Upgrading the Firmware from Release 1.0(2) to Release 1.4(1)

This chapter includes the following sections:

Required Order of Steps When Upgrading from Release 1.0(2)

When you upgrade from Cisco UCS, Release 1.0(2), upgrade the components in the following order. If you do not follow this order, the firmware upgrade may fail and the servers may experience communication issues with Cisco UCS Manager. In addition, the order of steps in this document and the recommended options minimize the disruption to data traffic.

1. (Optional) Call Home—If the Cisco UCS instance includes Call Home or Smart Call Home, disable Call Home if you do not want to receive unnecessary alerts when Cisco UCS Manager restarts components to complete the firmware activation.

2. Adapter—If you plan to upgrade the adapters directly, perform this step first. However, if you prefer or if the adapters require it, you can omit this step and upgrade the adapters as part of the last step, in a host firmware package.

3. BMC—If you upgrade the adapters in the host firmware package, perform this step first.

4 Cisco UCS Manager.

5 I/O module—Activate with Set Startup Version only.

6 Fabric interconnect—If you are upgrading a system with a cluster configuration, activate the subordinate fabric interconnect first.

7 Fabric interconnect—If you are upgrading a system with a cluster configuration, activate the primary fabric interconnect second

8 Host firmware package—Must be the last step in the upgrade process. We recommend that you upgrade the board controller firmware during this step to avoid an additional reboot of the server. You must upgrade the following firmware in a host firmware package:

- BIOS
- Storage controller
- Gen 2 adapters

9 (Optional) Call Home—If you disabled Call Home before the upgrading the firmware, enable Call Home.

Note In Release 1.3(1) the BMC was renamed to CIMC Controller. After you upgrade from this release, Cisco UCS Manager no longer uses the term BMC. Because this document is aimed at upgrading to the current release, the term CIMC is sometimes used rather than BMC.

Required Order of Steps for Adding a Cisco UCS B230 Server

When you add the first B230 server, you must perform the steps in the following order to add support in Cisco UCS Manager for the server:

1 If you have not already done so, upgrade the Cisco UCS instance to Release 1.4(1).

2 Insert the blade server into the chassis as described in the server installation guide.

3 Wait for Cisco UCS Manager to discover the new server. If server discovery does not begin within a few minutes, acknowledge the server.

Note You do not need to update the Management Extensions or Capability Catalog to add a B230 server. The required support is included in the Cisco UCS, Release 1.4(1) infrastructure bundle.

Required Order of Steps for Integrating a Cisco UCS Rack-Mount Server

After you complete the upgrade of the existing Cisco UCS components, you can integrate a Cisco UCS rack-mount server. When you integrate a rack-mount server, you must perform the steps in the following order:

1 If you have not already done so, configure the rack server discovery policy in Cisco UCS Manager.

2 Follow the instructions in the server installation guide for installing and integrating a rack-mount server in a system managed by Cisco UCS Manager.

3 Wait for Cisco UCS Manager to discover the new server. If server discovery does not begin within a few minutes, acknowledge the server.

Disabling Call Home

This step is optional.

When you upgrade a Cisco UCS instance, Cisco UCS Manager restarts the components to complete the upgrade process. This restart causes events that are identical to service disruptions and component failures that trigger Call Home alerts to be sent. If you do not disable Call Home before you begin the upgrade, you can ignore the alerts generated by the upgrade-related component restarts.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All** ➤ **Communication Services**.

Step 3 Click **Call Home**.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Admin** area, click **off** in the **State** field.

Note If this field is set to **off**, Cisco UCS Manager hides the rest of the fields on this tab.

Step 6 Click **Save Changes**.

Updating the Firmware on the Adapters, BMCs, and IOMs to Release 1.4(1)

Caution Do not remove the hardware that contains the endpoint or perform any maintenance on it until the update process has completed. If the hardware is removed or otherwise unavailable due to maintenance, the firmware update fails. This failure may corrupt the backup partition. You cannot update the firmware on an endpoint with a corrupted backup partition.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, click the **Equipment** node.

