Updating the Firmware on Cisco UCS C-Series Servers

This chapter includes the following topics:

Upgrading the Firmware on a Cisco UCS C-Series Server Using the HUU

Note Secure adapter update is enabled once server components are updated to 2.0(13e). Subsequently supported adapters can be updated.

Important After upgrading the Cisco IMC firmware, you must check the compatibility matrix to verify if the drivers are compliant with the upgraded version of Cisco IMC. If the driver versions are non-compliant, you must upgrade the driver versions to match the Cisco IMC version.

The *Hardware and Software Interoperability Matrix* is available here:

http://www.cisco.com/en/US/products/ps10477/prod_technical_reference_list.html

You can use the HUU ISO to upgrade components of the server from the host locally with a writable disk (DVD or CD), or remotely by mounting the HUU ISO as a virtual device. The following procedures explain how to upgrade the firmware using the HUU:

Downloading and Preparing the ISO for Upgrade

Procedure

Step 1 Download the HUU ISO file:

a) Navigate to the following URL: Software Download
b) Search for **Servers – Unified Computing**.
c) In the right-hand column, click **Cisco UCS C-Series Rack-Mount Standalone Server Software**.
d) Choose the name of your model of server in the right column.
e) Click **Unified Computing System (UCS) Server Firmware**.
f) Choose the release number.
g) Click **Download** to download the `ucs-server platform-huu-version_number.iso` file.
h) Enter your credentials in the login screen.
i) Continue through the subsequent screens to accept the license agreement and browse to a location where you want to save the file.
j) Click **Download**.
ISO bundle downloads to the chosen location.

Step 2 If you want to prepare the ISO for a local upgrade, complete this step; Otherwise, go to **Step 3.**

a) Burn the ISO image onto a writable disk (CD).
b) Connect a VGA monitor and USB keyboard to the Cisco C-Series server.
c) Insert the disk into the USB DVD drive of the Cisco C-Series server.
d) Perform one of the following updating the firmware procedures depending on the firmware components that you want to upgrade.

Step 3 Prepare the ISO for a remote upgrade using the **KVM Console**.

a) Use a browser to connect to the software on the server that you are upgrading.
b) in the address field of the browser, enter the IP address for that server, and then enter your username and password.
c) Click **Launch KVM Console** on the toolbar. to launch the **KVM Console**.

Note Select the server node on which you want to boot the HUU.

d) In the **KVM Console**, click **Virtual Media**.
e) Click **Activate Virtual Devices** and then **Accept this session**.
f) Click **Map CD/DVD** and browse for the `ucs-server-name-huu-version_number.iso` file.
g) Click **Map Device**.
h) In the **Client View** area, in the **Mapped** column, check the check box for the ISO file that you added and then wait for mapping to complete.
i) After the ISO file appears as a mapped remote device, perform one of the following procedures depending on the firmware components that you want to upgrade.

Updating Firmware Using the Update All Option

Procedure

Step 1 Boot the server and press **F6** when prompted to open the **Boot Menu** screen.

Step 2 In the **Boot Menu** screen, choose the prepared ISO:

- For a local upgrade, choose the physical or externally connected CD/DVD device and then press **Enter**.
- For a remote upgrade, choose **Cisco vKVM-Mapped vDVD1.22,** and press **Enter**.

The server boots from the selected device.

Step 3 After the HUU boots, **Cisco End User License Agreement (EULA)** appears, read the EULA and click:

- **`I Agree`** to agree with the license agreement and proceed with the update.
- **`I Disagree`** to cancel.

Note When you choose **I Disagree**, it cancel the upgrade and reboots the host.

After you accept the EULA, when the **Cisco Host Upgrade Utility** window appears with a list of all the components that are available for update.

Step 4 If you want to update all the listed components, click **Update all**.

- **Enabling Cisco IMC Secure Boot** confirmation dialog box appears.

Note This message appears for M3 servers only and only if the secure boot is not already enabled.

Step 5 Read the content on the confirmation box carefully and click **Yes**, if you want to go ahead to update the firmware and enable Cisco IMC secure boot.

Note
- If you are updating from a version below 2.0(x) to 2.0(x), when you click **YES** both the active and the backup versions of Cisco IMC will be updated to 2.0(x).
- During update the KVM connection will be lost, you have to reconnect to view the progress of the updates.

For more information on Cisco IMC secure boot, refer to the **Introduction to Cisco IMC Secure Boot** section in the *Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide, Release 2.0(1)*.

Step 6 Reboot the server to apply firmware changes.

Updating the Firmware of Specific Components

The following procedure explains how update the firmware of individual components:

Procedure

Step 1 If you want update specific components from the list, choose the components that you want to update.

