



Directly Upgrading Firmware at Endpoints

This chapter includes the following sections:

- [Direct Firmware Upgrade at Endpoints, page 1](#)
- [Updating the Firmware on Multiple Endpoints, page 4](#)
- [Adapter Firmware, page 5](#)
- [BIOS Firmware, page 7](#)
- [CIMC Firmware, page 8](#)
- [PSU Firmware Update, page 10](#)
- [Board Controller Firmware, page 11](#)
- [Cisco UCS Manager Firmware, page 16](#)
- [Fabric Interconnect Firmware, page 18](#)
- [Verifying Firmware Versions on Components, page 20](#)

Direct Firmware Upgrade at Endpoints

If you follow the correct procedure and apply the upgrades in the correct order, a direct firmware upgrade and the activation of the new firmware version on the endpoints is minimally disruptive to traffic in a Cisco UCS domain.

You can directly upgrade the firmware on the following endpoints:

- Adapters
- CIMCs
- I/O modules
- Board controllers
- Cisco UCS Manager
- Fabric interconnects

The adapter and board controller firmware can also be upgraded through the host firmware package in the service profile. If you use a host firmware package to upgrade this firmware, you can reduce the number of times a server needs to be rebooted during the firmware upgrade process.

**Note**

Upgrades of a CIMC through a management firmware package or an adapter through a firmware package in the service profile associated with the server take precedence over direct firmware upgrades. You cannot directly upgrade an endpoint if the service profile associated with the server includes a firmware package. To perform a direct upgrade, you must remove the firmware package from the service profile.

Stages of a Direct Firmware Upgrade

Cisco UCS Manager separates the direct upgrade process into two stages to ensure that you can push the firmware to an endpoint while the system is running without affecting uptime on the server or other endpoints.

Update

During this stage, the system copies the selected firmware version from the primary fabric interconnect to the backup partition in the endpoint and verifies that the firmware image is not corrupt. The update process always overwrites the firmware in the backup slot.

The update stage applies only to the following endpoints:

- Adapters
- CIMCs
- I/O modules

**Caution**

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

Activate

During this stage, the system sets the specified image version (normally the backup version) as the startup version and, if you do not specify **Set Startup Version Only**, immediately reboots the endpoint. When the endpoint is rebooted, the backup partition becomes the active partition, and the active partition becomes the backup partition. The firmware in the new active partition becomes the startup version and the running version.

The following endpoints only require activation because the specified firmware image already exists on the endpoint:

- Cisco UCS Manager
- Fabric interconnects
- Board controllers on those servers that support them

When the firmware is activated, the endpoint is rebooted and the new firmware becomes the active kernel version and system version. If the endpoint cannot boot from the startup firmware, it defaults to the backup version and raises a fault.

**Caution**

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.

Outage Impacts of Direct Firmware Upgrades

When you perform a direct firmware upgrade on an endpoint, you can disrupt traffic or cause an outage in one or more of the endpoints in the Cisco UCS domain.

Outage Impact of a Fabric Interconnect Firmware Upgrade

When you upgrade the firmware for a fabric interconnect, you cause the following outage impacts and disruptions:

- The fabric interconnect reboots.
- The corresponding I/O modules reboot.

Outage Impact of a Cisco UCS Manager Firmware Upgrade

A firmware upgrade to Cisco UCS Manager causes the following disruptions:

- Cisco UCS Manager GUI—All users logged in to Cisco UCS Manager GUI are logged out and their sessions ended.
Any unsaved work in progress is lost.
- Cisco UCS Manager CLI—All users logged in through telnet are logged out and their sessions ended.

Outage Impact of an I/O Module Firmware Upgrade

When you upgrade the firmware for an I/O module, you cause the following outage impacts and disruptions:

- For a standalone configuration with a single fabric interconnect, data traffic is disrupted when the I/O module reboots. For a cluster configuration with two fabric interconnects, data traffic fails over to the other I/O module and the fabric interconnect in its data path.
- If you activate the new firmware as the startup version only, the I/O module reboots when the corresponding fabric interconnect is rebooted.
- If you activate the new firmware as the running and startup version, the I/O module reboots immediately.
- An I/O module can take up to ten minutes to become available after a firmware upgrade.

