware in the nonactive, or backup, slot on the server.

- Activation—During this stage, Cisco IMC sets the nonactive firmware version as active, causing a disruption in service. When the server reboots, the firmware in the new active slot becomes the running version.

After you activate the Cisco IMC firmware, you can update the BIOS firmware. You must power off server during the entire BIOS update process, so the process is not divided into stages. Instead, you only need to enter one command and Cisco IMC installs and updates the BIOS firmware as quickly as possible. After the Cisco IMC finishes rebooting, the server can be powered on and returned to service.

Note You can either upgrade an older firmware version to a newer one, or downgrade a newer firmware version to an older one.

Cisco IMC in a secure mode ensures that all the firmware images prior to loading and execution are digitally signed and are verified for authenticity and integrity to protect the device from running tampered software.

Obtaining Firmware from Cisco

Procedure

Step 1 Navigate to http://www.cisco.com/.

Step 2 If you are not already logged in, click **Log In** at the top right-hand edge of the page and log in using your Cisco.com credentials.

Step 3 In the menu bar at the top, click **Support**.

Step 4 Click **All Downloads** in the roll down menu.

Step 5 If your server model is listed in the **Recently Used Products** list, click the server name. Otherwise, do the following:

a) In the left-hand box, click **Products**.

b) In the center box, click **Unified Computing and Servers**.

c) In the right-hand box, click **Cisco UCS C-Series Rack-Mount Standalone Server Software**.

d) In the right-hand box, click the server model whose software you want to download.

Step 6 Click the **Unified Computing System (UCS) Server Firmware** link.

Step 7 (Optional) Select a prior release from the menu bar on the left-hand side of the page.

Step 8 Click the **Download** button associated with the Cisco Host Upgrade Utility ISO for the selected release.

Step 9 Click **Accept License Agreement**.

Step 10 Save the ISO file to a local drive.
We recommend you upgrade the Cisco IMC and BIOS firmware on your server using this ISO file, which contains the Cisco Host Upgrade Utility. For detailed information about this utility, see the *Cisco Host Upgrade Utility Guide* for the version of the HUU that goes with the Cisco IMC software release that you want to install. The HUU guides are available at the following URL: http://www.cisco.com/en/US/products/ps10493/products_user_guide_list.html.

Step 11 (Optional) If you plan to upgrade the Cisco IMC and BIOS firmware manually, do the following:

a) From the ISO file, open the ZIP file containing the firmware installation files.
The ZIP file is on the top-level of the ISO file, and its name follows the format
ServerModel_ReleaseNumber`.ZIP`.

For example, `C240M3_1.4.4A.ZIP`.

You do not need to extract all of the files contained in this ZIP file. Instead, you only need to open it so that you can access the BIOS firmware installation CAP file and the ZIP file containing the Cisco IMC firmware installation BIN file.

b) From the *ServerModel_ReleaseNumber*`.ZIP` file, extract the BIOS firmware installation CAP file and save it to your local drive.
The CAP file is in the *ReleaseNumber*`/bios/cisco imc` folder, and its name follows the format
Server`-BIOS-`*Release-Number*`.CAP`.

For example, `1.4.4a/bios/cisco imc/C240-BIOS-1-4-4c-0.CAP`.

c) From the *ServerModel_ReleaseNumber*`.ZIP` file, open the ZIP file containing the Cisco IMC firmware installation files.
The ZIP file is in the *ReleaseNumber*`/cisco imc` folder and its name follows the format
server-model`-cisco imc-`*release*`.zip`.

For example, `1.4.4a/cisco imc/c240-m3-cisco imc.1.4.4a.zip`.

You do not need to extract all of the files contained in this zip file. Instead, you only need to open it so that you can access the Cisco IMC firmware installation BIN file.

d) From the *server-model*`-cisco imc-`*release*`.zip` file, extract the full Cisco IMC firmware installation BIN file and save it to your local drive.
The BIN file is in the *server-model*`-cisco imc-`*release* folder and its name follows the format
`upd-pkg-`*server-model*`-cisco imc.full.`*release*`.bin`.

For example, `c240-m3-cisco imc.1.4.4a/upd-pkg-c240-m3-cisco imc.full.1.4.4a.bin`.

Step 12 (Optional) If you plan to install the firmware from a remote server, copy the BIOS installation CAP file and the Cisco IMC installation BIN file to the remote server you want to use.
The remote server can be one of the following:

- TFTP
- FTP
- SFTP
- SCP
- HTTP

The server must have read permission for the destination folder on the remote server.

What to Do Next

Use the Cisco Host Upgrade Utility to upgrade all firmware on the server or manually install the Cisco IMC firmware on the server.

