Firmware Management

Overview of CIMC Firmware

The UCS E-Series M6 Servers use Cisco-certified firmware specific to the server model that you are using. You can download new releases of the firmware for all supported server models from Cisco.com.

To avoid potential problems, it is strongly recommended that you use the Host Upgrade Utility (HUU), which upgrades the CIMC, BIOS, and other firmware components to compatible levels.

Note Do not install the new BIOS firmware until after you have activated the compatible CIMC firmware, or the server will not boot.

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. 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.

Options for Upgrading Firmware

You can use the Cisco Host Upgrade Utility (HUU) to upgrade the firmware components.

HUU—We recommend that you use the HUU ISO file to upgrade all firmware components, which include the CIMC, BIOS and FPGA firmware. It is recommended to upgrade all firmware with the HUU ISO package.

Note Using the latest versions of CIMC or BIOS firmware with older versions of other firmware may result in unexpected behavior.

Obtaining Software from Cisco Systems

Use this procedure to download BIOS and CIMC firmware.

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**.

A roll-down menu appears.

Step 4 From the Downloads (center) pane, click **All Downloads** (located at the bottom right corner).

The **Download Software** page appears.

Step 5 From the left pane, click **Products**.

Step 6 From the center pane, click **Unified Computing and Servers**.

Step 7 From the right pane, click **Cisco UCS E-Series Software**.

Step 8 From the right pane, click the name of the server model for which you want to download the software.

The **Download Software** page appears with the following categories.

- **Unified Computing System (UCSE) Server Firmware**—Contains the Host Upgrade Utility.

Step 9 Click the appropriate software category link.

Step 10 Click the **Download** button associated with software image that you want to download.

The **End User License Agreement** dialog box appears.

Step 11 (Optional) To download multiple software images, do the following:

a) Click the **Add to cart** button associated with the software images that you want to download.

b) Click the **Download Cart** button located on the top right .

All the images that you added to the cart display.

c) Click the **Download All** button located at the bottom right corner to download all the images.

The **End User License Agreement** dialog box appears.

Step 12 Click **Accept License Agreement**.

Step 13 Do one of the following as appropriate:

- Save the software image file to a local drive.
- If you plan to install the software image from a TFTP server, copy the file to the TFTP server that you want to use.

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

What to do next

Install the software image.

Installing CIMC Firmware from a Remote Server

To avoid potential problems, it is strongly recommended that you use the Host Upgrade Utility (HUU), which upgrades the CIMC, BIOS, and other firmware components to compatible levels.

Note Do not install the new BIOS firmware until after you have activated the compatible CIMC firmware or the server will not boot.

Before you begin

- Log into CIMC as a user with admin privileges.
- Obtain the CIMC firmware file from Cisco Systems.

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 CIMC command mode.
Step 2	Server /cimc # **scope firmware**	Enters CIMC firmware command mode.

	Command or Action	Purpose
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 # **show detail**	(Optional) Displays the progress of the firmware update.

Example

This example updates the firmware:

```
Server# scope cimc
Server /cimc # scope firmware
Server /cimc/firmware # update tftp 10.20.34.56 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 #
```

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 the CIMC.
- Activate any other firmware.
- Export technical support or configuration data.

Note If you start an activation while an update is in process, the activation will fail.

Procedure

	Command or Action	Purpose
Step 1	Server # **scope cimc**	Enters CIMC command mode.
Step 2	Server /cimc # **scope firmware**	Enters CIMC firmware command mode.
Step 3	Server /cimc/firmware # **show** [**detail**]	Displays the available firmware images and status.
Step 4	Server /cimc # **activate**	Activates the selected image. If no image number is specified, the server activates the currently inactive image.

Example

This example activates the firmware image:

```
Server /cimc/firmware # show detail
Firmware Image Information:
    Update Stage: NONE
    Update Progress: 0%
    Current FW Version: 4.11(0)73
    FW Image 1 Version: 4.1-suthandy-030223-111138
    FW Image 1 State: BACKUP INACTIVATED
    FW Image 2 Version: 4.11(0)73
    FW Image 2 State: RUNNING ACTIVATED
    Boot-loader Version: 4.11(0)73
    Secure Boot: ENABLED

Server /cimc #
Server /cimc # activate
```

Changing Password Storage Format

This procedure explains how to change the format of the password storage.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters CIMC command mode.
Step 2	Server /cimc # **change-password-storage**	Changes the format of the password storage. You will be prompted before changing the format.