Outage Impact of a CIMC Firmware Upgrade

When you upgrade the firmware for a CIMC in a server, you impact only the CIMC and internal processes. You do not interrupt server traffic. This firmware upgrade causes the following outage impacts and disruptions to the CIMC:

- Any activities being performed on the server through the KVM console and vMedia are interrupted.
- Any monitoring or IPMI polling is interrupted.

Outage Impact of an Adapter Firmware Upgrade

If you activate the firmware for an adapter and do not configure the **Set Startup Version Only** option, you cause the following outage impacts and disruptions:

- The server reboots.
- Server traffic is disrupted.

Updating the Firmware on Multiple Endpoints

You can use this procedure to update the firmware on the following endpoints:

- Adapters
- CIMCs
- I/O modules



Caution

Do not remove the hardware that contains the endpoint or perform any maintenance on it until the update process completes. If the hardware is removed or otherwise unavailable due to maintenance, the firmware update fails. This failure might 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 **Equipment**.
 - 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** tab, 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 domain. This step might take a few minutes, based on 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, select **ALL**.
If you want to update all endpoint firmware of a specific type, such as all adapters or server BIOS, select that type from the drop-down list.
 - b) In the **Select** field, do one of the following:

- To activate all endpoints to the same version, click the **Version** radio button and select the appropriate version from the **Set Version** drop-down list.
- To activate all endpoints to the firmware version included in a specific bundle, click the **Bundle** radio button and select the appropriate bundle from the **Set Bundle** drop-down list .

c) Click **OK**.

If one or more endpoints cannot be directly updated, Cisco UCS Manager displays a notification message. After you acknowledge the notification message, Cisco UCS Manager updates the firmware for all other endpoints on servers that can be directly updated.

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 activate it. Cisco UCS Manager begins all updates at the same time. However, some updates might 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 (Optional) To monitor the progress of the update to a specific endpoint, right-click the endpoint and choose **Show Navigator**.

Cisco UCS Manager displays the progress in the **Update Status** area on the **General** tab. If the navigator has an **FSM** tab, you can also monitor the progress there. An entry in the **Retry #** field might not indicate that the update failed. The retry count also includes retries that occur when Cisco UCS Manager retrieves the update status.

What to Do Next

Activate the firmware.

Adapter Firmware

Updating the Firmware on an Adapter



Caution

Do not remove the hardware that contains the endpoint or perform any maintenance on it until the update process completes. If the hardware is removed or otherwise unavailable due to maintenance, the firmware update fails. This failure might 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 **Equipment**.
- Step 2** Expand **Equipment > Chassis > Chassis Number > Servers**.
- Step 3** Expand the node for the server which includes the adapter you want to update.
- Step 4** Expand **Adapters** and select the adapter you want to upgrade.
- Step 5** In the **General** tab, click **Update Firmware**.
- Step 6** In the **Update Firmware** dialog box, do the following:
- From the **Version** drop-down list, select the firmware version to update the endpoint.
 - Click **OK**.
- If one or more endpoints cannot be directly updated, Cisco UCS Manager displays a notification message. After you acknowledge the notification message, Cisco UCS Manager updates the firmware for all other endpoints on servers that can be directly updated.
- Cisco UCS Manager copies the selected firmware package to the backup memory slot, where it remains until you activate it.
- Step 7** (Optional) Monitor the status of the update in the **Update Status** area. The update process can take several minutes. Do not activate the firmware until the selected firmware package displays in the **Backup Version** field in the **Firmware** area of the **General** tab.
-

What to Do Next

Activate the firmware.

Activating the Firmware on an Adapter

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
- Step 2** Expand **Equipment > Chassis > Chassis Number > Servers**.
- Step 3** Expand the node for the server that includes the adapter for which you want to activate the updated firmware.
- Step 4** Expand **Adapters** and select the adapter for which you want to activate the firmware.
- Step 5** In the **General** tab, click **Activate Firmware**.
- Step 6** In the **Activate Firmware** dialog box, do the following:
- Select the appropriate version from the **Version To Be Activated** drop-down list. If one or more of the selected endpoints are not configured with the required version as the backup version, that version does not display in the **Set Version** drop-down list. You must select the version from the **Startup Version** column for each individual endpoint.
 - If you want to set the startup version and not change the version running on the endpoint, check the **Set Startup Version Only** check box. 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.

