



Cisco IMC Firmware Management

This chapter includes the following sections:

- [Overview of Firmware, page 1](#)
- [Obtaining Firmware from Cisco, page 3](#)
- [Introduction to Cisco IMC Secure Boot, page 4](#)
- [Installing Cisco IMC Firmware from a Remote Server, page 7](#)
- [Activating Installed CIMC Firmware, page 9](#)
- [Installing BIOS Firmware from a Remote Server, page 11](#)
- [Activating Installed BIOS Firmware, page 12](#)
- [Installing CMC Firmware from a Remote Server, page 14](#)
- [Activating Installed CMC Firmware, page 15](#)
- [Installing SAS Expander Firmware from a Remote Server, page 16](#)
- [Activating Installed SAS Expander Firmware, page 17](#)
- [Installing SAS Expander Firmware from a Remote Server, page 18](#)
- [Activating Installed SAS Expander Firmware, page 20](#)

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.
 - 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:
- In the left-hand box, click **Products**.
 - In the center box, click **Unified Computing and Servers**.
 - In the right-hand box, click **Cisco UCS C-Series Rack-Mount Standalone Server Software**.
 - 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:
- 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.
 - 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`.
 - 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.

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.

Introduction to Cisco IMC Secure Boot

About Cisco IMC Secure Mode



Note

Cisco IMC secure boot mode is enabled by default only on some Cisco UCS C-Series servers.

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.

**Warning**

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	Possibility
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 version 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(1)



Important This section is valid for Cisco IMC version 2.0(1) and prior releases.

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(x)
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



Important This section is valid for Cisco IMC version 2.0(1) and prior releases.

You can upgrade Cisco IMC to the latest version in a nonsecure mode with all the latest features 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 version, it gets upgraded to the latest version automatically.



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

**Warning**

"Some of the Cisco IMC firmware components are not installed properly! Please reinstall Cisco IMC firmware version 2.0(1) or higher to recover".

**Note**

If you are in the middle of (HUU) update, we recommend that you reconnect any KVM session to 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 Cisco IMC Firmware from a Remote Server

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 3.

**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 Cisco IMC command mode.
Step 2	server /cimc # scope firmware	Enters Cisco IMC 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: <ul style="list-style-type: none"> • TFTP • FTP • SFTP • SCP • HTTP

	Command or Action	Purpose
		<p>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.</p> <p>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.</p> <p>The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.</p>
Step 4	<pre>server /cimc/firmware # update-secure protocol IP Address path</pre>	<p>(Optional) Migrates to the Cisco IMC secure boot option. Migration implies the following:</p> <ul style="list-style-type: none"> • You can install and boot only signed Cisco IMC firmware images on the server. • You cannot install and boot Cisco IMC firmware versions prior to 1.5(3x). • You cannot disable Secure Boot later on. <p>Important This action is available for Cisco IMC 2.0(1) version only. For later versions, it is enabled by default.</p> <p>Warning 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.</p> <p>For Cisco IMC version 2.0(1), the secure boot is enabled only when the firmware installation is complete and you have activated the image.</p>
Step 5	<pre>server /cimc /firmware # show detail</pre>	<p>(Optional) Displays the progress of the firmware update.</p>

This example shows how to update the Cisco IMC firmware and to migrate Cisco IMC from a nonsecure boot to secure boot for Cisco IMC version 2.0:

```
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
Firmware update has started.
Please check the status using "show detail"
Server /cimc /firmware # update-secure tftp 1.1.1.1 /cimc-pkg.bin
Migrating to Cisco IMC Secure Boot option implies:
-You can install and boot only signed Cisco IMC firmware images on the server.
-You cannot install and boot Cisco IMC firmware versions prior than 1.5(3x).
-You cannot disable Secure Boot later on.
```

After installing the firmware with the Secure Boot migration, you must activate the image before performing any other regular server-based tasks. The Secure Boot option is enabled only when the firmware installation is complete and you have activated the image.

```
Continue?[y|N]y
Update to Secure Boot selected, proceed with update.
Firmware update initialized.
Please check the status using "show detail".
server /cimc /firmware # show detail
Firmware Image Information:
  Update Stage: DOWNLOAD
  Update Progress: 5
  Current FW Version: 2.0(0.29)
  FW Image 1 Version: 2.0(0.28)
  FW Image 1 State: BACKUP INACTIVATED
  FW Image 2 Version: 2.0(0.29)
  FW Image 2 State: RUNNING ACTIVATED
  Boot-loader Version: 2.0(0.9).35
  Secure Boot: DISABLED
```

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

```
server /cimc /firmware #
```

This example shows how to update the Cisco IMC 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
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 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 [Activating Installed CIMC Firmware, on page 9](#).
- Power off the server.