Introduction to Cisco IMC Secure Boot

About Cisco IMC Secure Mode

You can update Cisco IMC to the latest version using Host Upgrade Utility (HUU), web UI, or CLI. If you use HUU to upgrade Cisco IMC, you are prompted to enable secure boot mode. If you choose **Yes**, the system enters a secure mode and install the firmware twice. If you choose **No**, it enters a nonsecure mode. If you use either the web UI or CLI to upgrade Cisco IMC, you must upgrade to version 2.0(x). After you boot the system with version 2.0(x), it boots in a nonsecure mode by default. You must enable secure mode. when you enable secure mode, you are automatically reinstalling the firmware. In the web UI, the secure mode option is available as a checkbox within the Cisco IMC firmware update page. In the CLI, you can enable the secure mode by using the **update-secure** command.

During the first upgrade to Cisco IMC version 2.0, a warning message might display stating that some of the features and applications are not installed correctly and a second upgrade is required. We recommend that you perform the second upgrade with or without the secure boot option enabled to correctly install the Cisco IMC firmware version 2.0(x) in a secure mode. After the installation is complete, you must activate the image. After you boot your system with the secure boot option enabled, Cisco IMC remains in secure mode and you cannot disable it later on. If you do not activate the image and reinstall any other firmware images, Cisco IMC may become unresponsive.

After you install the firmware with the secure boot migration, you must activate the image before performing any other regular server-based tasks. If you do not activate this image, and if you reinstall any other firmware images, Cisco IMC might become unresponsive.

The secure boot is enabled only when the firmware installation is complete and you have activated the image.

Note   When Cisco IMC is in a secure mode, it means the following:

- Only signed Cisco IMC firmware images can be installed and booted on the device.

- Secure Cisco IMC mode cannot be disabled later on.

- Any Cisco IMC versions can be upgraded to the latest version directly.

- Cisco IMC firmware versions cannot be installed or booted prior to version 1.5(3x).

- Cisco IMC version 2.0 cannot be downgraded to version 1.4(x), 1.5, 1.5(2x), or 1.5(1), 1.5(2) or to any nonsecure firmware version.

Supported Cisco IMC Version When Downgrading from the Latest Version

The following table lists the Cisco IMC versions in a secure mode that can be downgraded to prior versions.

From Cisco IMC Version	To Cisco IMC Version	Possible
2.0(x)	Prior to 1.5(1)	Not possible
2.0(x)	1.5(3x) or later	Possible
2.0(x)	Prior to 1.5(3x)	Not possible

Note When the Cisco IMC verison you are using is in a nonsecure mode, you can downgrade Cisco IMC to any prior version.

Note If you use HUU to downgrade Cisco IMC versions prior to 1.5(4), you must first downgrade Cisco IMC and then downgrade other firmware. Activate the firmware and then downgrade the BIOS firmware.

Number of Updates Required for Cisco IMC Version 2.0

Supported Cisco IMC Version When Upgrading to the Latest Version

The following table lists the number of updates required for Cisco IMC to correctly install all the applications of the latest version.

From Cisco IMC Version	To a Nonsecure Cisco IMC Version 2.0(x)	To a Secure Cisco IMC Version 2.0
Prior to 1.5(2)	Double update	Double update
1.5(2)	Single update	Double update
1.5(3)	Single update	Double update
1.5(3x) or Later	Single update	Double update

Updating Cisco IMC in a Nonsecure Mode

You can upgrade Cisco IMC to the latest version in a nonsecure mode with all the latest feature and applications installed correctly. When you upgrade Cisco IMC to the latest version using the web UI or CLI, you might need to update the firmware twice manually depending upon the version you are using. See, Supported Cisco IMC Version when Upgrading to the Latest Version. If you use HUU to upgrade the Cisco IMC verison, it gets upgraded to the latest verison automatically.

Note If you are installing from a Cisco IMC version prior to 1.5(2x), the following message is displayed:

"Some of the Cisco IMC firmware components are not installed properly! Please reinstall Cisco IMC firmware version 2.0 or higher to recover".

Note If you are in the middle of (HUU) update, we recommend that you reconnect any KVM session to get the current status of the update.

When Cisco IMC runs in a nonsecure mode, it implies the following:

- Any signed or unsigned Cisco firmware images can be installed on the device.
- Any Cisco IMC versions can be upgraded to the latest version directly.
- Cisco IMC firmware versions can be installed or booted to any prior versions.

Installing the Cisco IMC Firmware from a Remote Server

Before You Begin

- Log in to the Cisco IMC GUI as a user with admin privileges.
- Obtain the Cisco Host Upgrade Utility ISO file from Cisco.com and extract the firmware installation files as described in .

Procedure

Step 1   In the **Navigation** pane, click the **Admin** tab.

Step 2   On the **Admin** tab, click **Firmware Management**.

Step 3   In the **Actions** area, click **Install Cisco IMC Firmware from Remote Server**.

