



# Upgrading Earlier Release Version Servers for Cisco UCS Manager Integration

This chapter includes the following sections:

- [Required Items for Upgrade, page 1](#)
- [Upgrading the C-Series Server Firmware, page 2](#)
- [Updating Cisco UCS P81E VIC Firmware and uboot Image in Integrated Servers, page 5](#)
- [Migrating the Configuration to Release 2.2 or Later, page 7](#)

## Required Items for Upgrade

The following are the minimum Server CIMC version and Cisco UCS Manager version requirements for upgrade for C-Series server integration with Cisco UCS Manager:

Server	CIMC	BIOS	UCS Manager
Cisco UCS C22 M3 Server	1.4(6)	1.4.7a	2.1(2a)
Cisco UCS C24 M3 Server	1.4(6)	1.4.7a	2.1(2a)
Cisco UCS C220 M3 Server	1.4(6)	1.4.7a	2.1(2a)
Cisco UCS C220 M4 Server (requires 2.2.3 or above)	2.0(3d)	2.0.3	2.2(3a)
Cisco UCS C240 M3 Server	1.4(6)	1.4.7a	2.1(2a)

Server	CIMC	BIOS	UCS Manager
Cisco UCS C240 M4 Server (requires 2.2.3 or above)	2.0(3d)	2.0.3	2.2(3a)
Cisco UCS C260 M2 Server	1.4(6)	1.4.7	2.1(2a)
Cisco UCS C420 M3 Server	1.4(7)	1.4.8	2.1(2a)
Cisco UCS C460 M2 Server	1.4(6)	1.4.7	2.1(2a)
Cisco UCS C460 M4 Server	1.5(7a)	1.5.7	2.2(2a)

## Upgrading the C-Series Server Firmware

If your server CIMC release version does not meet the requirement for integration with Cisco UCS Manager, make sure to upgrade the server firmware before connecting the server with Cisco UCS domain. For more information on upgrading the C-Series server firmware, see the host upgrade utility quick start guide for your release [http://www.cisco.com/en/US/products/ps10493/products\\_user\\_guide\\_list.html](http://www.cisco.com/en/US/products/ps10493/products_user_guide_list.html)



### Important

When you upgrade the C-Series server firmware for Cisco UCS C220 M4 or C240 M4 servers to Cisco UCS Manager 2.2(6c), you will see the following critical alarm:

Board controller upgraded, manual a/c power cycle required on server x

This alarm, documented in CSCuv45173, is incorrectly categorized as a critical alarm. It does not impact the functionality of the server, and can be ignored.

To avoid seeing this alarm, you can do one of the following:

- Create a custom host firmware package in Cisco UCS Manager to exclude the board controller firmware from the Cisco UCS Manager 2.2(6c) update and keep the older version.
- Upgrade Cisco UCS Manager infrastructure (A Bundle) to Release 2.2(6c) and continue to run the host firmware (C Bundle) on any Cisco UCS C220 M4 or C240 M4 server at a lower version, according to the mixed firmware support matrix in Table 2 of the *Release Notes for Cisco UCS Manager, Release 2.2*.

### Procedure

**Step 1** Download the HUU ISO file:

- Navigate to the following URL: <http://www.cisco.com/cisco/software/navigator.html>.

- b) In the middle column, click **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 Now** to download the `ucs-server platform-huu-version_number.iso` file.
- h) Verify the information on the next page, and click **Proceed With Download**.
- i) Continue through the subsequent screens to accept the license agreement and browse to a location where you want to save the file.

**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) Go to Step 4.

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

- a) Use a browser to connect to the CIMC GUI software on the server that you are upgrading.
- b) In the address field of the browser, enter the CIMC 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**.
- d) In the **KVM Console**, click the **Virtual Media**.
- e) Click **Add Image** and click the `ucs-server-name-huu-version_number.iso` file.
- f) 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.
- g) After the ISO file appears as a mapped remote device, go to Step 4.

**Step 4** Boot the server and press F6 when prompted to open the **Boot Menu** screen.

**Step 5** 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 6** 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.

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

- Note**
- If you are updating to 2.0 (x) from versions 1.5(11) and before, or from version 1.5.3 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.

**Step 8** If you want update specific components from the list, choose the components that you want to update.

**Step 9** Click **Update**.

- Note**
- We recommend you 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: BIOS, CIMC, or CMC, we recommend that you also update the firmware of the other two components.
  - If you update the CIMC firmware, click **Exit** and then **Ok** to activate the CIMC firmware.
  - If you choose to update CIMC 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.