If a server is not associated with a service profile, the activated firmware remains in the pending-next-boot state. Cisco UCS Manager does not reboot the endpoints or activate the firmware until the server is associated with a service profile. If necessary, you can manually reboot or reset an unassociated server to activate the firmware.

- c) Click **OK**.
-

BIOS Firmware

Updating the BIOS Firmware on a Server

**Caution**

Do not remove the hardware that contains the endpoint or perform any maintenance on it until the update process completes. If the hardware is removed or otherwise unavailable due to maintenance, the firmware update fails. This failure might 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 **Equipment**.
 - Step 2** Expand **Equipment > Chassis > Chassis Number > Servers**.
 - Step 3** Expand the node for the server for which you want to update the BIOS firmware.
 - Step 4** On the **General** tab, click the **Inventory** tab.
 - Step 5** Click the **Motherboard** tab.
 - Step 6** In the **Actions** area, click **Update Bios Firmware**.
 - Step 7** In the **Update Firmware** dialog box, do the following:
 - a) From the **Version** drop-down list, select the firmware version to which you want to update the server BIOS.
 - b) (Optional) If you want to update the firmware regardless of any possible incompatibilities or currently executing tasks, check the **Force** check box.
 - c) Click **OK**.

Cisco UCS Manager copies the selected server BIOS firmware package to the backup memory slot, where it remains until you explicitly activate it.

The update is complete when the **BIOS** area of the **Motherboard** tab displays **Ready** in the **Update Status** column for the **Backup Version**.
-

What to Do Next

Activate the firmware.

Activating the BIOS Firmware on a Server

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
- Step 2** Expand **Equipment > Chassis > Chassis Number > Servers**.
- Step 3** Expand the node for the server for which you want to activate the updated BIOS firmware.
- Step 4** On the **General** tab, click the **Inventory** tab.
- Step 5** Click the **Motherboard** tab.
- Step 6** In the **Actions** area, click **Activate Bios Firmware**.
- Step 7** In the **Activate Firmware** dialog box, do the following:
- Select the appropriate server BIOS version from the **Version To Be Activated** drop-down list.
 - If you want to set the start up version and not change the version running on the server, check the **Set Startup Version Only** check box.
If you configure **Set Startup Version Only**, the activated firmware moves into the pending-next-reboot state and the server is not immediately rebooted. The activated firmware does not become the running version of firmware until the server is rebooted.
 - Click **OK**.
-

CIMC Firmware

Updating the CIMC Firmware on a Server

**Caution**

Do not remove the hardware that contains the endpoint or perform any maintenance on it until the update process completes. If the hardware is removed or otherwise unavailable due to maintenance, the firmware update fails. This failure might 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 **Equipment**.
- Step 2** Expand **Equipment > Chassis > Chassis Number > Servers**.
- Step 3** Expand the node for the server for which you want to update the CIMC.
- Step 4** In the **General** tab, click the **Inventory** tab.
- Step 5** Click the **CIMC** tab.
- Step 6** In the **Actions** area, click **Update Firmware**.
- Step 7** In the **Update Firmware** dialog box, do the following:
- From the **Version** drop-down list, select the firmware version to update the endpoint.
 - Click **OK**.
- Cisco UCS Manager copies the selected firmware package to the backup memory slot, where it remains until you activate it.
- Step 8** (Optional) Monitor the status of the update in the **Update Status** area. The update process can take several minutes. Do not activate the firmware until the selected firmware package displays in the **Backup Version** field in the **Firmware** area of the **General** tab.
-

What to Do Next

Activate the firmware.

Activating the CIMC Firmware on a Server

The activation of firmware for a CIMC does not disrupt data traffic. However, it will interrupt all KVM sessions and disconnect any vMedia attached to the server.