Note For C220 M4, C240 M4 and C3160, you do not have to 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 Cisco IMC 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 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 CIMC Firmware, on page 9 .
Step 5	Server /cimc/firmware # top	Returns to the server root level.
Step 6	Server# scope bios	Enters the BIOS command mode.
Step 7	Server /bios # update protocol IP Address path	It specifies the following: <ul style="list-style-type: none"> • Protocol, it can be TFTP, FTP, SFTP, SCP or HTTP.

	Command or Action	Purpose
		<p>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.</p> <p>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.</p> <p>The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.</p> <ul style="list-style-type: none"> • The IPv4 or IPv6 address or the host name of the remote server. • The file path to the BIOS firmware file on the remote server.

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

```

Server# scope bios
Server /bios# show detail
BIOS:
  BIOS Version: C220M4.2.0.3.0.080720142114
  Backup BIOS Version: C220M4.2.0.2.68.073120141827
  Boot Order: (none)
  Boot Override Priority:
  FW Update/Recovery Status: None, OK
  UEFI Secure Boot: disabled
  Configured Boot Mode: None
  Actual Boot Mode: Unknown
  Last Configured Boot Order Source: UNKNOWN
Server /bios # update ftp 192.0.20.34 //upgrade_bios_files/C220-BIOS-1-4-3j-0.CAP
<CR> Press Enter key
Firmware update has started.
Please check the status using "show detail"
Server /bios #

```

Activating Installed BIOS Firmware



Note

Activate BIOS Firmware (activate) option is available only for some C-Series servers. For servers that do not have the this option, rebooting the server activates the 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# scope bios	Enters the BIOS command mode.
Step 2	Server /bios # show detail	Displays the available firmware images and status.
Step 3	Server /bios # activate	Activates the currently inactive image.
Step 4	At the prompt, enter y to activate the selected firmware image.	

This example activates firmware and then verifies the activation:

```
Server# scope bios
Server /bios # show detail
BIOS
  Version: C240M4.2.0.2.67.072320142231
  Backup BIOS Version: C240M4.2.0.2.66.071820142034
  Boot Order: (none)
  Boot Override Priority:
  FW Update/Recovery Status: None, OK
  UEFI Secure Boot: disabled
  Configured Boot Mode: None
  Actual Boot Mode: Legacy
  Last Configured Boot Order Source: BIOS

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

Server# scope bios
Server /bios # show detail
BIOS
  Version: C240M4.2.0.2.66.071820142034
  Backup BIOS Version: C240M4.2.0.2.67.072320142231
  Boot Order: (none)
  Boot Override Priority:
  FW Update/Recovery Status: None, OK
  UEFI Secure Boot: disabled
  Configured Boot Mode: None
  Actual Boot Mode: Legacy
  Last Configured Boot Order Source: BIOS
```

Installing CMC Firmware from a Remote Server

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 3.
- This action is available only on some C-Series servers.



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 chassis	Enters chassis command mode.
Step 2	server /chassis # scope cmc <i>l 2</i>	Enters CMC on the chosen SIOC controller command mode.
Step 3	server /chassis/cmc # update protocol IP <i>Address path</i>	<p>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:</p> <ul style="list-style-type: none"> • TFTP • FTP • SFTP • SCP • HTTP <p>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.</p> <p>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.</p> <p>The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.</p>

	Command or Action	Purpose
Step 4	<code>server /chassis/cmc # show detail</code>	(Optional) Displays the progress of the firmware update.

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 colusa_cmc.2.0.2a.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(2a)
  FW Image 1 Version: 2.0(2a)
  FW Image 1 State: RUNNING ACTIVATED
  FW Image 2 Version: 2.0(2a)
  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 /2	Enters the CMC of the chosen SIOC slot command mode.
Step 3	Server /cmc # activate	Activates the selected image for the chosen CMC.
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.

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
```

Installing SAS Expander Firmware from a Remote Server

Before You Begin

- You must be logged in as admin to perform this action.
- Server must be powered on.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope sas-expander {1 2}	Enters the SAS expander command mode.
Step 3	Server /chassis/sas-expander # show detail	Displays the available firmware images and status.
Step 4	Server /chassis/sas-expander # update protocol <i>IP_Address path</i>	It specifies the following: <ul style="list-style-type: none"> • Protocol, it can be TFTP, FTP, SFTP, SCP or HTTP.

	Command or Action	Purpose
		<p>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.</p> <p>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.</p> <p>The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.</p> <ul style="list-style-type: none"> • The IPv4 or IPv6 address or the host name of the remote server. • The file path to the SAS expander firmware file on the remote server.

This example updates the SAS expander firmware:

```

Server# scope chassis
Server /chassis # scope sas-expander 1
Server /chassis/sas-expander # show detail
Firmware Image Information:
  ID: 1
  Name: SASEXP1
  Update Stage: NONE
  Update Progress: 0
  Current FW Version: 65103900
  FW Image 1 Version: 65103900
  FW Image 1 State: RUNNING ACTIVATED
  FW Image 2 Version: 65103900
  FW Image 2 State: BACKUP INACTIVATED
Server /chassis/sas-expander # update ftp 192.0.20.34
//upgrade_sas_expander_files/sas-expander-2-0-12a.fw
<CR> Press Enter key
Firmware update has started.
Please check the status using "show detail"
Server /chassis/sas-expander #

```

Activating Installed SAS Expander Firmware

Before You Begin

- You must be logged in as admin to perform this action.
- Install the firmware on the expander.
- Host must be powered on.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope sas-expander {1 2}	Enters the SAS expander command mode.
Step 3	Server /chassis/sas-expander # activate	Activates the currently inactive image.
Step 4	At the prompt, enter y to activate the selected firmware image.	

This example activates firmware and then verifies the activation:

```
Server# scope chassis
Server /chassis # scope sas-expander 1
Server /chassis/sas-expander # show detail
ID: 1
  Name: SASEXP1
  Update Stage: NONE
  Update Progress: 0
  Current FW Version: 65103900
  FW Image 1 Version: 65103900
  FW Image 1 State: RUNNING INACTIVATED
  FW Image 2 Version: 65103900
  FW Image 2 State: BACKUP INACTIVATED

Server /chassis/sas-expander # activate
This operation will activate "65103900" after next host power off
Continue?[y|N] y

Server /chassis/sas-expander # show detail
ID: 1
  Name: SASEXP1
  Update Stage: NONE
  Update Progress: 0
  Current FW Version: 65103900
  FW Image 1 Version: 65103900
  FW Image 1 State: RUNNING ACTIVATED
  FW Image 2 Version: 65103900
  FW Image 2 State: BACKUP INACTIVATED
Server /chassis/sas-expander #
```

Installing SAS Expander Firmware from a Remote Server

Before You Begin

- You must be logged in as admin to perform this action.
- Server must be powered on.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope sas-expander {1 2}	Enters the SAS expander command mode.
Step 3	Server /chassis/sas-expander # show detail	Displays the available firmware images and status.
Step 4	Server /chassis/sas-expander # update protocol IP_Address path	<p>It specifies the following:</p> <ul style="list-style-type: none"> • Protocol, it can be TFTP, FTP, SFTP, SCP or HTTP. <p>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.</p> <p>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.</p> <p>The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.</p> <ul style="list-style-type: none"> • The IPv4 or IPv6 address or the host name of the remote server. • The file path to the SAS expander firmware file on the remote server.

This example updates the SAS expander firmware:

```

Server# scope chassis
Server /chassis # scope sas-expander 1
Server /chassis/sas-expander # show detail
Firmware Image Information:
  ID: 1
  Name: SASEXP1
  Update Stage: NONE
  Update Progress: 0
  Current FW Version: 65103900
  FW Image 1 Version: 65103900
  FW Image 1 State: RUNNING ACTIVATED
  FW Image 2 Version: 65103900
  FW Image 2 State: BACKUP INACTIVATED
Server /chassis/sas-expander # update ftp 192.0.20.34
//upgrade_sas_expander_files/sas-expander-2-0-12a.fw
<CR> Press Enter key
Firmware update has started.

```

Please check the status using "show detail"
 Server /chassis/sas-expander #

Activating Installed SAS Expander Firmware

Before You Begin

- You must be logged in as admin to perform this action.
- Install the firmware on the expander.
- Host must be powered on.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope sas-expander {1 2}	Enters the SAS expander command mode.
Step 3	Server /chassis/sas-expander # activate	Activates the currently inactive image.
Step 4	At the prompt, enter y to activate the selected firmware image.	

This example activates firmware and then verifies the activation:

```

Server# scope chassis
Server /chassis # scope sas-expander 1
Server /chassis/sas-expander # show detail
  ID: 1
    Name: SASEXP1
    Update Stage: NONE
    Update Progress: 0
    Current FW Version: 65103900
    FW Image 1 Version: 65103900
    FW Image 1 State: RUNNING INACTIVATED
    FW Image 2 Version: 65103900
    FW Image 2 State: BACKUP INACTIVATED

Server /chassis/sas-expander # activate
This operation will activate "65103900" after next host power off
Continue?[y|N] y

Server /chassis/sas-expander # show detail
  ID: 1
    Name: SASEXP1
    Update Stage: NONE
    Update Progress: 0
    Current FW Version: 65103900
    FW Image 1 Version: 65103900
    FW Image 1 State: RUNNING ACTIVATED
    FW Image 2 Version: 65103900
    FW Image 2 State: BACKUP INACTIVATED
Server /chassis/sas-expander #

```