Directly Upgrading Firmware at Endpoints

This chapter includes the following sections:

- Direct Firmware Upgrade at Endpoints, page 1
- Adapter Firmware, page 4
- BIOS Firmware, page 7
- CIMC Firmware, page 8
- IOM Firmware, page 11
- PSU Firmware Update, page 11
- Board Controller Firmware, page 13
- Cisco UCS Manager Firmware, page 19
- Fabric Interconnect Firmware, 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.

Adapter Firmware

Updating and Activating 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

	Command or Action	Purpose
Step 1	UCS-A# **scope adapter** *chassis-id* / *blade-id* / *adapter-id*	Enters chassis server adapter mode for the specified adapter.
Step 2	UCS-A /chassis/server/adapter # **show image**	Displays the available software images for the adapter.
Step 3	UCS-A /chassis/server/adapter # **update firmware** *version-num*	Updates the selected firmware version on the adapter.
Step 4	UCS-A /chassis/server/adapter # **commit-buffer**	(Optional) Commits the transaction. Use this step only if you intend to use the **show firmware** command in Step 5 to verify that the firmware update completed successfully

	Command or Action	Purpose
		before activating the firmware in Step 6. You can skip this step and commit the **update-firmware** and **activate-firmware** commands in the same transaction; however, if the firmware update does not complete successfully, the firmware activation does not start. Cisco UCS Manager copies the selected firmware image to the backup memory partition and verifies that image is not corrupt. The image remains as the backup version until you explicitly activate it.
Step 5	UCS-A /chassis/server/adapter # **show firmware**	(Optional) Displays the status of the firmware update. Use this step only if you want to verify that the firmware update completed successfully. The firmware update is complete when the update status is Ready. The CLI does not automatically refresh, so you may have to enter the **show firmware** command multiple times until the task state changes from Updating to Ready. Continue to Step 6 when the update status is Ready.
Step 6	UCS-A /chassis/server/adapter # **activate firmware** *version-num* [**set-startup-only**]	Activates the selected firmware version on the adapter. Use the **set-startup-only** keyword if you want to move the activated firmware into the pending-next-boot state and not immediately reboot the server. The activated firmware does not become the running version of firmware on the adapter until the server is rebooted. You cannot use the **set-startup-only** keyword for an adapter in the host firmware package.
Step 7	UCS-A /chassis/server/adapter # **commit-buffer**	Commits the transaction. 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.
Step 8	UCS-A /chassis/server/adapter # **show firmware**	(Optional) Displays the status of the firmware activation. Use this step only if you want to verify that the firmware activation completed successfully. The CLI does not automatically refresh, so you may have to enter the **show firmware** command multiple times until the task state changes from Activating to Ready.

The following example updates and activates the adapter firmware to version 2.2(1b) in the same transaction, without verifying that the firmware update and firmware activation completed successfully:

```
UCS-A# scope adapter 1/1/1
UCS-A# /chassis/server/adapter # show image
Name                                               Type                Version       State
-------------------------------------------------- ------------------- ------------- -----
```

```
ucs-m81kr-vic.2.2.1b.bin                          Adapter             2.2(1b)
Active

UCS-A# /chassis/server/adapter # update firmware 2.2(1b)
UCS-A# /chassis/server/adapter* # activate firmware 2.2(1b) set-startup-only
UCS-A# /chassis/server/adapter* # commit-buffer
UCS-A# /chassis/server/adapter #
```

