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.

Note

- You can either upgrade an older firmware version to a newer one, or downgrade a newer firmware version to an older one.
- This procedure only applies to the Cisco UCS C-Series server running on Stand-Alone mode. Contact Cisco Technical Assistance Center to upgrade firmware for UCS C-Series running on Cisco UCS Manager integrated mode.

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:

Beginning with Release 3.0, the BIOS and Cisco IMC firmware files are no longer embedded inside the HUU as a standalone .zip file. BIOS and Cisco IMC firmware must now be extracted using the **getfw** utility, which is available in the GETFW folder of the HUU. Perform the following steps to extract the BIOS or Cisco IMC firmware files:

Note To perform this:

- Openssl must be installed in the target system.
- Squashfs kernel module must be loaded in the target system.

Viewing the GETFW help menu:

```
[root@RHEL65-***** tmp]# cd GETFW/
[root@RHEL65-***** GETFW]# ./getfw -h
Help:
  Usage: getfw {-b -c -C -H -S -V -h} [-s SRC] [-d DEST]
    -b      : Get BIOS Firmware
    -c      : Get CIMC Firmware
    -C      : Get CMC Firmware
    -H      : Get HDD Firmware
    -S      : Get SAS Firmware
    -V      : Get VIC Firmware
    -h      : Display Help
    -s SRC  : Source of HUU ISO image
    -d DEST : Destination to keep Firmware/s
  Note : Default BIOS & CIMC get extracted
```

Extracting the BIOS firmware:

```
[root@RHEL65-***** GETFW]# ./getfw -s /root/Desktop/HUU/ucs-c2xxx-huu-3.0.1c.iso -d /tmp/HUU
FW/s available at '/tmp/HUUucs-c2xxx-huu-3.0.1c'
[root@RHEL65-***** GETFW]# cd /tmp/HUU/
[root@RHEL65-***** HUU]# cd ucs-c2xxx-huu-3.0.1c/
[root@RHEL65-***** ucs-c2xxx-huu-3.0.1c]# ls
bios  cimc
[root@RHEL65-***** ucs-c2xxx-huu-3.0.1c]# cd bios/
[root@RHEL65-***** bios]# ls
bios.cap
[root@RHEL65-***** bios]#
```

Extracting the CIMC firmware:

```
[root@RHEL65-***** GETFW]# ./getfw -s /root/Desktop/HUU/ucs-c2xxx-huu-3.0.1c.iso -d /tmp/HUU
FW/s available at '/tmp/HUUucs-c2xxx-huu-3.0.1c'
[root@RHEL65-***** GETFW]# cd /tmp/HUU/
[root@RHEL65-***** HUU]# cd ucs-c2xxx-huu-3.0.1c/
[root@RHEL65-***** ucs-c2xxx-huu-3.0.1c]# ls
bios  cimc
[root@RHEL65-***** ucs-c2xxx-huu-3.0.1c]# cd cimc/
[root@RHEL65-***** cimc]# ls
cimc.cap
[root@RHEL65-***** cimc]#
```

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.

Note The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type.

If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint.

The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.

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.

Installing Cisco IMC Firmware from a Remote Server

Before you begin

- Log in to the Cisco IMC as a user with admin privileges.
- Activate the Cisco IMC firmware that goes with the BIOS version you want to install, as described in the **Activating Installed Cisco IMC Firmware** section.
- Power off the server.

Note You must not initiate a Cisco IMC update when another Cisco IMC update is already in progress.

Procedure

	Command or Action	Purpose
Step 1	Server /server # **scope server** {**1** | **2**}	Enters server command mode of server 1 or 2.
Step 2	server /server # **scope bmc**	Enters bmc command mode.
Step 3	server /server/bmc # **scope firmware**	Enters the firmware command mode.

	Command or Action	Purpose
Step 4	server /server/bmc/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 **Note** The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type. If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
Step 5	(Optional) server /server/bmc/firmware # **show detail**	Displays the progress of the firmware update.