Step 3 In the **Work** pane, click the **Firmware Management** tab.

Step 4 On the **Installed Firmware** subtab, click **Update Firmware**.

Cisco UCS Manager GUI opens the **Update Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS instance. This step may take a few minutes, depending upon the number of chassis and servers.

Step 5 In the **Update Firmware** dialog box, do the following:

a) From the **Filter** drop-down list on the menu bar, choose **ALL**.
If you would prefer to update one type of endpoint at a time, choose that endpoint from the **Filter** drop-down list.

b) From the **Set Version** drop-down list on the menu bar, choose the firmware version included in the Release 1.4(1) firmware bundle from the drop-down list.

c) Click **Apply** to begin the updates and leave the dialog box open so you can monitor the progress of the updates to each endpoint.
If the service profile for the server includes a host firmware package, Cisco UCS Manager cannot update the adapter firmware for that server. After you acknowledge the notification message, Cisco UCS Manager updates the firmware for all other endpoints on servers that do not have associated host firmware packages. If you want to update the adapter firmware for a server directly, you must remove all host firmware packages from the associated service profiles. Removing the adapter firmware from the host firmware package is not sufficient to enable you to update the adapters directly.

Cisco UCS Manager copies the selected firmware image to the backup memory partition and verifies that the image is not corrupt. The image remains as the backup version until you explicitly activate it. Cisco UCS Manager begins all updates at the same time. However, some updates may complete at different times.

The update is complete when the **Update Firmware** dialog box displays **ready** in the **Update Status** column for all updated endpoints.

Step 6 When all updates are completed, click **OK**.

What to Do Next

Activate the firmware.

Activating the Firmware on the Adapters, BMCs, and IOMs to Release 1.4(1)

This procedure ensures that the firmware activation for these endpoints causes minimal disruption to data traffic. If you do not activate the endpoints in the following order with the correct options configured, the endpoints may reboot and cause a temporary disruption in data traffic.

Caution Do not select **ALL** from the **Filter** drop-down list in the **Activate Firmware** dialog box to activate all endpoints simultaneously. Many firmware releases and patches have dependencies that require the endpoints to be activated in a specific order for the firmware update to succeed. This order can change depending upon the contents of the release or patch. Activating all endpoints does not guarantee that the updates occur in the required order and can disrupt communications between the endpoints, the fabric interconnects, and Cisco UCS Manager. For information about the dependencies in a specific release or patch, see the release notes provided with that release or patch.

This procedure continues directly from the previous one and assumes you are on the **Firmware Management** tab.

Procedure

Step 1 In the **Installed Firmware** tab, choose **Activate Firmware**.
If one or more of the selected endpoints are not configured with the desired version as the backup version, Cisco UCS Manager GUI does not display that version in the **Set Version** drop-down list. You must select the version from the **Startup Version** column for each individual endpoint.

Step 2 If the adapter firmware is not updated through a host firmware package in a service profile, do the following in the **Activate Firmware** dialog box to activate the adapter firmware:

a) From the **Filter** drop-down list, choose **Interface Cards**.
b) From the **Set Version** drop-down list, choose the firmware version included in the Release 1.4(1) firmware bundle.
c) Check the **Ignore Compatibility Check** check box.
The firmware for this release is not compatible with previous releases. Therefore, you must check the **Ignore Compatibility Check** check box to ensure that the activation succeeds.
d) Check the **Set Startup Version Only** check box.
Note During a direct upgrade, you should configure **Set Startup Version Only** for an adapter. With this setting, the activated firmware moves into the pending-next-boot state, and the server is not immediately rebooted. The activated firmware does not become the running version of firmware on the adapter until the server is rebooted. You cannot configure **Set Startup Version Only** for an adapter in the host firmware package.
e) Click **Apply**.
When the **Activate Status** column for all adapters displays **pending-next-boot** or **ready**, continue with Step 3.