Caution

Do not remove the hardware that contains the endpoint or perform any maintenance on it until the update process completes. If the hardware is removed or otherwise unavailable due to maintenance, the firmware update fails. This failure might 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 **Equipment**.
- Step 2** Expand **Equipment > Chassis > Chassis Number > Servers**.
- Step 3** Expand the node for the server that includes the CIMC for which you want to activate the updated firmware.
- Step 4** On the **General** tab, click the **Inventory** tab.
- Step 5** Click the **CIMC** tab.
- Step 6** In the **Actions** area, click **Activate Firmware**.
- Step 7** In the **Activate Firmware** dialog box, do the following:

- a) Select the appropriate version from the **Version To Be Activated** drop-down list.
If one or more of the selected endpoints are not configured with the required version as the backup version, that version does not display in the **Set Version** drop-down list. You must select the version from the **Startup Version** column for each individual endpoint.
 - b) If you want to set the startup version and not change the version running on the endpoint, check the **Set Startup Version Only** check box.
If you configure **Set Startup Version Only**, the activated firmware moves to the pending-next-reboot state and the endpoint is not immediately rebooted. The activated firmware does not become the running version of firmware until the endpoint reboots.
 - c) Click **OK**.
-

PSU Firmware Update

Beginning with Release 3.0(2), you can update PSU firmware directly from Cisco UCS Manager. The following PSU models are supported:

- Emerson Dual Voltage (DV) PSU with PID: UCSB-PSU-2500-ACDV
- Delta Dual Voltage (DV) PSU with PID: UCSB-PSU-2500-ACDV

Updating the Firmware on a PSU



Caution

Do not remove the hardware that contains the endpoint or perform any maintenance on it until the update process completes. If the hardware is removed or otherwise unavailable due to maintenance, the firmware update fails. This failure might 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 **Equipment**.
- Step 2** On the **Equipment** tab, expand **Equipment > Chassis**.
- Step 3** Select the chassis for which you want to manage the PSUs.
- Step 4** In the **Work** pane, click **PSUs**.
- Step 5** Click the **Firmware Management** tab.
- Step 6** Right-click the PSU that you want to upgrade and choose **Update Firmware**.
- Step 7** In the **Update Firmware** dialog box, do the following:
 - a) From the **Version** drop-down list, select the firmware version to which you want to update the endpoint.
 - b) Click **OK**.

Cisco UCS Manager copies the selected firmware package to the backup memory slot, where it remains until you explicitly activate it.

- Step 8** (Optional) Monitor the status of the update in the **Update Status** area. The update process can take several minutes. Do not activate the firmware until the selected firmware package displays in the **Backup Version** field in the **Firmware** area of the **General** tab.
-

What to Do Next

Activate the firmware.

Activating the Firmware on a PSU

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
- Step 2** On the **Equipment** tab, expand **Equipment > Chassis**.
- Step 3** Select the chassis for which you want to manage the PSUs.
- Step 4** In the **Work** pane, click **PSUs**.
- Step 5** Right-click the PSU that you want to upgrade and choose **Activate Firmware**.
- Step 6** In the **General** tab, click **Activate Firmware**.
- Step 7** In the **Activate Firmware** dialog box, do the following:
- Select the appropriate version from the **Version To Be Activated** drop-down list. If one or more of the selected endpoints are not configured with the required version as the backup version, that version does not display in the **Set Version** drop-down list. You must select the version from the **Startup Version** column for each individual endpoint.
 - If you want to set the startup version and not change the version running on the endpoint, check the **Set Startup Version Only** check box. If you configure **Set Startup Version Only**, the activated firmware moves to the pending-next-reboot state and the endpoint is not immediately rebooted. The activated firmware does not become the running version of firmware until the endpoint reboots.
 - Click **OK**.
-

Board Controller Firmware

Board controllers maintain various programmable logic and power controllers for all B-Series blade servers, and C-Series rack servers. The board controller update utility enables you to make critical hardware updates.

Board controllers, introduced in Cisco UCS Manager Release 2.1(2a), allow you to make optimizations for components, such as voltage regulators, through an update to a digital controller configuration file by using the board controller update utility. Earlier, updating a voltage regulator required changing physical components.

These updates are at a hardware level, and are designed to be backward-compatible. Therefore, having the latest version of the board controller is always preferred.