Example

This example changes the format:

```
Server# scope cimc
Server /cimc # change-password-storage

This operation will change the user password storage form to be SHA512 with salt.
Note that, once you start this operation:
1. You cannot change the password storage format back.
2. The IPMI over LAN feature will stop working.
3. You need to change the passwords of all local users to have them stored in the new format.
Are you sure you want to continue?[y|N]

Press Y to change the format.
```

Installing BIOS Firmware from the TFTP Server

To avoid potential problems, it is strongly recommended that you use the Host Upgrade Utility (HUU), which upgrades the CIMC, BIOS, and other firmware components to compatible levels.

If you choose to upgrade the CIMC and BIOS firmware manually—instead of using the HUU—you must update the CIMC firmware first, and then the BIOS firmware. Do not install the new BIOS firmware until after you have activated the compatible CIMC firmware or the server will not boot.

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

Note Before you update the BIOS firmware, power off the server and put the module in maintenance mode.

Before you begin

Obtain the CIMC firmware file from Cisco Systems.

Procedure

	Command or Action	Purpose
Step 1	Server # **scope bios**	Enters BIOS command mode.
Step 2	Server /bios # **update protocol** *ip-address path-and-filename*	Starts the BIOS firmware update. The server will obtain the update firmware at the specified path and file name from the TFTP server at the specified IP address.
Step 3	Server /bios # **show detail**	(Optional) Displays the progress of the BIOS firmware update.
Step 4	Server /bios # **activate**	Activates the installed BIOS firmware.

Example

This example updates the BIOS firmware:

```
Server# scope bios
Server /bios # update 10.20.34.56 //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 /bios #
```

Troubleshooting the UCS E-Series M6 Server Access Issues

If you have problems accessing the E-Series M6 Server, it could be that the CIMC firmware image is corrupted, or the file system is corrupted, or the CIMC firmware installation did not complete successfully. Do one of the following as appropriate:

- If the CIMC firmware image is corrupted, see Recovering from a Corrupted CIMC Firmware Image, on page 7.
- If the file system is corrupted, see Recovering from a Corrupted File System, on page 9.
- If the CIMC firmware installation did not complete successfully, reinstall the CIMC firmware.

Important Due to security considerations, the **boot backup** command is disabled.

Recovering from a Corrupted CIMC Firmware Image

Before you begin

- Connect the server to your PC. Connect one end of the serial cable to the E-Series Server serial port and the other end to your PC.
- Depending on the interface option that you specify, do one of the following:
  - Dedicated—Attach an Ethernet cable to the Management (dedicated) port of the E-Series M6 Server.
  - Shared-Lom-GE2—Attach an Ethernet cable to the E-Series M6 Server's external GE2 interface.
  - Shared-Lom-Console—Use the Cisco IOS CLI to configure the E-Series M6 Server's internal console interface.
- To view the serial output, start the Minicom.
- Make sure that the communications settings are configured as: 9600 baud, 8 bits, No parity, and 1 stop bit.

Procedure

	Command or Action	Purpose
Step 1	Router # **hw-module subslot** *slot* **stop**	Shuts down the power to the specified E-Series M6 Server.
Step 2	Router # **hw-module subslot** *slot* **start**	Restarts the power to the specified E-Series M6 Server.
Step 3	***	From the Minicom, enter the *** command to enter the bootloader prompt.
Step 4	ucse-cimc > boot current recovery	Boots the E-Series M6 Server from the current image.
Step 5	Recovery-shell # **interface** [**dedicated** | **shared-lom-console** | **shared-lom-ge1** | **shared-lom-ge2** | **shared-lom-ge3**] *interface-ip-address* **netmask** *gateway-ip-address*	Specifies the IP address, subnet mask, and the gateway IP address of the specified interface.
Step 6	Recovery-shell # **ping** *tftp-ip-address*	Pings the remote TFTP server in which the CIMC firmware is located to verify network connectivity.
Step 7	Recovery-shell # **update** *tftp-ip-address image-filename*	Installs the CIMC firmware image, which is located on a remote TFTP server.
Step 8	Recovery-shell # **reboot**	Reboots CIMC.