Step 3 If the BMC firmware is not updated through a management firmware package in a service profile, do the following in the **Activate Firmware** dialog box to activate the BMC firmware:

a) From the **Filter** drop-down list, choose **BMC**.
b) From the **Set Version** drop-down list, choose the firmware version included in the Release 1.4(1) firmware bundle.
If one or more of the selected endpoints are not configured with the desired version as the backup version, Cisco UCS Manager GUI does not display that version in the **Set Version** drop-down list. You must select the version from the **Startup Version** column for each individual endpoint.
c) Check the **Ignore Compatibility Check** check box.
d) Click **Apply**.
The activation of firmware for a BMC does not disrupt data traffic. However, it will interrupt all KVM sessions and disconnect any vMedia attached to the server.

When the **Activate Status** column for all BMC components displays **ready** continue with Step 4.

Step 4 To activate the IOM firmware, do the following in the **Activate Firmware** dialog box:

a) From the **Filter** drop-down list, choose **IO Modules**.
b) From the **Set Version** drop-down list, select the firmware version included in the Release 1.4(1) firmware bundle.
c) Check the **Ignore Compatibility Check** check box.
d) Check the **Set Startup Version Only** check box.

Important When you configure **Set Startup Version Only** for an I/O module, the I/O module is rebooted when the fabric interconnect in its data path is rebooted. If you do not configure **Set Startup Version Only** for an I/O module, the I/O module reboots and disrupts traffic. In addition, if Cisco UCS Manager detects a protocol and firmware version mismatch between the fabric interconnect and the I/O module, Cisco UCS Manager automatically updates the I/O module with the firmware version that matches the firmware in the fabric interconnect and then activates the firmware and reboots the I/O module again.

e) Click **Apply**.
When the **Activate Status** column for all IOMs displays **pending-next-boot**, continue with Step 5.

Step 5 Click **OK**.

Activating the Board Controller Firmware on a Server to Release 1.4(1)

Only certain servers, such as the Cisco UCS B440 High Performance blade server and the Cisco UCS B230 blade server, have board controller firmware. The board controller firmware controls many of the server functions, including eUSBs, LEDs, and I/O connectors.

This procedure continues from the previous one and assumes that you are on the **Installed Firmware** tab.

Note This activation procedure causes the server to reboot. Depending upon whether or not the service profile associated with the server includes a maintenance policy, the reboot can occur immediately. To reduce the number of times a server needs to be rebooted during the upgrade process, we recommend that you upgrade the board controller firmware through the host firmware package in the service profile.

Procedure

Step 1 On the **Installed Firmware** subtab, click **Activate Firmware**.
Cisco UCS Manager GUI opens the **Update Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS instance. This step may take a few minutes, depending upon the number of chassis and servers.

Step 2 From the **Filter** drop-down list on the menu bar of the **Activate Firmware** dialog box, select **Board Controller**.
Cisco UCS Manager GUI displays all servers that have board controllers in the **Activate Firmware** dialog box.

Step 3 From the **Set Version** drop-down list on the menu bar of the **Activate Firmware** dialog box, choose the board controller firmware version included in the Release 1.4(1) firmware bundle.

Step 4 Check the **Ignore Compatibility Check** check box.

Step 5 Click **OK**.

Activating the Cisco UCS Manager Software to Release 1.4(1)

This procedure continues directly from the previous one and assumes you are on the **Firmware Management** tab.

Procedure

Step 1 On the **Installed Firmware** subtab, click **Activate Firmware**.
Cisco UCS Manager GUI opens the **Update Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS instance. This step may take a few minutes, depending upon the number of chassis and servers.

Step 2 From the **Filter** drop-down list, choose **UCS Manager**.

Step 3 On the **UCS Manager** row of the **Activate Firmware** dialog box, do the following:

a) From the drop-down list in the **Startup Version** column, select the firmware version included in the Release 1.4(1) firmware bundle from the drop-down list.

b) Check the **Ignore Compatibility Check** check box.