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 10** 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.

- To update the firmware of all the hard disks, click **Update All**.  
With this option, HDDs with the latest firmware installed are not updated.
- To update a specific HDD, choose the HDD and click **Update**.

**Step 11** Reboot the server.

**Step 12** Reboot the server, and click **Last Update Verify** to verify if the update was successfully completed. 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 13** 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.

**Step 14** Click **Exit** to exit from the HUU.

- Note**
- If you have updated the CIMC and not the BIOS, when you click **Exit**, CIMC gets activated and you lose connectivity to the CIMC and KVM.
  - If you have selected LOM for update and you are on shared LOM mode, when you click **Exit**, you lose connectivity to the CIMC and KVM.

---

## What to Do Next

After upgrading the server to the compatible server release version, you must establish the physical connection for the server to make it a part of Cisco UCS domain. To connect the server to your Cisco UCS FEXes and FIs, see [Connecting the C-Series Server with Cisco UCS Domain in Cluster Setup](#) for SingleConnect or [Connecting the C-Series Server with Cisco UCS Domain in Cluster Setup](#) for dual-wire management.

# Updating Cisco UCS P81E VIC Firmware and uboot Image in Integrated Servers

If your Cisco UCS P81E VIC firmware and uboot version is earlier than 2.0(2g), when you integrate the server with any Cisco UCS Manager version, the UCS Manager software will return discovery and associate/disassociate failures. To avoid such failures you can do the following:

- Before you integrate the server with UCS System, upgrade your P81E VIC firmware and uboot image to the required minimum 2.0(2g) level in standalone mode.
- If your server is already integrated, you cannot upgrade the P81E VIC uboot image in the UCS Manager software. You have to remove the server from the integration and then use Cisco Host Upgrade Utility to upgrade the card and server firmware.

The following procedure provides the process to upgrade when your server is integrated with Cisco UCS Manager.

## Procedure

- Step 1** Decommission the server from UCS Manager.
- Step 2** Disconnect the cables from the 1-Gb LOM ports on the server.
- Step 3** Connect an Ethernet line from your LAN to one of the 1-Gb LOM ports (not to the dedicated management port, which is disabled in UCSM mode).
- Step 4** Find the Host Upgrade Utility ISO file download for your server online and download it to a temporary location on your workstation:
- a) See the following URL: <http://www.cisco.com/cisco/software/navigator.html>
  - b) Click **Unified Computing and Servers** in the middle column.
  - c) Click **Cisco UCS C-Series Rack-Mount Standalone Server Software** in the right-hand column.
  - d) Click your model of server in the right-hand column.
  - e) Click **Unified Computing System (UCS) Server Firmware**.
  - f) Click the release number that you are downloading.
  - g) Click **Download Now** to download the ISO file.
  - h) Verify the information on the next page, then click **Proceed With Download**.
  - i) Continue through the subsequent screens to accept the license agreement and then browse to a location where you will save the ISO file.
- Step 5** Prepare the ISO. For local upgrade, on a local media and for remote upgrade, as a virtual device:

Option	Description
Local upgrade	<p>Perform the steps before going to Step 3:</p> <ol style="list-style-type: none"> <li>1 Burn the ISO image onto a writable DVD.</li> <li>2 Connect a VGA monitor and USB keyboard to the Cisco C-Series server.</li> <li>3 Insert the DVD into the DVD drive of the Cisco C-Series server or an external DVD drive.</li> </ol>

Option	Description
Remote upgrade	<p>Perform the steps before going to Step 3:</p> <ol style="list-style-type: none"> <li>1 Use a browser to connect to the CIMC Manager software on the server that you are upgrading.</li> <li>2 Enter the CIMC IP address for that server in the address field of the browser, then enter your user name and password.</li> <li>3 Launch a KVM Console window (click the KVM keyboard icon).</li> <li>4 When the Virtual KVM Console window launches, select <b>Tools &gt; Launch Virtual Media</b>.</li> <li>5 In the Virtual Media Session window, click <b>Add Image</b> and navigate to the utility ISO file and select it. Navigate to the location where you downloaded the ISO. The ISO image is displayed in the <b>Client View</b> area.</li> <li>6 In the <b>Virtual Media Session</b> window, select the check box in the <b>Mapped</b> column for the ISO file that you added, and then wait for mapping to complete. Observe the progress in the <b>Details</b> area.</li> </ol> <p>Now the ISO image is mapped to the remote device.</p>

**Step 6** Boot the server and press F6 when prompted to open the Boot Menu screen.

**Step 7** On the Boot Menu screen, select the device where you prepared the ISO in Step 2:

- If you are upgrading locally, select the physical CD/DVD device and then press Enter (for example, SATA5:TSSTcorp CDDVDW TS-L633C).
- If you are upgrading remotely, select **Cisco Virtual CD/DVD** and then press Enter.

