CIMC Firmware Management

This chapter includes the following sections:

Overview of Firmware

C-Series servers use Cisco-certified firmware 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 new BIOS firmware, it must be from the same software release as the CIMC firmware running on the server. Do not install new BIOS firmware until after you have activated the matching CIMC 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, CIMC, 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 CIMC 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 elect to update the firmware manually, you must update the CIMC firmware first. The CIMC firmware update process is divided into the following stages to minimize the amount of time the server will be offline:

- Installation. During this stage, CIMC installs the selected CIMC firmware in the non-active, or backup, slot on the server.

- Activation. During this stage, CIMC sets the non-active firmware version as active and reboots the server, causing a disruption in service. When the server reboots, the firmware in the new active slot becomes the running version.

After you activate the CIMC firmware, you can update the BIOS firmware. The server must be powered off during the entire BIOS update process, so the process is not divided into stages. Instead, you only need to issue a single command and CIMC installs and updates the BIOS firmware as quickly as possible. Once the CIMC 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.

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 CIMC 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 CIMC 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 CIMC 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 CIMC 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/cimc folder, and its name follows the format *Server*-BIOS-*Release-Number*.CAP.

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

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

For example, 1.4.4a/cimc/c240-m3-cimc.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 CIMC firmware installation BIN file.

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

For example, c240-m3-cimc.1.4.4a/upd-pkg-c240-m3-cimc.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 CIMC 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 CIMC firmware on the server.

Installing CIMC Firmware from a Remote Server

Before You Begin

- Log in to the CIMC CLI 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.

Note If you start an update while an update is already in process, both updates will fail.

Procedure

	Command or Action	**Purpose**
Step 1	Server# **scope cimc**	Enters the CIMC command mode.
Step 2	Server /cimc # **scope firmware**	Enters the CIMC firmware command mode.
Step 3	Server /cimc/firmware # **update** *protocol IP Address path*	Specifies the protocol, IP address of the remote server and the file path to the firmware file on the server. The protocol can be one of the following: • TFTP • FTP • SFTP • SCP • HTTP
Step 4	Server /cimc/firmware # **show detail**	(Optional) Displays the progress of the firmware update.

This example updates the CIMC firmware:

```
Server# scope cimc
Server /cimc # scope firmware
Server /cimc/firmware # update ftp 192.0.20.34 //test/dnld-ucs-k9-bundle.1.0.2h.bin
  <CR>  Press Enter key
Firmware update has started.
Please check the status using "show detail"
Server /cimc/firmware #
```

What to Do Next

Activate the new firmware.

Activating Installed CIMC Firmware

Before You Begin

Install the CIMC firmware on the server.

👉

Important While the activation is in progress, do not:

- Reset, power off, or shut down the server.

- Reboot or reset CIMC.

- Activate any other firmware.

- Export technical support or configuration data.

Procedure

	Command or Action	**Purpose**
Step 1	Server# **scope cimc**	Enters the CIMC command mode.
Step 2	Server /cimc # **scope firmware**	Enters the firmware command mode.
Step 3	Server /cimc/firmware # **show detail**	Displays the available firmware images and status.
Step 4	Server /cimc/firmware # **activate** [**1** | **2**]	Activates the selected image. If no image number is specified, the server activates the currently inactive image.
Step 5	At the prompt, enter y to activate the selected firmware image.	The BMC reboots, terminating all CLI and GUI sessions until the reboot completes.
Step 6	Log back into the CLI and repeat steps 1–3 to verify the activation.	(Optional)

This example activates firmware image 1 and then verifies the activation after the BMC reboots:

```
Server# scope cimc
Server /cimc # scope firmware
Server /cimc/firmware # show detail
Firmware Image Information:
    Update Stage: NONE
    Update Progress: 100
    Current FW Version: 1.3(3a)
    FW Image 1 Version: 1.4(3j)
    FW Image 1 State: BACKUP INACTIVATED
    FW Image 2 Version: 1.3(3a)
    FW Image 2 State: RUNNING ACTIVATED
    Boot-loader Version: 1.4(3.21).18

Server /cimc/firmware # activate 1
This operation will activate firmware 1 and reboot the BMC.
Continue?[y|N]y
.
.
 -- BMC reboot --
.
.
-- Log into CLI as Admin --

Server# scope cimc
```

```
Server /cimc # scope firmware
Server /cimc/firmware # show detail
Firmware Image Information:
    Update Stage: NONE
    Update Progress: 100
    Current FW Version: 1.4(3j)
    FW Image 1 Version: 1.4(3j)
    FW Image 1 State: RUNNING ACTIVATED
    FW Image 2 Version: 1.3(3a)
    FW Image 2 State: BACKUP INACTIVATED
    Boot-loader Version: 1.4(3.21).18
```

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 CIMC CLI as a user with admin privileges.

- Activate the CIMC firmware that goes with the BIOS version you want to install, as described in Activating Installed CIMC Firmware, on page 4.

- Power off the server.

Note If you start an update while an update is already in process, both updates will fail.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters the CIMC command mode.
Step 2	Server /cimc # **scope firmware**	Enters the firmware command mode.
Step 3	Server /cimc/firmware # **show detail**	Displays the available firmware images and status.
Step 4	Make sure the firmware version shown in the **Current FW Version** field matches the BIOS firmware version you are installing.	**Important** If the CIMC firmware version does not match, activate the CIMC firmware before continuing with this procedure or the server will not boot. For details, see Activating Installed CIMC Firmware, on page 4.
Step 5	Server /cimc/firmware # **top**	Returns to the server root level.
Step 6	Server# **scope bios**	Enters the BIOS command mode.

	Command or Action	Purpose
Step 7	Server /bios # **update** *protocol*	Specifies the protocol to be used. It can be TFTP, FTP, SFTP, SCP or HTTP.
Step 8	Server /bios # **update** *IP Address*	Specifies the IP address or the host name of the remote server.
Step 9	Server /bios # **update** *path*	Specifies the file path to the BIOS firmware file on the remote server.

This example updates the BIOS firmware to CIMC software release 1.4(3j):

```
Server# scope cimc
Server /cimc # scope firmware
Server /cimc/firmware # show detail
Firmware Image Information:
    Update Stage: NONE
    Update Progress: 100
    Current FW Version: 1.4(3j)
    FW Image 1 Version: 1.4(3j)
    FW Image 1 State: RUNNING ACTIVATED
    FW Image 2 Version: 1.3(3a)
    FW Image 2 State: BACKUP INACTIVATED
    Boot-loader Version: 1.4(3.21).18
Server /cimc/firmware # top
Server # scope bios
Server /bios # update ftp 192.0.20.34 //upgrade_bios_files/C260-BIOS-1-4-3j-0.CAP
 <CR>  Press Enter key
Firmware update has started.
Please check the status using "show detail"
Server /bios #
```