Step 4 Click **OK**.
Cisco UCS Manager disconnects all active sessions, logs out all users, and activates the software. When the upgrade is complete, you are prompted to log back in.

Activating the Fabric Interconnect Firmware for a Cluster Configuration

Activating the Firmware on a Subordinate Fabric Interconnect to Release 1.4(1)

Before You Begin

Determine which fabric interconnect in the cluster is the subordinate fabric interconnect. For more information, see Verifying the High Availability Status and Roles of a Cluster Configuration.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, click the **Equipment** node.

Step 3 In the **Work** pane, click the **Firmware Management** tab.

Step 4 On the **Installed Firmware** subtab, click **Activate Firmware**.
Cisco UCS Manager GUI opens the **Update Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS instance. This step may take a few minutes, depending upon the number of chassis and servers.

Step 5 From the **Filter** drop-down list on the menu bar, choose **Fabric Interconnects**.

Step 6 On the menu bar, check the **Ignore Compatibility Check** check box.

Step 7 On the row of the **Activate Firmware** dialog box for the subordinate fabric interconnect, do the following:

a) In the **Kernel** row, choose the firmware version included in the Release 1.4(1) firmware bundle from the drop-down list in the **Startup Version** column.

b) In the **System** row, choose the firmware version included in the Release 1.4(1) firmware bundle from the drop-down list in the **Startup Version** column.

Step 8 Click **Apply**.
Cisco UCS Manager updates and activates the firmware and reboots the fabric interconnect and any I/O module in the data path to that fabric interconnect, disrupting data traffic to and from that fabric interconnect. However, assuming the Cisco UCS instance is configured to permit traffic and port failover, data traffic fails over to the primary fabric interconnect and is not disrupted.

Step 9 Verify the high availability status of the subordinate fabric interconnect.

Note If the **High Availability Details** area for the fabric interconnect does not show the following values, contact Cisco Technical Support immediately. Do not continue to update the primary fabric interconnect.

Field Name	Required Value
Ready field	**Yes**
State field	**Up**

What to Do Next

If the high availability status of the subordinate fabric interconnect contains the required values, update and activate the primary fabric interconnect.

Activating the Firmware on a Primary Fabric Interconnect to Release 1.4(1)

This procedure continues directly from the previous one and assumes you are on the **Firmware Management** tab.

Before You Begin

Activate the subordinate fabric interconnect.

Procedure

Step 1 On the **Installed Firmware** subtab, click **Activate Firmware**.
Cisco UCS Manager GUI opens the **Update Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS instance. This step may take a few minutes, depending upon the number of chassis and servers.

Step 2 From the **Filter** drop-down list on the menu bar, choose **Fabric Interconnects**.

Step 3 On the menu bar, check the **Ignore Compatibility Check** check box.

Step 4 On the row of the **Activate Firmware** dialog box for the primary fabric interconnect, do the following:

a) In the **Kernel** row, choose the firmware version included in the Release 1.4(1) firmware bundle from the drop-down list in the **Startup Version** column.
b) In the **System** row, choose the firmware version included in the Release 1.4(1) firmware bundle from the drop-down list in the **Startup Version** column.

Step 5 Click **Apply**.
Cisco UCS Manager updates and activates the firmware and reboots the fabric interconnect and any I/O module in the data path to that fabric interconnect, disrupting data traffic to and from that fabric interconnect. However, assuming the Cisco UCS instance is configured to permit traffic and port failover, data traffic fails over to the other fabric interconnect, which becomes the primary. When it comes back up, this fabric interconnect is the subordinate fabric interconnect.

Step 6 Verify the high availability status of the fabric interconnect.

Note If the **High Availability Details** area for the fabric interconnect does not show the following values, contact Cisco Technical Support immediately.