Example

This example recovers the CIMC firmware image in an E-Series M6 Server:

```
Router# hw-module subslot 2/0 stop
Router# hw-module subslot 2/0 start

***

ucse-cimc > boot current recovery
recovery-shell# interface shared-lom-ge2 192.168.0.138 255.255.255.0 192.168.0.1
Network configuration:
IP config: addr: 192.168.0.138 Mask: 255.255.255.0
Gateway: 192.168.0.1
recovery-shell# ping 10.20.34.56
PING 10.20.34.56 (10.20.34.56): 56 data bytes
64 bytes from 10.20.34.56: seq=0 ttl=60 time=10.000 ms
64 bytes from 10.20.34.56: seq=1 ttl=60 time=0.000 ms
--- 10.20.34.56 ping statistics ---
10 packets transmitted, 10 packets received, 0% packet loss round-trip min/avg/max =
0.000/1.000/10.000 ms
recovery-shell# update 10.20.34.56 update_pkg-cimc.combined.bin
downloading firmware image "update_pkg-cimc.combined.bin" from " 10.20.34.56 "
download firmware image done, size in bytes: 22384144
installing firmware image, please wait ... activating installed image
done
Stage: NONE
Status: SUCCESS

Error: Success
recovery-shell# reboot
```

Recovering from a Corrupted File System

Use this procedure if you see the following error message in the CIMC boot log files.

```
UNEXPECTED INCONSISTENCY; RUN fsck MANUALLY
```

Before you begin

- Connect the server to your PC. Connect one end of the serial cable to the E-Series Server serial port and the other end to your PC.
- Depending on the interface option that you specify, do one of the following:
  - Dedicated—Attach an Ethernet cable to the Management (dedicated) port of the E-Series M6 Server.
  - Shared-Lom-GE2—Attach an Ethernet cable to the E-Series M6 Server's external GE2 interface.
  - Shared-Lom-Console—Use the Cisco IOS CLI to configure the E-Series M6 Server's internal console interface.
- To view the serial output, start the Minicom.
- Make sure that the communications settings are configured as: 9600 baud, 8 bits, No parity, and 1 stop bit.

Procedure

	Command or Action	Purpose
Step 1	Router # **hw-module subslot** *slot* **stop**	Shuts down the power to the specified E-Series M6 Server.
Step 2	Router # **hw-module subslot** *slot* **start**	Restarts the power to the specified E-Series M6 Server.
Step 3	***	From the Minicom, enter the *** command to enter the bootloader prompt.
Step 4	ucse-cimc > boot current recovery	Boots the E-Series M6 Server from the current image.
Step 5	Recovery-shell # **fs-check** [**p3** | **p4**]	Checks the file system of the specified partition and recovers the corrupted file system **Note** You can only use p3 and p4 partitions with this command. Use this command on the partition that is corrupted. The corrupted partition is the one that displays the **run fsk** error message during CIMC bootup. • If the command output displays **clean**, it indicates that the corrupted files are recovered. Enter the **reboot** command to reboot CIMC. Skip the steps that follow. • If the command output does not display **clean**, proceed to Step 6.

	Command or Action	Purpose
Step 6	Recovery-shell # **reboot**	(Optional) If the **fs-check [p3 | p4]**command does not recover the corrupted file system, and the output does not display **clean**, enter the **reboot** command to format the partitions. Skip the steps that follow. **Note** When the p3 partition is formatted, the CIMC configuration is lost.
Step 7	Recovery-shell # **interface** [**dedicated** | **shared-lom-console** | **shared-lom-ge1** | **shared-lom-ge2** | **shared-lom-ge3**] *interface-ip-address* **netmask** *gateway-ip-address*	Specifies the IP address, subnet mask, and the gateway IP address of the specified interface.
Step 8	Recovery-shell # **ping** *tftp-ip-address*	Pings the remote TFTP server in which the CIMC firmware is located to verify network connectivity.
Step 9	Recovery-shell # **update** *tftp-ip-address image-filename*	Installs the CIMC firmware image, which is located on a remote TFTP server.
Step 10	Recovery-shell # **reboot**	Reboots CIMC.