The following example updates the adapter firmware to version 2.2(1b), verifies that the firmware update completed successfully before starting the firmware activation, activates the adapter firmware, and verifies that the firmware activation completed successfully:

```
UCS-A# scope adapter 1/1/1
UCS-A# /chassis/server/adapter # show image
Name                                               Type                Version       State
-------------------------------------------------- ------------------- ------------- -----
ucs-m81kr-vic.2.2.1b.bin                           Adapter             2.2(1b)
Active

UCS-A# /chassis/server/adapter # update firmware 2.2(1b)
UCS-A# /chassis/server/adapter* # commit-buffer
UCS-A# /chassis/server/adapter # show firmware
Adapter 1:
    Running-Vers: 2.1(2a)
    Package-Vers: 2.1(2a)B
    Update-Status: Updating
    Activate-Status: Ready

UCS-A# /chassis/server/adapter # show firmware
Adapter 1:
    Running-Vers: 2.1(2a)
    Package-Vers: 2.1(2a)B
    Update-Status: Ready
    Activate-Status: Ready

UCS-A# /chassis/server/adapter # activate firmware 2.2(1b)
Warning: When committed this command will reset the end-point
UCS-A# /chassis/server/adapter* # commit-buffer
UCS-A# /chassis/server/adapter # show firmware
Adapter 1:
    Running-Vers: 2.1(2a)
    Package-Vers: 2.1(2a)B
    Update-Status: Ready
    Activate-Status: Activating

UCS-A# /chassis/server/adapter # show firmware
Adapter 1:
    Running-Vers: 2.1(2a)
    Package-Vers: 2.1(2a)B
    Update-Status: Ready
    Activate-Status: Pending Next Boot

UCS-A# /chassis/server/adapter # exit
UCS-A# /chassis/server # cycle cycle-immediate
UCS-A# /chassis/server* # commit-buffer
UCS-A# /chassis/server # scope adapter 1
UCS-A# /chassis/server/adapter # show firmware
Adapter 1:
    Running-Vers: 2.2(1b)
    Package-Vers: 2.2(1b)B
    Update-Status: Ready
    Activate-Status: Ready
UCS-A# /chassis/server/adapter #
```

BIOS Firmware

Updating and Activating the BIOS Firmware on a Server

Important You can update and activate BIOS firmware on a server using the Cisco UCS Manager CLI on all M3 generation servers. The earlier servers do not support BIOS firmware update using the Cisco UCS Manager CLI.

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

	Command or Action	Purpose
Step 1	UCS-A# **scope server** *chassis-id / blade-id*	Enters chassis server mode for the specified server.
Step 2	UCS-A /chassis/server # scope bios	Enters chassis server BIOS mode.
Step 3	UCS-A /chassis/server/bios # **show image**	Displays the available BIOS firmware images.
Step 4	UCS-A /chassis/server/bios # **update firmware** *version-num*	Updates the selected BIOS firmware for the server.
Step 5	UCS-A /chassis/server/bios # **commit-buffer**	(Optional) Commits the transaction. Use this step only if you intend to use the **show firmware** command in Step 6 to verify that the firmware update completed successfully before activating the firmware in Step 7. You can skip this step and commit the **update-firmware** and **activate-firmware** commands in the same transaction; however, if the firmware update does not complete successfully, the firmware activation does not start. Cisco UCS Manager copies the selected firmware image to the backup memory partition and verifies that image is not corrupt. The image remains as the backup version until you explicitly activate it.
Step 6	UCS-A /chassis/server/bios # **show firmware**	(Optional) Displays the status of the firmware update.

	Command or Action	Purpose
		Use this step only if you want to verify that the firmware update completed successfully. The firmware update is complete when the update status is Ready. The CLI does not automatically refresh, so you may have to enter the **show firmware** command multiple times until the task state changes from Updating to Ready. Continue to Step 7 when the update status is Ready.
Step 7	UCS-A /chassis/server/bios # **activate firmware** *version-num*	Activates the selected server BIOS firmware version.
Step 8	UCS-A /chassis/server/bios # **commit-buffer**	Commits the transaction.
Step 9	UCS-A /chassis/bios # **show firmware**	(Optional) Displays the status of the firmware activation. Use this step only if you want to verify that the firmware activation completed successfully. The CLI does not automatically refresh, so you may have to enter the **show firmware** command multiple times until the task state changes from Activating to Ready.