Guidelines for Activating Cisco UCS B-Series M3 and M4 Blade Server Board Controller Firmware

The following guidelines apply to Cisco UCS B-Series M3 and M4 blade server board controller firmware:

- You never need to downgrade the board controller firmware.
- The board controller firmware version of the blade server should be the same as or later than the installed software bundle version. Leaving the board controller firmware at a later version than the version that is currently running in your existing Cisco UCS environment does not violate the software matrix or TAC supportability.
- Board controller firmware updates are backward compatible with the firmware of other components.

Some Cisco UCS B200 M4 blade servers running on releases prior to Release 2.2(4b) may generate a false Cisco UCS Manager alert, documented in CSCuu15465. This false board controller mismatch alert was resolved in Cisco UCS Manager Capability Catalogs 2.2(4c)T and 2.2(5b)T. You will not see this alert if you use either the 2.2(4c)T or the 2.2(5b)T capability catalog.



Note

For more information, refer to <https://tools.cisco.com/bugsearch/bug/CSCuu15465>

You can apply the capability catalog update as follows:

- 1 Download 2.2(4c) Infra/Catalog or 2.2(5b) Infra/Catalog software bundle. [Downloading and Managing Firmware in Cisco UCS Manager](#) provides detailed information about downloading software bundles.
- 2 Load catalog version 2.2(4c)T or 2.2(5b)T (or the catalog version included) and activate the catalog. [Activating a Capability Catalog Update](#) provides detailed information about activating a capability catalog through Cisco UCS Manager.
- 3 Decommission the newly inserted blade server.
- 4 Associate the service profile with the host firmware pack policy that has the earlier board controller version. When the service profile is associated with the updated host firmware pack policy, any false mismatch alert (such as the one caused by the CSCuu15465 bug) will not be raised any more.
- 5 Click **Save**.
- 6 Re-discover the blade server.

Guidelines for Activating Cisco UCS C-Series M3 and M4 Rack Server Board Controller Firmware

The following guidelines apply to Cisco UCS C-Series M3 and M4 rack server board controller firmware:

- The board controller firmware and the CIMC firmware must be of the same package version.
- 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*.



Note For more information, refer to <https://tools.cisco.com/bugsearch/bug/CSCuv45173>

- If the activation status of the board controller displays **Pending Power Cycle** after you upgrade the board controller, a manual power cycle is required. A fault is also generated. After the power cycle is complete, the fault is cleared and the board controller activation status displays **Ready**.

Activating the Board Controller Firmware on a Cisco UCS B-Series M2 Blade Server

The board controller firmware controls many of the server functions, including eUSBs, LEDs, and I/O connectors.



Note This activation procedure causes the server to reboot. Depending upon whether the service profile associated with the server includes a maintenance policy, the reboot can occur immediately. Cisco recommends that you upgrade the board controller firmware through the host firmware package in the service profile as the last step of upgrading a Cisco UCS domain, along with upgrading the server BIOS. This reduces the number of times a server needs to reboot during the upgrade process.

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
- 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** tab, click **Activate Firmware**.
Cisco UCS Manager GUI opens the **Activate Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS domain. This step might take a few minutes, based on the number of chassis and servers.
- Step 5** 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 6** In the **Select** field, do one of the following:
 - To activate the board controller firmware on all servers to the same version, click the **Version** radio button and select the appropriate version from the **Set Version** drop-down list.

- To activate the board controller firmware on all servers to the firmware version included in a specific bundle, click the **Bundle** radio button and select the appropriate bundle from the **Set Bundle** drop-down list .

Step 7 Click **OK**.

Activating the Board Controller Firmware on Cisco UCS B-Series M3 and M4 Blade Servers

The board controller firmware controls many of the server functions, including eUSBs, LEDs, and I/O connectors.



Note

This activation procedure causes the server to reboot. Depending upon whether the service profile associated with the server includes a maintenance policy, the reboot can occur immediately. Cisco recommends that you upgrade the board controller firmware through the host firmware package in the service profile as the last step of upgrading a Cisco UCS domain, along with upgrading the server BIOS. This reduces the number of times a server needs to reboot during the upgrade process.

The following limitations apply to M3 and M4 board controller firmware:

- You cannot downgrade the firmware after the upgrade is complete.
- You must be using Cisco UCS Manager, Release 2.1(2a) or greater.
- The board controller firmware version of the blade server should be the same or newer than the installed software bundle version.