Step 4   In the **Install Cisco IMC Firmware** dialog box, complete the following fields:

Name	Description

Install Cisco IMC Firmware from drop-down list	The remote server type. This can be one of the following:
	
	  • **TFTP Server**
	  • **FTP Server**
	  • **SFTP Server**
	  • **SCP Server**
	  • **HTTP Server**

TFTP Server IP/Hostname field	The IP address or hostname of the server on which the Cisco IMC firmware installation file resides. Depending on the setting in the **Install Cisco IMC Firmware from** drop-down list, the name of the field might vary.
Image Path and Filename field	The path and filename of the Cisco IMC firmware installation file on the remote server.

Name	Description
Enable Cisco IMC Secure Boot check box	If checked, enables secure mode for Cisco IMC. **Note** If checked, a confirmation dialog box appears with a message that if secure boot is enabled, only a signed Cisco IMC firmware image can be installed on the device. Also, any unsigned Cisco IMC firmware images or images of Cisco IMC versions prior to 1.5(3x) are not supported. If you want to continue Cisco IMC in a secure boot, choose **Ok** or **Cancel**. **Important** After you enable secure boot, you cannot disable it later on.
Install Firmware button	Reinstalls Cisco IMC firmware with the latest updates. If you install the firmware with Cisco IMC secure boot enabled, you must activate the firmware image. **Note** After installing the firmware with the Secure Boot migration, you must activate the image before performing any other regular server-based tasks. If you do not activate this image, and if you reinstall any other firmware images, Cisco IMC might become unresponsive. The secure boot is enabled only when the firmware installation is complete and you have activated the image.
Close button	Closes the dialog box without saving any changes made while the dialog box was open.

Step 5   Click **Install Firmware**.

What to Do Next

Activate the Cisco IMC firmware Immediately.

Installing the Cisco IMC Firmware Through the Browser

Before You Begin

- Log in to the Cisco IMC GUI as a user with admin privileges.

- Obtain the Cisco Host Upgrade Utility ISO file from Cisco.com and extract the firmware installation files as described in Obtaining Firmware from Cisco, on page 2.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Firmware Management**.

Step 3 In the **Actions** area, click **Install Cisco IMC Firmware through Browser Client**.

Step 4 In the **Install Firmware** dialog box, click **Browse** and use the **Choose File** dialog box to select the .bin file that you want to install.

Step 5 (Optional) Check the **Enable Cisco IMC Secure Boot** check box to enable secure mode for Cisco IMC.

    Note   This option is available only for Cisco IMC version 2.0 and later version.

            If checked, a confirmation dialog box appears with a message that if secure boot is enabled, you can install only signed Cisco IMC firmware images on the device. Also, any unsigned Cisco IMC firmware images or images of Cisco IMC versions prior to 1.5(3x) are not supported. If you want to continue Cisco IMC in a secure boot, choose **OK**. If you do not want to continue Cisco IMC in a secure boot, choose **Cancel**.

    Important   After you enable secure boot, you cannot disable it later, and Cisco IMC continues to be in secure mode.

Step 6 Click **Install Firmware**.

    Note   After installing the firmware with the Secure Boot migration, you must activate the image before performing any other regular server-based tasks. If you do not activate this image, and if you reinstall any other firmware images, Cisco IMC might become unresponsive.

The secure boot is enabled only when the firmware installation is complete and you have activated the image.

What to Do Next

Activate the Cisco IMC firmware immediately.

Activating Installed Cisco IMC Firmware

Before You Begin

Install the Cisco IMC firmware on the server.

    Important   While the activation is in progress, do not:

- Reset, power off, or shut down the server.
- Reboot or reset Cisco IMC.
- Activate any other firmware.
- Export technical support or configuration data.

Procedure

Step 1   In the **Navigation** pane, click the **Admin** tab.

Step 2   On the **Admin** tab, click **Firmware Management**.

Step 3   In the **Actions** area, click **Activate Cisco IMC Firmware**.
The **Activate Firmware** dialog box appears.

Step 4   In the **Activate Firmware** dialog box, choose the firmware image to activate.

Step 5   Click **Activate Firmware**.

Installing BIOS Firmware from a Remote Server

Note   This procedure is not available on some servers. For other BIOS installation methods, see the *Cisco UCS C-Series Rack-Mount Server BIOS Upgrade Guide* available at the following URL: http://www.cisco.com/en/US/docs/unified_computing/ucs/c/sw/bios/b_Upgrading_BIOS_Firmware.html.

Before You Begin

- Log in to the Cisco IMC GUI as a user with admin privileges.

- Activate the Cisco IMC firmware that goes with the BIOS version you want to install, as described in Activating Installed Cisco IMC Firmware, on page 8.

- Power off the server.