Example

This example recovers the CIMC firmware from the current image using the **fs-checkp3** command in an E-Series M6 Server:

```
Router# hw-module subslot 1/0 stop
Router# hw-module subslot 1/0 start

***

ucse-cimc > boot current recovery
recovery-shell# fs-check p3
e2fsck 1.41.14 (22-Dec-2010)
/dev/mmcblk0p3: recovering journal
/dev/mmcblk0p3: clean, 429/7840 files, 3331/31296 blocks
recovery-shell# fs-check p4
e2fsck 1.41.14 (22-Dec-2010)
/dev/mmcblk0p4: clean, 51/506912 files, 1880262/2025296 blocks
recovery-shell# reboot
```

Recovery Shell Commands

Recovery Shell Commands	Description
Recovery-shell # **dedicated-interface** *interface-ip-address netmask gateway-ip-address*	Specifies the IP address, subnet mask, and the gateway IP address of the dedicated interface.
Recovery-shell # **dedicated-interface (DEPRECATED)**	Shows the current configuration of the dedicated port.

Recovery-shell # **interface [dedicated | shared-lom-console | shared-lom-ge1 | shared-lom-ge2 | shared-lom-ge3]** *interface-ip-address netmask gateway-ip-address*	Specifies the IP address, subnet mask, and the gateway IP address of the specified interface.
Recovery-shell # **interface**	Shows the configuration on the interface.
Recovery-shell # **ping** *tftp-ip-address*	Pings the remote TFTP server in which the CIMC firmware is located to verify network connectivity.
Recovery-shell # **update** *tftp-ip-address image-filename*	Installs the CIMC firmware image, which is located on a remote TFTP server.
Recovery-shell # **fs-check [p3 | p4]**	Checks the file system of the specified partition and recover the corrupted file system.
Recovery-shell # **active image**	Shows the current active image that CIMC is running, which can be image 1 or image 2.
Recovery-shell # **active image [1 | 2]**	Changes the active image to 1 or 2. If the specified image is already active, a message is displayed. Otherwise, the specified image is made active. After you use the active image command, use the **reboot** command for the newly configured image to take effect.
Recovery-shell # **reboot**	Reboots the CIMC firmware.

Recovering Password

Before you begin

- Connect the server to your PC. Connect one end of the serial cable to the E-Series Server serial port and the other end to your PC.
- Depending on the interface option that you specify, do one of the following:
  - Dedicated—Attach an Ethernet cable to the Management (dedicated) port of the E-Series M6 Server.
  - Shared-Lom-GE2—Attach an Ethernet cable to the E-Series M6 Server's external GE2 interface.
  - Shared-Lom-Console—Use the Cisco IOS CLI to configure the E-Series M6 Server's internal console interface.
- To view the serial output, start the Minicom.
- Make sure that the communications settings are configured as: 9600 baud, 8 bits, No parity, and 1 stop bit.

Step 1 Router # **hw-module subslot** *1/0* **oir power-cycle**

Power-cycles the E-Series M6 Server.

Step 2 Type '***' to Stop Autoboot: 0”

At this prompt, type ****.

Step 3 ucse-cimc > **boot current recovery**

Type **`boot current recovery`** to boot up into recovery mode.

Step 4 Recovery-shell #

```
Recovery-shell is a menu-driven limited functionality interface

main options:

1. configure interface
   2. show interfaces
   3. ping
   4. cimc image options
   5. emmc options
   6. admin password reset
   7. enter debug shell
   8. exit and reboot
```

Step 5 Recovery-shell (enter your choice) # **emmc format p3**

Formats the p3 partition on the EMMC card that will clear the configuration, including the password.

Note When you partition EMMC, the contents of the EMMC card, such as the CIMC configuration, ISO file and password, are either lost or cleared.

```
ACT2 Reset Completed. Kindly reboot the system and login with default password. Recovery-shell is a
menu-driven limited functionality interface main options:

1. configure interface
  2. show interfaces
  3. ping
  4. cimc image options
  5. emmc options
  6. admin password reset
  7. enter debug shell
  8. exit and reboot
```

Step 6 Recovery shell (enter your choice) # **8**

```
Press 8 to exit and reboot the device
```

Example

This example recovers the password if you do not remember the CMIC password:

```
server # login: admin
Password:
****************WARNING!*****************
Default credentials were used for login.
   Administrator password needs to be
     changed for security purposes.
*****************************************
Enter current password: password
Please change the password...
```

```
Enter new password: <strong-password>
Re-enter new password: <strong-password>
Updating password...
Password updated successfully.
```