The following example updates and activates the BIOS firmware in the same transaction, without verifying that the firmware update and activation completed successfully:

```
UCS-A# scope server 1/1
UCS-A# /chassis/server # scope bios
UCS-A# /chassis/server/bios # show image
Name                                     Type         Version
---------------------------------------- ------------ -------
ucs-b230-m1-bios.B230.2.0.1.1.49.gbin Server Bios  B230.2.0.1.1.49
ucs-b230-m1-bios.B230.2.0.2.0.00.gbin Server Bios  B230.2.0.2.0.00

UCS-A# /chassis/server/bios # update firmware B230.2.0.2.0.00
UCS-A# /chassis/server/bios* # activate firmware B230.2.0.2.0.00
UCS-A# /chassis/server/bios* # commit-buffer
UCS-A# /chassis/server/bios #
```

CIMC Firmware

Updating and 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

	Command or Action	Purpose
Step 1	UCS-A# **scope server** *chassis-id* / *blade-id*	Enters chassis server mode for the specified server.
Step 2	UCS-A /chassis/server # **scope cimc**	Enters chassis server CIMC mode.
Step 3	UCS-A /chassis/server/cimc # **show image**	Displays the available software images for the adapter.
Step 4	UCS-A /chassis/server/cimc # **update firmware** *version-num*	Updates the selected firmware version on the CIMC in the server.
Step 5	UCS-A /chassis/server/cimc # **commit-buffer**	(Optional) Commits the transaction. Use this step only if you intend to use the **show firmware** command in Step 6 to verify that the firmware update completed successfully before activating the firmware in Step 7. You can skip this step and commit the **update-firmware** and **activate-firmware** commands in the same transaction; however, if the firmware update does not complete successfully, the firmware activation does not start. Cisco UCS Manager copies the selected firmware image to the backup memory partition and verifies that image is not corrupt. The image remains as the backup version until you explicitly activate it.
Step 6	UCS-A /chassis/server/cimc # **show firmware**	(Optional) Displays the status of the firmware update. Use this step only if you want to verify that the firmware update completed successfully. The firmware update is complete when the update status is Ready. The CLI does not automatically refresh, so you may have to enter the **show firmware** command multiple times until the task state changes from Updating to Ready. Continue to Step 7 when the update status is Ready.
Step 7	UCS-A /chassis/server/cimc # **activate firmware** *version-num*	Activates the selected firmware version on the CIMC in the server.
Step 8	UCS-A /chassis/server/cimc # **commit-buffer**	Commits the transaction.

	Command or Action	Purpose
Step 9	UCS-A /chassis/server/cimc # **show firmware**	(Optional) Displays the status of the firmware activation. Use this step only if you want to verify that the firmware activation completed successfully. The CLI does not automatically refresh, so you may have to enter the **show firmware** command multiple times until the task state changes from Activating to Ready.

The following example updates and activates the CIMC firmware to version 2.2(1b) in the same transaction, without verifying that the firmware update and firmware activation completed successfully:

```
UCS-A# scope server 1/1
UCS-A# /chassis/server # scope cimc
UCS-A# /chassis/server/cimc # show image
Name                                       Type              Version
------------------------------------------ ----------------- -------------
ucs-b200-m1-k9-cimc.2.2.1b.bin             CIMC              2.2(1b)
ucs-b200-m3-k9-cimc.2.2.1b.bin             CIMC              2.2(1b)
ucs-b22-m3-k9-cimc.2.2.1b.bin              CIMC              2.2(1b)
...

UCS-A# /chassis/server/cimc # update firmware 2.2(1b)
UCS-A# /chassis/server/cimc* # activate firmware 2.2(1b) set-startup-only
UCS-A# /chassis/server/cimc* # commit-buffer
UCS-A# /chassis/server/cimc #
```