Caution   When you install the new BIOS firmware, it must be from the same software release as the Cisco IMC firmware that is running on the server. Do not install the new BIOS firmware until after you have activated the matching Cisco IMC firmware or the server will not boot.

To avoid potential problems, we strongly recommend that you use the Cisco Host Upgrade Utility (HUU), which upgrades the BIOS, Cisco IMC, and other firmware to compatible levels. For detailed information about this utility, see the *Cisco Host Upgrade Utility Guide* for the version of the HUU that goes with the Cisco IMC software release that you want to install. The HUU guides are available at the following URL: http://www.cisco.com/en/US/products/ps10493/products_user_guide_list.html.

Procedure

Step 1   In the **Navigation** pane, click the **Server** tab.

Step 2   On the **Server** tab, click **Summary**.

Step 3   In the **Server Status** area, verify that the **Power State** field says "Off". If it says "On", click **Power Off Server** in the **Actions** area and wait for the server to power off before continuing.

Step 4   In the **Navigation** pane, click the **Admin** tab.

Step 5   On the **Admin** tab, click **Firmware Management**.

Step 6   In the **Cisco IMC Firmware** area, make sure the firmware version shown in the **Running Version** field matches the BIOS firmware version you are installing.

>   **Important**   If the Cisco IMC firmware version does not match, activate the Cisco IMC firmware before continuing with this procedure or the server will not boot. For details, see Activating Installed Cisco IMC Firmware, on page 8.

Step 7   In the **Actions** area, click **Install BIOS Firmware from Remote Server**.

Step 8   In the **Install BIOS Firmware** dialog box, complete the following fields:

Name	Description
Install BIOS Firmware from drop-down list	The remote server type. This can be one of the following: • **TFTP Server** • **FTP Server** • **SFTP Server** • **SCP Server** • **HTTP Server**
Server IP/Hostname field	The IP address or hostname of the server on which the BIOS firmware installation file resides. Depending on the setting in the **Install BIOS Firmware from** drop-down list, the name of the field may vary.
Image Path and Filename field	The path and filename of the BIOS firmware installation file on the remote server.
Username	The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP.
Password	The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.

Step 9   Click **Install Firmware**.

Step 10   Watch the messages in the **Status** field in the **Last BIOS Firmware Install** area until the status changes to "Completed Successfully".

Step 11   Power on the server to complete the BIOS upgrade.

Installing BIOS Firmware Through the Browser

Note   This procedure is not available on some servers. For other BIOS installation methods, see the *Cisco UCS C-Series Rack-Mount Server BIOS Upgrade Guide* available at the following URL: http://www.cisco.com/en/US/docs/unified_computing/ucs/c/sw/bios/b_Upgrading_BIOS_Firmware.html.

Before You Begin

- Log in to the Cisco IMC GUI as a user with admin privileges.

- Activate the Cisco IMC firmware that goes with the BIOS version you want to install, as described in Activating Installed Cisco IMC Firmware, on page 8.

- Power off the server.

Caution   When you install the new BIOS firmware, it must be from the same software release as the Cisco IMC firmware that is running on the server. Do not install the new BIOS firmware until after you have activated the matching Cisco IMC firmware or the server will not boot.

To avoid potential problems, we strongly recommend that you use the Cisco Host Upgrade Utility (HUU), which upgrades the BIOS, Cisco IMC, and other firmware to compatible levels. For detailed information about this utility, see the *Cisco Host Upgrade Utility Guide* for the version of the HUU that goes with the Cisco IMC software release that you want to install. The HUU guides are available at the following URL: http://www.cisco.com/en/US/products/ps10493/products_user_guide_list.html.

Procedure

Step 1   In the **Navigation** pane, click the **Server** tab.

Step 2   On the **Server** tab, click **Summary**.

Step 3   In the **Server Status** area, verify that the **Power State** field says "Off". If it says "On", click **Power Off Server** in the **Actions** area and wait for the server to power off before continuing.

Step 4   In the **Navigation** pane, click the **Admin** tab.

Step 5   On the **Admin** tab, click **Firmware Management**.

Step 6   In the **Cisco IMC Firmware** area, make sure the firmware version shown in the **Running Version** field matches the BIOS firmware version you are installing.

Important   If the Cisco IMC firmware version does not match, activate the Cisco IMC firmware before continuing with this procedure or the server will not boot. For details, see Activating Installed Cisco IMC Firmware, on page 8.

Step 7 In the **Actions** area, click **Install BIOS Firmware through Browser Client**.

Step 8 In the **Install BIOS Firmware** dialog box, click **Browse** and use the **Choose File** dialog box to select the CAP file you want to install.

Step 9 Click **Install Firmware**.

Step 10 Watch the messages in the **Status** field in the **Last BIOS Firmware Install** area until the status changes to "Completed Successfully".

Step 11 Power on the server to complete the BIOS upgrade.