Example

This example shows how to update the Cisco IMC firmware:

```
server# scope server 1
server /server # scope bmc
server /server/bmc # scope firmware
server /server/bmc/firmware # update ftp 192.0.20.34 //test/dnld-ucs-k9-bundle.1.0.2h.bin
Firmware update has started.
Please check the status using "show detail"
server /server/bmc/firmware # show detail
Firmware Image Information:
     Update Stage: NONE
    Update Progress: 5
    Current FW Version: 2.0(6.56)
```

```
    FW Image 1 Version: 2.0(6.56)
    FW Image 1 State: RUNNING ACTIVATED
    FW Image 2 Version: 2.0(6.55)
    FW Image 2 State: BACKUP INACTIVATED
    Boot-loader Version: 2.0(6.56).36
    Secure Boot: ENABLED

server /server/bmc/firmware #
```

What to do next

Activate the new firmware.

Activating Installed Cisco IMC Firmware

Before you begin

Install the Cisco IMC firmware on the server.

Important p

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

	Command or Action	Purpose
Step 1	Server /server # **scope server** {**1** | **2**}	Enters server command mode of server 1 or 2.
Step 2	server /server # **scope bmc**	Enters bmc command mode.
Step 3	server /server/bmc # **scope firmware**	Enters the firmware command mode.
Step 4	Server /server/bmc/firmware # **show detail**	Displays the available firmware images and statuses.
Step 5	Server /server/bmc/firmware # **activate**	Activates the selected image. If no image number is specified, the server activates the currently inactive image.
Step 6	At the prompt, enter **y** to activate the selected firmware image.	The BMC reboots, terminating all CLI and GUI sessions until the reboot completes.

	Command or Action	Purpose
Step 7	(Optional) Log back into the CLI and repeat steps 1–4 to verify the activation.	

Example

This example activates firmware image 2 and then verifies the activation after the BMC reboots:

```
Server# scope server 1
Server/server# scope bmc
Server /server/bmc # scope firmware
Server /server/bmc/firmware # show detail
Firmware Image Information:
     Update Stage: NONE
    Update Progress: 100
    Current FW Version: 2.0(6.55)
    FW Image 1 Version: 2.0(6.56)
    FW Image 1 State: BACKUP INACTIVATED
    FW Image 2 Version: 2.0(6.55)
    FW Image 2 State: RUNNING ACTIVATED
    Boot-loader Version: 2.0(6.55).36
    Secure Boot: ENABLED


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

Server# scope server 1
Server/server# scope bmc
Server /server/bmc # scope firmware
Server /server/bmc/firmware # show detail
Firmware Image Information:
    Update Stage: NONE
    Update Progress: 100
    Current FW Version: 2.0(6.55)
    FW Image 1 Version: 2.0(6.56)
    FW Image 1 State: RUNNING ACTIVATED
    FW Image 2 Version: 2.0(6.55)
    FW Image 2 State: BACKUP INACTIVATED
    Boot-loader Version: 2.0(6.55).36
    Secure Boot: ENABLED
Server /server/bmc/firmware #
```

Installing BIOS Firmware from a Remote Server

Before you begin

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

- Activate the Cisco IMC firmware that goes with the BIOS version you want to install, as described in the **Activating Installed BIOS Firmware** section.
- Power off the server.

Note You must not initiate a BIOS update while another BIOS update is already in progress.

Procedure

	Command or Action	Purpose
Step 1	Server /server # **scope server** {**1** | **2**}	Enters server command mode of server 1 or 2.
Step 2	server /server # **scope bios**	Enters BIOS command mode.
Step 3	server /server/bios # **update** *protocol IP Address pathrecovery*	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 **Note** The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type. If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
Step 4	(Optional) server /server/bios # **show detail**	Displays the progress of the firmware update.

Example

This example updates the BIOS firmware to Cisco IMC software release 2.0(7c):

```
Server# scope server 1
Server /server# scope bios
Server /server/bios# show detail
BIOS:
    BIOS Version: server-name.2.0.7c.0.071620151216
    Backup BIOS Version: server-name.2.0.7c.0.071620151216
    Boot Order: (none)
    Boot Override Priority:
    FW Update/Recovery Status: None, OK
    UEFI Secure Boot: disabled
    Configured Boot Mode: Legacy
    Actual Boot Mode: Legacy
    Last Configured Boot Order Source: CIMC
Server /server/bios # update ftp 192.0.20.34 //upgrade_bios_files/C3620-BIOS-2-0-7c-0.CAP
 <CR>  Press Enter key
Firmware update has started.
Check the status using "show detail"
Server /bios #
```

Activating Installed BIOS Firmware

Before you begin

- Install the BIOS firmware on the server.
- Power off the host.