The following example updates the CIMC firmware to version 2.2(1b), verifies that the firmware update completed successfully before starting the firmware activation, activates the CIMC firmware, and verifies that the firmware activation completed successfully:

```
UCS-A# scope server 1/1
UCS-A# /chassis/server # scope cimc
UCS-A# /chassis/server/cimc # show image
Name                                       Type              Version
------------------------------------------ ----------------- -------------
ucs-b200-m1-k9-cimc.2.2.1b.bin             CIMC              2.2(1b)
ucs-b200-m3-k9-cimc.2.2.1b.bin             CIMC              2.2(1b)
ucs-b22-m3-k9-cimc.2.2.1b.bin              CIMC              2.2(1b)
...

UCS-A# /chassis/server/cimc # update firmware 2.2(1b)
UCS-A# /chassis/server/cimc* # commit-buffer
UCS-A# /chassis/server/cimc # show firmware
Running-Vers    Update-Status   Activate-Status
--------------- --------------- ---------------
2.1(1)          Updating        Ready

UCS-A# /chassis/server/cimc # show firmware
Running-Vers    Update-Status   Activate-Status
--------------- --------------- ---------------
2.1(1)          Ready           Ready

UCS-A# /chassis/server/cimc # activate firmware 2.2(1b)
UCS-A# /chassis/server/cimc* # commit-buffer
UCS-A# /chassis/server/cimc # show firmware
Running-Vers    Update-Status   Activate-Status
--------------- --------------- ---------------
2.1(1)          Ready           Activating
```

```
UCS-A# /chassis/server/cimc # show firmware
Running-Vers    Update-Status   Activate-Status
--------------- --------------- ---------------
2.2(1b)          Ready           Ready
```

IOM Firmware

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

	Command or Action	Purpose
Step 1	UCS-A# **scope chassis** *chassis-id*	Enters chassis mode for the specified chassis.
Step 2	UCS-A /chassis # **scope psu** *psu-id*	Enters PSU mode for the specified PSU.
Step 3	UCS-A /chassis/psu # **show detail**	Displays the available software images for the PSU.
Step 4	UCS-A /chassis/psu # **update firmware** *version-num* [**force**]	Updates the selected firmware version on the PSU. You can use the optional **force** keyword to activate the firmware regardless of any possible incompatibilities or currently executing tasks. **Caution** Review the checklist that displays and ensure you have met all the requirements before you continue with the upgrade.
Step 5	UCS-A /chassis/psu # **commit-buffer**	(Optional) Commits the transaction. Cisco UCS Manager copies the selected firmware image to the backup memory partition and verifies that image is not

	Command or Action	Purpose
		corrupt. The image remains as the backup version until you explicitly activate it.

The following example shows how to update the PSU firmware and commit the transaction:

```
UCS-A# scope chassis 1
UCS-A# /chassis # scope psu 2
UCS-A# /chassis/psu # show detail
PSU:
    PSU: 2
    Overall Status: Operable
    Operability: Operable
    Threshold Status: OK
    Power State: On
    Presence: Equipped
    Thermal Status: OK
    Voltage Status: OK
    Product Name: Platinum II AC Power Supply for UCS 5108 Chassis
    PID: UCSB-PSU-2500ACDV
    VID: V00
    Part Number: 341-0571-01
    Vendor: Cisco Systems Inc
    Serial (SN): AZS1705000B
    HW Revision: 0
    Firmware Version: 05.11
    Type: DV
    Wattage (W): 0
    Input Source: Unknown
    Current Task:
UCS-A# /chassis/psu # update firmware 05.10
UCS-A# /chassis/psu* # commit-buffer
UCS-A# /chassis/psu #
```

Activating 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

	Command or Action	Purpose
Step 1	UCS-A# **scope chassis** *chassis-id*	Enters chassis mode for the specified chassis.
Step 2	UCS-A /chassis # **scope psu** *psu-id*	Enters PSU mode for the specified PSU.
Step 3	UCS-A /chassis/psu # **activate firmware** *version-num*	Activates the selected firmware version on the PSU.

	Command or Action	Purpose
Step 4	UCS-A /chassis/psu # **commit-buffer**	Commits the transaction. **Note** Committing the transaction resets the end points.

The following example activates the PSU firmware and commits the transaction:

```
UCS-A# scope chassis 1
UCS-A# /chassis # scope psu 2
UCS-A# /chassis/psu # activate firmware 02.08.05
Warning: When committed this command will reset the end-point
UCS-A# /chassis/psu* # commit-buffer
UCS-A# /chassis/psu #
```

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

	Command or Action	Purpose
Step 1	UCS-A# **scope server** *chassis-id* / *server-id*	Enters chassis server mode for the specified server.
Step 2	UCS-A /chassis/server # **scope boardcontroller**	Enters board controller mode for the server.
Step 3	UCS-A /chassis/server/boardcontroller # **show image**	(Optional) Displays the available software images for the board controller.
Step 4	UCS-A /chassis/server/boardcontroller # **show firmware**	(Optional) Displays the current running software image for the board controller.
Step 5	UCS-A /chassis/server/boardcontroller # **activate firmware** *version-num*	Activates the selected firmware version on the board controller in the server.
Step 6	UCS-A /chassis/server/boardcontroller # **commit-buffer**	Commits the transaction to the system configuration.