If you want to downgrade the secure adapter update firmware, complete steps **2** through **4** below. Else continue to step **5**.

Step 2 To downgrade the secure adapter update firmware, map the HUU and allow it to boot.

Step 3 On the virtual **KVM Console**, wait for the message 'Loading firmware tools' to display, when the HUU boots up.

Step 4 Disable **enable-security-version-check** once you see the 'Loading firmware tools' message.

a) From the Cisco IMC command line interface, run the command **scope cimc->scope adapter-secure-update->enable-security-version-check yes/no/status**.

b) From the Cisco IMC web UI, log on to the **Utilities** tab.
c) From the XML API, enter the following data:

Request:

```
<configConfMo cookie='1458615470/be0d9210-2e9a-1e9a-8004-816d1e1b0ff4'
 inHierarchical='false' dn='sys/rack-unit-1'>
  <inConfig>
    <computeRackUnit dn='sys/rack-unit-1' adaptorSecureUpdate='Disabled'/>
  </inConfig>
</configConfMo><IP>/nuova
```

Response:

```
<configConfMo dn="sys/rack-unit-1"
cookie="1474315600/b51b2682-3ce2-1ce2-8038-c4ae729d8b18"
 response="yes">
 <outConfig>
  <computeRackUnit dn="sys/rack-unit-1" adminPower="policy" availableMemory="196608"
   model="UCSC-C240-M4L" memorySpeed="1866" name="UCS C240 M4L" numOfAdaptors="1"
   numOfCores="12" numOfCoresEnabled="12" numOfCpus="2" numOfEthHostIfs="2"
numOfFcHostIfs="2"
   numOfThreads="24" operPower="on" originalUuid="0CA8BC15-2499-46F2-BFFE-686B224AB52E"

   presence="equipped" serverId="1" serial="FCH1927V0FC" totalMemory="196608" usrLbl=""

   uuid="0CA8BC15-2499-46F2-BFFE-686B224AB52E" vendor="Cisco Systems Inc"
   cimcResetReason="ac-cycle" adaptorSecureUpdate="Disabled" status="modified" >
    </computeRackUnit>
 </outConfig>
</configConfMo>
```

Step 5 Click **Update** to return to the update process.

Note
- We recommend you to update the firmware on all components using the **Update all** option, unless you want to specifically update the firmware of a component.
- When you update the firmware of one of the following three components: BMC, BIOS, or CMC, we recommend that you also update the firmware of the other two components.
- If you update the BMC firmware, click **Exit** and then **Ok** to activate the BMC firmware.
- If you choose to update BMC and any other component with it and if you have not chosen BIOS, then on exit, you will be prompted to update the **Chassis Firmware**, click **Yes** in the confirmation box to update the chassis firmware.

Important On the S3260 servers, when you click **Update** or **Update all** to update the chassis components of CMC1 and CMC2 simultaneously, the update on the second triggering server component is skipped, and the subsequent component is updated.

This initiates the update and the status of the update is displayed in the **Update Status** column. You can also view a more detailed log of a series of activities and statuses that are involved while updating the firmware in the **Execution Logs** section.

Step 6 Click **Exit** to exit from the HUU.

Note After clicking **Exit** you must wait for a few minutes before the server automatically powers up, indicating the completion of updating and activating of the new firmware.

Note If you have updated the BMC and not the BIOS, when you click **Exit**, BMC gets activated and you lose connectivity to the BMC and KVM.

Updating the HDD Firmware

The following procedure provides steps to update the HDD firmware:

Procedure

Step 1 If you want to update the firmware of the hard disk of a server, click **Update HDD Firmware**. A window displays a list of hard disk drives on the server that support new firmware. Hard disk drives that do not support firmware upgrades are not listed.

Important Updating the firmware of the hard disk drive could result in data loss. Cisco recommends that you take a complete system backup prior to updating the firmware.

a) To update the firmware of all the hard disks, click **Update All**.

With this option, HDDs with the latest firmware installed are not updated.

b) To update a specific HDD, choose the HDD and click **Update**.

Step 2 Reboot the server to apply firmware changes.

Verifying the Update Status and Saving Logs

The following procedure provides steps to verify the last update and save logs:

Procedure

Step 1 After you have updated the firmware, boot the server back into HUU ISO, and click **Last Update Verify**.

This action compares the previously updated firmware version for each component that was updated using the HUU with the current version of the firmware on the components and provides the status of the update.

Step 2 If you want to save the log files of the update status for later use, click **Save Logs**.

Log files that contain a detailed status of the update are saved to an external USB device that is connected to the server physically or through the KVM vMedia.

Note If an error occurs while updating the firmware, you are prompted to save the error log. Click **Save Logs** to save the log to an externally connected USB. This log can be used for identifying the cause of the error and troubleshooting.