Before you activate the board controller firmware on M3 and M4 blade servers, consider the following guidelines:

- Leaving the board controller firmware at a later version than the version that is currently running in your existing Cisco UCS environment does not violate the software matrix or TAC supportability.
- Board controller firmware updates are always backward compatible with the firmware of other components. However, you cannot downgrade the board controller firmware in Cisco UCS Manager.
- If blade server components, such as CIMC, and adapter, are running a firmware version that is earlier than the firmware version of the board controller, you do not need to upgrade the blade components to match the firmware version running on the board controller.

Additionally, you may be impacted by a defect, documented in CSCuu15465, which creates a board controller "mismatch" alert. This is a false alert and was resolved in UCSM Capability Catalogs 2.2(4c)T and 2.2(5b)T.



Note

For more information, please refer to <https://tools.cisco.com/bugsearch/bug/CSCuu15465>

You can apply the capability catalog update as follows:

- 1 Download 2.2(4c) Infra/Catalog or 2.2(5b) Infra/Catalog software bundle. [Downloading and Managing Firmware in Cisco UCS Manager](#) provides detailed information about downloading software bundles.
- 2 Load catalog version 2.2(4c)T or 2.2(5b)T (or the catalog version included) and activate the catalog. [Activating a Capability Catalog Update](#) provides detailed information about activating a capability catalog through Cisco UCS Manager.
- 3 Decommission the newly inserted blade server.
- 4 Associate the blade server with the host firmware pack policy that has the earlier board controller version. No false mismatch alerts are raised because the catalog has the fix for CSCuu15465.



Note This is a catalog-only fix

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
 - 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** tab, click **Activate Firmware**.
Cisco UCS Manager GUI opens the **Activate Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS domain. This step might take a few minutes, based on the number of chassis and servers.
 - Step 5** 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 6** For the board controller you want to update, select a version from the **Startup Version** drop-down list.
 - Step 7** Click **OK**.
 - Step 8** (Optional) You can also use the **Force Board Controller Activation** option to update the firmware version when you upgrade CPUs with different architectures. For example, when you upgrade from Sandy Bridge to Ivy Bridge CPUs.
-

Activating the Board Controller Firmware on Cisco UCS C-Series M3 and M4 Rack Servers

The board controller firmware controls many of the server functions, including eUSBs, LEDs, and I/O connectors.

**Note**

This activation procedure causes the server to reboot. Depending upon whether the service profile associated with the server includes a maintenance policy, the reboot can occur immediately. Cisco recommends that you upgrade the board controller firmware through the host firmware package in the service profile as the last step of upgrading a Cisco UCS domain, along with upgrading the server BIOS. This reduces the number of times a server needs to reboot during the upgrade process.

The following limitations apply to M3 and M4 board controller firmware:

- You must be using Cisco UCS Manager, Release 2.2(1a) or greater.
- The board controller firmware and the CIMC firmware must be of the same package version.
- If the activation status of the board controller displays **Pending Power Cycle** after you upgrade the board controller, a manual power cycle is required. A fault is also generated. After the power cycle is complete, the fault is cleared and the board controller activation status displays **Ready**.

Procedure

-
- Step 1** In the **Navigation** pane, click **Equipment**.
- 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** tab, click **Activate Firmware**.
Cisco UCS Manager GUI opens the **Activate Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS domain. This step might take a few minutes, based on the number of chassis and servers.
- Step 5** 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 6** For the board controller you want to update, select a version from the **Startup Version** drop-down list.
- Step 7** Click **OK**.
- Step 8** (Optional) You can also use the **Force Board Controller Activation** option to update the firmware version when you upgrade CPUs with different architectures. For example, you upgrade from Sandy Bridge to Ivy Bridge CPUs.
-

Cisco UCS Manager Firmware

Consider the following guidelines and best practices while activating firmware on the Cisco UCS Manager software:

- In a cluster configuration, Cisco UCS Manager on both fabric interconnects must run the same version.
- Cisco UCS Manager activation brings down management for a brief period. All virtual shell (VSH) connections are disconnected.
- In a cluster configuration, Cisco UCS Manager on both fabric interconnects is activated.

- A Cisco UCS Manager update does not affect server application I/O because fabric interconnects do not need to be reset.
- If Cisco UCS Manager is updated while the subordinate fabric interconnect is down, the subordinate fabric interconnect is automatically updated when it comes back up.