The following example activates the board controller firmware:

```
UCS-A# scope server 1/1
UCS-A# /chassis/server # scope boardcontroller
UCS-A# /chassis/server/boardcontroller # show image
Name                                 Type              Version            State
------------------------------------ ----------------- ------------------ -----
ucs-b440-m1-pld.B440100C-B4402006.bin  Board Controller  B440100C-B4402006  Active

UCS-A# /chassis/server/boardcontroller # show firmware
BoardController:
    Running-Vers: B440100C-B4402006
    Activate-Status: Ready

UCS-A# /chassis/server/boardcontroller # activate firmware B440100C-B4402006
UCS-A# /chassis/server/boardcontroller* # commit-buffer
```

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 the 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

	Command or Action	Purpose
Step 1	UCS-A# **scope server** *chassis-id* / *server-id*	Enters chassis server mode for the specified server.
Step 2	UCS-A /chassis/server # **scope boardcontroller**	Enters board controller mode for the server.
Step 3	UCS-A /chassis/server/boardcontroller # **show image**	(Optional) Displays the available software images for the board controller.
Step 4	UCS-A /chassis/server/boardcontroller # **show firmware**	(Optional) Displays the current running software image for the board controller.
Step 5	UCS-A /chassis/server/boardcontroller # **activate firmware** *version-num*	Activates the selected firmware version on the board controller in the server.
Step 6	UCS-A /chassis/server/boardcontroller # **commit-buffer**	Commits the transaction to the system configuration.

The following example activates the M3 board controller firmware:

```
UCS-A# scope server 1/1
UCS-A# /chassis/server # scope boardcontroller
UCS-A# /chassis/server/boardcontroller # show image
Name                                 Type              Version     State
------------------------------------ ----------------- ---------   -----
ucs-b200-m3-brdprog.11.0.bin         Board Controller    11.0      Active
ucs-b22-m3-brdprog.8.0.bin           Board Controller    8.0       Active

UCS-A# /chassis/server/boardcontroller # show firmware
BoardController:
    Running-Vers: 11.0
    Package-Vers:
    Activate-Status: Ready

UCS-A# /chassis/server/boardcontroller # activate firmware 11.0
UCS-A# /chassis/server/boardcontroller* # commit-buffer
```

Activating the Board Controller Firmware on a 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

	Command or Action	Purpose
Step 1	UCS-A# **scope server** *server-id*	Enters chassis server mode for the specified server.
Step 2	UCS-A /server # **scope boardcontroller**	Enters board controller mode for the server.
Step 3	UCS-A /server/boardcontroller # **show image**	(Optional) Displays the available software images for the board controller.
Step 4	UCS-A /server/boardcontroller # **show firmware**	(Optional) Displays the current running software image for the board controller.
Step 5	UCS-A /server/boardcontroller # **activate firmware** *version-num*	Activates the selected firmware version on the board controller in the server.
Step 6	UCS-A /server/boardcontroller # **commit-buffer**	Commits the transaction to the system configuration.

The following example activates the M3 board controller firmware:

```
UCS-A# scope server 7
UCS-A# /server # scope boardcontroller
```

```
UCS-A# /server/boardcontroller # show image
Name                                 Type              Version     State
-------------------------------------- ----------------- ---------   -----
ucs-c220-m3-brdprog.3.0.bin           Board Controller    3.0      Active
ucs-c220-m3-brdprog.3.0.bin           Board Controller    3.0       Active

UCS-A# /server/boardcontroller # show firmware
BoardController:
    Running-Vers: N/A
    Package-Vers:
    Activate-Status: Ready

UCS-A# /server/boardcontroller # activate firmware 3.0 force
Warning: When committed this command will reset the end-point.

UCS-A# /server/boardcontroller* # commit-buffer
```

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

	Command or Action	Purpose
Step 1	UCS-A# **scope system**	Enters system mode.