The server is rebooted from the device you choose.

**Step 8** A screen appears with the server BIOS and CIMC firmware versions. Answer the prompt, Have you read the Cisco EULA (end user license agreement)?

- Press y to accept the EULA and continue the update.
- Press n to read the EULA. The EULA is displayed and you are prompted to press y to continue the update, or n to cancel. If you press n, the server will reboot without updating.
- Press q to exit without updating. This selection reboots the server.

The **Host Upgrade Menu** screen displays.

- Step 9** Select the option to **Update UCS P81E VIC**. This will update the card firmware and uboot image to the required level.
- Step 10** Select the option to **Update CIMC Firmware**. This will update the CIMC firmware.
- Step 11** Verify the firmware levels on the next screen.
- Step 12** Select the option to **Reboot the machine**.
- Step 13** When you see the F8 prompt during rebooting, press F8 to open the CIMC Configuration Utility.
- Step 14** In the CIMC Configuration Utility, select the option **CIMC Factory Default**, then press F10 to save your changes.
- Step 15** Return the cables from the FEXes to the 1-Gb LOM ports on the server.
- Step 16** Recommission the server in UCS Manager.
- 

## Migrating the Configuration to Release 2.2 or Later

When a Cisco UCS C-Series server is integrated with Cisco UCS Manager, discovered and associated with a service profile, you can migrate the configuration to a later version of Cisco UCS Manager.



### Note

- This migration process causes server downtime.
  - This procedure describes the scenario where management path from the server connects to the FEX and the data path connects directly to the FI.
- 

### Procedure

---

- Step 1** Shut down the server OS.
- Step 2** In Cisco UCS Manager, decommission all C-series servers from the Cisco UCS domain.
- Step 3** **Unconfigure** all FI server ports that are connected to the Nexus 2248 FEX.  
Issue an NX-OS **show fex** command to verify that the FEX is unconfigured. Wait until the command return does not list the FEX.
- Step 4** Disconnect the cable that connects the FEX and the FI.
- Step 5** In Cisco UCS Manager CLI, issue a **remove fex fex\_ID** command to remove the FEX from the database.
- Step 6** In Cisco UCS Manager GUI, **Unconfigure** all FI server ports that are connected to the server's adapter card.
- Step 7** Disconnect the cable that connects the FI and the server's adapter card.
- Step 8** Disconnect the cable that connects the FEX and the server's LOM connector.
- Step 9** Upgrade your Cisco UCS Manager software to or later and the FI firmware to the corresponding level.
- Step 10** Repeat steps 3 through 9 on the second fabric interconnect in your configuration.
- Step 11** Connect the C-Series server directly to your network and upgrade the firmware by using the standalone CIMC utility.
- a) Connect an Ethernet line from your LAN to one of the 1-Gb LOM ports on the server. Do not use the dedicated management port, this is disabled in the Cisco UCS Manager integrated mode.

- b) Follow the instructions in [Updating Cisco UCS P81E VIC Firmware and uboot Image in Integrated Servers](#), then return to the next step in this procedure.

**Step 12** Physically replace the Nexus 2248 FEX with a Nexus 2232PP FEX in your rack.

**Step 13** Connect the cables as shown in the image. See [Physical Connectivity Illustrations](#).

In this new configuration, the data and management paths both connect from the server to the FEX. The paths between the FEX and the FI carry both data and management traffic.

**Important** Issuing an NX-OS **show fex** command to verify the FEX. Wait until the command return lists the new Nexus 2232PP FEX. The FEX will automatically upgrade to the corresponding FI firmware version.

**Step 14** After both fabric interconnects are cabled, from Cisco UCS Manager, re-commission the decommissioned C-series servers.

When the server is discovered in Cisco UCS Manager, the previously assigned service profile is automatically re-associated with the server.

---