Directly Upgrading Firmware at Endpoints

This chapter includes the following sections:

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:

- Chassis:
  - CMC
  - Shared Adapter
  - Storage Controller
  - Board controller
- Server:

- CIMC
- BIOS
- Board Controller

- Infrastructure:
  - Fabric interconnects
  - Cisco UCS Manager

The CIMC and BIOS 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 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.

To trigger firmware upgrade on M-Series chassis components, use the following order:

1. Update CMC firmware
2. Update Shared Adapter firmware
3. Activate CMC firmware
4. Activate Shared Adapter firmware
5. Activate Storage Controller
6. Activate Board Controller

To trigger firmware upgrade on endpoints, use the following order:

1. Update CIMC
2. Activate CIMC
3. Update BIOS
4. Activate BIOS
5. Activate Board Controller

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:

- Chassis:
  - Chassis Management Controller (CMC)
  - Shared Adapter
- Server:
  - Cisco Integrated Management Controller (CIMC)
  - BIOS

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
- CMC
- Shared Adapter
- Board controllers for chassis and server
- Storage controller
- CIMC
- BIOS

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.

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 fabric interconnect 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 a CMC Firmware Upgrade

When you upgrade the firmware for CMC in a chassis you do not cause any outage.

Outage Impact of a Shared Adapter Firmware Upgrade

If you activate the firmware for a shared adapter, you cause the following outage impacts and disruptions:

- The server reboots.
- Server traffic is disrupted.
- The storage controller reboots.

Outage Impact of a Storage Controller Firmware Upgrade

If you activate the firmware for a storage controller, you cause the following outage impacts and disruptions:

- The server reboots.
- Server traffic is disrupted.
- The storage controller reboots.

Outage Impact of a Board Controller Firmware Upgrade

If you activate the firmware for a board controller, you cause the following outage impacts and disruptions:

- The shared adapter reboots.
- The cartridge and server reboot.
- Server traffic is disrupted.
- The storage controller reboots.

Outage Impact of a BIOS Firmware Upgrade

A firmware upgrade to the BIOS causes the server to reboot.

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 a Board Controller Firmware Upgrade on a Server

If you activate the firmware for a board controller on a server, you cause the server to be powered off during the upgrade and powered on after the upgrade is complete.

While activating the storage controller, board controller and shared adapter firmware, it is recommended that you power down the servers. In case you do not power down the servers during activation, Cisco UCSM will attempt to power down the servers and wait for a maximum of 16 minutes. During this time, if Cisco UCSM still finds that the servers are not powered down, FSM will fail and Cisco UCSM will not power up the servers that it powered down. FSM will try to come up after 8 minutes.

If UCSM successfully powers down the servers, it will power up the associated servers, based on their desired power states, after activation is complete.

Updating and Activating the CMC Firmware on a Chassis

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 server mode for the specified server.
Step 2	UCS-A /chassis # **scope cmc**	Enters chassis CMC mode.
Step 3	UCS-A /chassis/cmc # **update firmware** *version-num*	Updates the selected firmware version on the CMC in the chassis.
Step 4	UCS-A /chassis/cmc # **commit-buffer**	(Optional) Commits the transaction. Use this step only if you intend to use the **show update status** command in Step 5 to verify that the firmware update completed successfully before activating the firmware in Step 6. You can

	Command or Action	Purpose
		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/cmc # **show update status**	(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 update status** 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/cmc # **activate firmware** *version-num*	Activates the selected firmware version on the CMC in the server.
Step 7	UCS-A /chassis/cmc # **commit-buffer**	Commits the transaction.
Step 8	UCS-A /chassis/cmc # **show activate status**	(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 activate status** command multiple times until the task state changes from Activating to Ready.
Step 9	CS-A /chassis/cmc # **show firmware**	(Optional) Displays the running firmware version, the Update status and the Activate status.