Upgrade Validation

Cisco UCS Manager validates the upgrade or downgrade process and displays all firmware upgrade validation failures, such as deprecated hardware, in the **Upgrade Validation** tab. If there are upgrade validation failures, the upgrade fails, and Cisco UCS Manager rolls back to the earlier version. You must resolve these faults before continuing with the upgrade.

When upgrading or downgrading the infrastructure firmware through the Auto Install method, if you do not want Cisco UCS Manager to report issues with the upgrade or downgrade process, check the **Skip Validation** check box. Conversely, to report issues with the upgrade or downgrade process, clear the **Skip Validation** check box. The **Skip Validation** check box is cleared by default.

Activating the Cisco UCS Manager Software

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
 - 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** tab, click **Activate Firmware**.
Cisco UCS Manager GUI opens the **Activate Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS domain. This step might take a few minutes, based on the number of chassis and servers.
 - Step 5** 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 version to which you want to update the software.
 - b) 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. If you are prompted to re-login immediately after being disconnected, the login will fail. You must wait until the activation of Cisco UCS Manager is completed, which takes a few minutes.

Cisco UCS Manager makes the selected version the startup version and schedules the activation to occur when the fabric interconnects are upgraded.
-

Fabric Interconnect Firmware

Activating the Firmware on a Subordinate Fabric Interconnect

Before You Begin

Determine which fabric interconnect in the cluster is the subordinate fabric interconnect.

Procedure

-
- Step 1** In the **Navigation** pane, click **Equipment**.
- 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** tab, click **Activate Firmware**.
Cisco UCS Manager GUI opens the **Activate Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS domain. This step might take a few minutes, based on 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 row of the **Activate Firmware** dialog box for the subordinate fabric interconnect, do the following:
- In the **Kernel** row, choose the firmware version to which you want to upgrade from the drop-down list in the **Startup Version** column.
 - In the **System** row, choose the firmware version to which you want to upgrade from the drop-down list in the **Startup Version** column.
- Step 7** 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 domain is configured to permit traffic and port failover, data traffic fails over to the primary fabric interconnect and is not disrupted.
- Step 8** Verify the high availability status of the subordinate fabric interconnect.
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

This procedure continues directly from [Activating the Firmware on a Subordinate Fabric Interconnect](#), on page 18 and assumes you are on the **Firmware Management** tab.

Before You Begin

Activate the subordinate fabric interconnect.

Procedure

-
- Step 1** On the **Installed Firmware** tab, click **Activate Firmware**.
Cisco UCS Manager GUI opens the **Activate Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS domain. This step might take a few minutes, based on 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 row of the **Activate Firmware** dialog box for the subordinate fabric interconnect, do the following:
- In the **Kernel** row, choose the firmware version to which you want to upgrade from the drop-down list in the **Startup Version** column.
 - In the **System** row, choose the firmware version to which you want to upgrade from the drop-down list in the **Startup Version** column.
- Step 4** 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 domain 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 5** Verify the high availability status of the fabric interconnect.
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

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.

**Tip**

If you ever need to recover the password to the admin account that was created when you configured the fabric interconnects for the Cisco UCS domain, you must know the running kernel version and the running system version. If you do not plan to create additional accounts, Cisco recommends that you save the path to these firmware versions in a text file so that you can access them if required.

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
- Step 2** On the **Equipment** tab, click the **Equipment** node.
- Step 3** Expand the **Fabric Interconnects** node and click the standalone fabric interconnect.
- Step 4** On the **General** tab, click **Activate Firmware**.
- Step 5** In the **Activate Firmware** dialog box, complete the following fields:

Name	Description
Kernel Version drop-down list	Choose the version that you want to use for the kernel.
Force check box	If checked, Cisco UCS attempts the installation even if a previous attempt to install the selected version failed or was interrupted.
System Version drop-down list	Choose the version you want to use for the system.
Force check box	If checked, Cisco UCS attempts the installation even if a previous attempt to install the selected version failed or was interrupted.

- Step 6** 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 domain.

Verifying Firmware Versions on Components

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
- 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** tab, review the firmware versions listed for each component.