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

	Command or Action	Purpose
Step 1	Server /server # **scope server** {**1** | **2**}	Enters server command mode of server 1 or 2.
Step 2	server /server # **scope bios**	Enters BIOS command mode.
Step 3	Server /server/bios # **activate**	Activates the currently inactive image.

	Command or Action	Purpose
Step 4	At the prompt, enter **y** to activate the selected firmware image.	Initiates the activation.

Example

This example activates firmware and then verifies the activation:

```
Server# scope server 1
Server /server# scope bios
Server /server/bios# show detail
BIOS:
    BIOS Version: server-name.2.0.7c.0.071620151216
    Backup BIOS Version: server-name.2.0.7c.0.071620151216
    Boot Order: (none)
    Boot Override Priority:
    FW Update/Recovery Status: None, OK
    UEFI Secure Boot: disabled
    Configured Boot Mode: Legacy
    Actual Boot Mode: Legacy
    Last Configured Boot Order Source: CIMC

Server /server/bios # activate
This operation will activate "C240M4.2.0.2.66.071820142034" after next host power off
Continue?[y|N]

Server# scope server 1
Server /server# scope bios
Server /server/bios# show detail
BIOS:
    BIOS Version: server-name.2.0.7c.0.071620151216
    Backup BIOS Version: server-name.2.0.7c.0.071620151216
    Boot Order: (none)
    Boot Override Priority:
    FW Update/Recovery Status: None, OK
    UEFI Secure Boot: disabled
    Configured Boot Mode: Legacy
    Actual Boot Mode: Legacy
    Last Configured Boot Order Source: CIMC
```

Installing CMC Firmware from a Remote Server

Note You must not initiate a CMC update while another CMC update is already in progress.

Before you begin

- Log in to the Cisco IMC 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

	Command or Action	Purpose
Step 1	server # **scope chassis**	Enters chassis command mode.
Step 2	server /chassis # **scope cmc** *1|2*	Enters CMC on the chosen SIOC controller command mode.
Step 3	server /chassis/cmc # **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 **Note** The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type. If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
Step 4	(Optional) server /chassis/cmc # **show detail**	Displays the progress of the firmware update.

Example

This example shows how to update the CMC firmware:

```
server # scope chassis
server /chassis # scope cmc 1
server /chassis/cmc # update  http 10.104.236.99 colusa2_cmc.2.0.7a.img
CMC Firmware update initialized.
```

```
Please check the status using "show detail"
Server /chassis/cmc # show detail
Firmware Image Information:
    Name: CMC1
    Update Stage: DOWNLOAD
    Update Progress: 25
    Current FW Version: 2.0(7a)
    FW Image 1 Version: 2.0(7a)
    FW Image 1 State: RUNNING ACTIVATED
    FW Image 2 Version: 2.0(7a)
    FW Image 2 State: BACKUP INACTIVATED
server /chassis/cmc #
```

What to do next

Activate the new firmware.

Activating Installed CMC Firmware

Note CMCs are configured to have one in an active state while other acts as a backup, when you activate the backup CMC the previously active CMC changes to backup CMC activating the other.

Before you begin

Install the CMC 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.

- CMC-1 activation interrupts Cisco IMC network connectivity.

Procedure

	Command or Action	Purpose
Step 1	server # **scope chassis**	Enters chassis command mode.
Step 2	Server# **scope cmc***1*|*2*	Enters the CMC of the chosen SIOC slot command mode.
Step 3	Server /cmc # **activate**	Activates the selected image for the chosen CMC.

	Command or Action	Purpose
Step 4	At the prompt, enter **y** to activate the selected firmware image.	The CMC-1 reboots, terminating all CLI and GUI sessions until the reboot completes, but CMC-2 reboot will not affect any active sessions.