Field Name	Required Value
Ready field	**Yes**
State field	**Up**

Activating the Firmware on a Standalone Fabric Interconnect to Release 1.4(1)

For a standalone configuration with a single fabric interconnect, you can minimize the disruption to data traffic when you perform a direct firmware upgrade of the endpoints. However, you must reboot the fabric interconnect to complete the upgrade and, therefore, cannot avoid disrupting traffic.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, click the **Equipment** node.

Step 3 In the **Work** pane, click the **Firmware Management** tab.

Step 4 On the **Installed Firmware** subtab, click **Activate Firmware**.
Cisco UCS Manager GUI opens the **Update Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS instance. This step may take a few minutes, depending upon the number of chassis and servers.

Step 5 From the **Filter** drop-down list, choose **Fabric Interconnects**.

Step 6 On the menu bar, check the **Ignore Compatibility Check** check box.

Step 7 On the row of the **Activate Firmware** dialog box for the fabric interconnect, do the following:

a) In the **Kernel** row, choose the firmware version included in the Release 1.4(1) firmware bundle from the drop-down list in the **Startup Version** column.

b) In the **System** row, choose the firmware version included in the Release 1.4(1) firmware bundle from the drop-down list in the **Startup Version** column.

Step 8 Click **OK**.

Cisco UCS Manager activates the firmware and reboots the fabric interconnect and any I/O module in the data path to that fabric interconnect. For a standalone fabric interconnect, this disrupts all data traffic in the Cisco UCS instance.

Updating a Host Firmware Package to Release 1.4(1)

You must upgrade the BIOS and storage controller firmware through the host firmware package when you upgrade to Release 1.4(1). If you do not upgrade those packages, the servers may experience communication issues with Cisco UCS Manager and the CIMC.

⚠ **Caution** If the policy is included in one or more service profiles associated with a server and those service profiles do not include maintenance policies, Cisco UCS Manager updates and activates the firmware in the server and adapter with the new versions and reboots the server as soon as you save the host firmware package policy.

This procedure assumes that the host firmware package already exists and that you have upgraded Cisco UCS Manager to Release 1.4(1). For information on how to create a host firmware package or on how to update an existing one in a previous release , see the appropriate *Cisco UCS Manager GUI Configuration Guide* for the release that Cisco UCS Manager is running.

Before You Begin

Before you update a host firmware package, do the following:

- Upgrade Cisco UCS Manager and the fabric interconnects.
- Determine an appropriate maintenance window to reduce the impact of the disruption of data traffic when the server reboots.
- Ensure you know the 1.4(1) firmware version and model number (PID) for the servers or servers.

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers** ➤ **Policies**.

Step 3 Expand the node for the organization that includes the policy you want to update.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Expand **Host Firmware Packages** and choose the policy you want to update.

Step 5 On each subtab of the **General** tab, do the following for each type of firmware you want to include in the package:

a) In the **Select** column, ensure that the check box for the appropriate lines are checked.

b) In the **Vendor**, **Model**, and **PID** columns, verify that the information matches the servers you want to update with this package.
The model and model number (PID) must match the servers that are associated with this firmware package. If you select the wrong model or model number, Cisco UCS Manager cannot install the firmware update.

c) In the **Version** column, choose the firmware version from the release 1.4(1) firmware image.

Step 6 Click **Save Changes**.
Cisco UCS Manager verifies the model numbers and vendor against all servers associated with service profiles that include this policy. If the model numbers and vendor match a firmware version in the policy, Cisco UCS Manager updates the firmware according to the settings in the maintenance policies included in the service profiles.

What to Do Next

Verify that the firmware on the endpoints included in the host firmware package has been updated to release 1.4(1). If the firmware has not been updated, check the model numbers and vendors in the host firmware package against those on the endpoints that were not updated.

Enabling Call Home

This step is optional. You only need to enable Call Home if you disabled it before you began the firmware upgrades.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All** ➤ **Communication Services**.

Step 3 Click **Call Home**.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Admin** area, click **on** in the **State** field.

Note If this field is set to **on**, Cisco UCS Manager GUI displays the rest of the fields on this tab.

Step 6 Click **Save Changes**.