	Command or Action	Purpose
Step 2	UCS-A /system # **show image**	Displays the available software images for Cisco UCS Manager (system).
Step 3	UCS-A /system # **activate firmware** *version-num*	Activates the selected firmware version on the system. **Note** Activating Cisco UCS Manager does not require rebooting the fabric interconnect; however, management services will briefly go down and all VSH shells will be terminated as part of the activation.
Step 4	UCS-A /system # **commit-buffer**	Commits the transaction. Cisco UCS Manager makes the selected version the startup version and schedules the activation to occur when the fabric interconnects are upgraded.

The following example upgrades Cisco UCS Manager to version 2.2(1b) and commits the transaction:

```
UCS-A# scope system
UCS-A# /system # show image
Name                                               Type             Version     State
-------------------------------------------------- ---------------- ----------- -----
ucs-manager-k9.2.2.1b.bin                          System           2.2(1b)      Active

UCS-A# /system # activate firmware 2.2(1b)
UCS-A# /system* # commit-buffer
UCS-A# /system #
```

Fabric Interconnect Firmware

Activating the Firmware on a Fabric Interconnect

When updating the firmware on two fabric interconnects in a high availability cluster configuration, you must activate the subordinate fabric interconnect before activating the primary fabric interconnect. For more information about determining the role for each fabric interconnect, see Verifying the High Availability Status and Roles of a Cluster Configuration.

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

	Command or Action	Purpose
Step 1	UCS-A# **scope fabric-interconnect** {**a** | **b**}	Enters fabric interconnect mode for the specified fabric interconnect.
Step 2	UCS-A /fabric-interconnect # **show image**	Displays the available software images for the fabric interconnect.
Step 3	UCS-A /fabric-interconnect # **activate firmware** {**kernel-version** *kernel-ver-num* | **system-version** *system-ver-num*}	Activates the selected firmware version on the fabric interconnect.
Step 4	UCS-A /fabric-interconnect # **commit-buffer**	Commits the transaction. Cisco UCS Manager updates and activates the firmware, and then 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.

The following example upgrades the fabric interconnect to version 5.2(3)N2(2.21.92) and commits the transaction:

```
UCS-A# scope fabric-interconnect a
UCS-A /fabric-interconnect # show image
Name                                       Type                 Version
------------------------------------------ -------------------- ------------------
ucs-6100-k9-kickstart.5.2.3.N2.2.21b.bin   Fabric Interconnect  5.2(3)N2(2.21.92)
ucs-6100-k9-system.5.2.3.N2.2.21b.bin      Fabric Interconnect  5.2(3)N2(2.21.92)

UCS-A /fabric-interconnect # activate firmware kernel-version 5.2(3)N2(2.21.92) system-version
 5.2(3)N2(2.21.92)
UCS-A /fabric-interconnect* # commit-buffer
UCS-A /fabric-interconnect #
```

Forcing a Fabric Interconnect Failover

This operation can only be performed in the Cisco UCS Manager CLI.

You must force the failover from the primary fabric interconnect.

Important During a cluster failover, the virtual IP address will be unreachable until a new primary fabric interconnect is elected.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **show cluster state**	Displays the state of fabric interconnects in the cluster and whether the cluster is HA ready.
Step 2	UCS-A# **connect local-mgmt**	Enters local management mode for the cluster.
Step 3	UCS-A (local-mgmt) # **cluster** {**force primary** | **lead** {**a** | **b**}}	Changes the subordinate fabric interconnect to primary using one of the following commands: **force** Forces local fabric interconnect to become the primary. **lead** Makes the specified subordinate fabric interconnect the primary.

The following example changes fabric interconnect b from subordinate to primary:

```
UCS-A# show cluster state
Cluster Id: 0xfc436fa8b88511e0-0xa370000573cb6c04

A: UP, PRIMARY
B: UP, SUBORDINATE

HA READY
UCS-A# connect local-mgmt
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2011, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php

UCS-A(local-mgmt)# cluster lead b
UCS-A(local-mgmt)#
```