Example

This example activates CMC firmware on the SIOC slot 1:

```
Server # scope chassis
Server /chassis # scope cmc 1
Server /chassis/cmc #  activate
Warning: The CMC will be rebooted immediately to complete the activation.
The network may go down temporarily till CMC boots up again
Continue?[y|N]y
```

Managing SAS Expander and HDD Firmware

Updating and Activating SAS Expander Firmware

Procedure

	Command or Action	Purpose
Step 1	Server # **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **scope sas-expandersas expander ID**	Enters SAS expander mode.
Step 3	Server /chassis/sas-expander # **update** *protocol IP Address path*	Initiates the firmware update by specifying 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

	Command or Action	Purpose
		Note The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type. If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
Step 4	(Optional) Server /chassis/sas-expander # **show detail**	Displays the status of the firmware upgrade.

Example

This example shows how to update and activate the SAS expander firmware:

```
Server# scope chassis
Server /chassis # scope sas-expander 1
Updating the firmware
Server /chassis/sas-expander# update tftp 10.10.10.10 /tftpboot/skasargo/<firmware file>
updating the firmware.
Checking the status of the upgrade
Server /chassis/sas-expander# show detail
Firmware Image Information:
    ID: 1
    Name: SASEXP1
    Update Stage: In Progress
    Update Progress: 25
    Current FW Version: 04.08.01_B056
    FW Image 1 Version: 04.08.01_B056
    FW Image 1 State: RUNNING ACTIVATED
    FW Image 2 Version: 04.08.01_B056
    FW Image 2 State: BACKUP INACTIVATED

Activating the firmware
svbu-huu-sanity-col2-1-vcmc /chassis/sas-expander # activate
This operation will activate backup firmware and reboot the SAS-Expander.
Continue?[y|N]y

Server /chassis/sas-expander #
```

Updating HDD Firmware

Procedure

	Command or Action	Purpose
Step 1	Server # **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis/dynamic-storage # **scope dynamic-storage**	Enters dynamic storage command mode.
Step 3	Server /chassis/dynamic-storage # **update-drive** *protocol IP Address path HDD slot-ids*	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 **Note** The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type. If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to. **Note** You can update firmware for multiple servers from the same vendor.
Step 4	(Optional) Server /chassis/dynamic-storage # **show physical-drive-fw**	Displays the status of the firmware upgrade.

Example

This example provides steps to update the HDD firmware:

```
Server# scope chassis
Server /chassis # scope dynamic-storage
Updating for a single HDD
Server /chassis/dynamic-storage #update-drive tftp 10.10.10.10 /tftpboot/skasargo/sg4.lod
14
updating FW for slot 1 HDD
Updating for Multiple HDD
Server /chassis/dynamic-storage#update-drive tftp 10.10.10.10 /tftpboot/skasargo/sg4.lod
1-14
updating fw for multiple HDDs
Viewing the Status of the Upgrade
Server /chassis/dynamic-storage# show physical-drive-fw

Slot  Vendor    Product ID         Current_FW Update Stage Update Progress
----- --------- ------------------ ---------- ------------ --------------------
1     TOSHIBA   MG03SCA400         5702       Progress        25
2     TOSHIBA   MG03SCA400         5702       NONE            0
3     TOSHIBA   MG03SCA400         5702       NONE            0
4     TOSHIBA   MG03SCA400         5702       NONE            0
5     TOSHIBA   MG03SCA400         5702       NONE            0
6     TOSHIBA   MG03SCA400         5702       NONE            0
7     TOSHIBA   MG03SCA400         5702       NONE            0
8     TOSHIBA   MG03SCA400         5702       NONE            0
9     TOSHIBA   MG03SCA400         5702       NONE            0
10    TOSHIBA   MG03SCA400         5702       NONE            0
11    TOSHIBA   MG03SCA400         5702       NONE            0
12    TOSHIBA   MG03SCA400         5702       NONE            0
13    TOSHIBA   MG03SCA400         5702       NONE            0
14    TOSHIBA   MG03SCA400         5702       NONE            0
Server /chassis/dynamic-storage #
```