The following example updates and activates the CMC firmware to version 2.0(2.30) in the same transaction, without verifying that the firmware update and firmware activation completed successfully:

```
UCS-A# scope chassis 2
UCS-A# /chassis # scope cmc
UCS-A# /chassis/cmc # update firmware 2.0(2.30)
UCS-A# /chassis/cmc* # activate firmware 2.0(2.30)
UCS-A# /chassis/cmc* # commit-buffer
UCS-A# /chassis/cmc # show firmware
CMC:
    Running-Vers: 2.0(2.30)
    Package Vers: 2.5(0.147)M
    Update-Status: Ready
    Activate-Status: Ready
```

The following example updates the CMC firmware to version 2.0(2.30), verifies that the firmware update completed successfully before starting the firmware activation, activates the CMC firmware, and verifies that the firmware activation completed successfully:

```
UCS-A# scope chassis 2
UCS-A# /chassis # scope cmc
UCS-A# /chassis/cmc # update firmware 2.0(2.30)
UCS-A# /chassis/cmc* # commit-buffer
UCS-A# /chassis/cmc # show update status
Status: Ready
UCS-A# /chassis/cmc # activate firmware 2.0(2.30)
UCS-A# /chassis/cmc* # commit-buffer
UCS-A# /chassis/cmc # show activate status
Status: Ready
UCS-A# /chassis/cmc # show firmware
CMC:
    Running-Vers: 2.0(2.30)
    Package Vers: 2.5(0.147)M
    Update-Status: Ready
    Activate-Status: Ready
```

Updating and Activating the Shared Adapter Firmware on a Chassis

In Cisco M-Series, updating and activating the shared adapter firmware affects all servers in a chassis.

Before You Begin

Gracefully power down the servers.

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 adapter**	Enters chassis adapter mode.
Step 3	UCS-A /chassis/adapter # **show image**	Displays the available software images for the shared adapter.
Step 4	UCS-A /chassis/adapter # **update firmware** *version-num*	Updates the selected firmware version on the shared adapter.
Step 5	UCS-A /chassis/adapter # **commit-buffer**	(Optional) Commits the transaction. Use this step only if you intend to use the **show update status** 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;

	Command or Action	Purpose
		however, if the firmware update does not complete successfully, the firmware activation does not start.
Step 6	UCS-A /chassis/adapter # **show update status**	(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 update status** 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/adapter # **activate firmware** *version-num*	Activates the selected firmware version on the shared adapter.
Step 8	UCS-A /chassis/adapter # **commit-buffer**	Commits the transaction.
Step 9	UCS-A /chassis/adapter # **show activate status**	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 activate status** command multiple times until the task state changes from Activating to Ready.
Step 10	UCS-A /chassis/adapter # **show firmware**	(Optional) Displays the running firmware version, the Update status and the Activate status.

The following example updates and activates the shared adapter firmware to version 4.0(2S33) in the same transaction, without verifying that the firmware update and firmware activation completed successfully:

```
UCS-A# scope chassis 1
UCS-A# /chassis # scope adapter
UCS-A# /chassis/adapter # show image
Name                                       Type                Version
------------------------------------------ ------------------- -------
ucs-m83-8p40-vic.4.0.2S12.bin              IOM                 4.0(2S12)
ucs-m83-8p40-vic.4.0.2S17.bin              IOM                 4.0(2S17)
ucs-m83-8p40-vic.4.0.2S22.bin              IOM                 4.0(2S22)
ucs-m83-8p40-vic.4.0.2S27.bin              IOM                 4.0(2S27)
ucs-m83-8p40-vic.4.0.2S33.bin              IOM                 4.0(2S33)

UCS-A# /chassis/adapter # update firmware 4.0(2S33)
UCS-A# /chassis/adapter* # activate firmware 4.0(2S33)
UCS-A# /chassis/adapter* # commit-buffer
UCS-A# /chassis/adapter # show firmware
Adapter:
    Running-Vers: 4.0(2S33)
    Package-Vers: 2.5(0.210)M
    Update-Status: Ready
    Activate-Status: Ready
```

The following example updates the shared adapter firmware to version 4.0(2S33), verifies that the firmware update completed successfully before starting the firmware activation, activates the shared adapter firmware, and verifies that the firmware activation completed successfully:

```
UCS-A# scope chassis 1
UCS-A# /chassis # scope adapter
UCS-A# /chassis/adapter # show image
Name                                       Type                Version
------------------------------------------ ------------------- -------
ucs-m83-8p40-vic.4.0.2S12.bin              IOM                 4.0(2S12)
ucs-m83-8p40-vic.4.0.2S17.bin              IOM                 4.0(2S17)
ucs-m83-8p40-vic.4.0.2S22.bin              IOM                 4.0(2S22)
ucs-m83-8p40-vic.4.0.2S27.bin              IOM                 4.0(2S27)
ucs-m83-8p40-vic.4.0.2S33.bin              IOM                 4.0(2S33)

UCS-A# /chassis/adapter # update firmware 4.0(2S33)
UCS-A# /chassis/adapter* # commit-buffer
UCS-A# /chassis/adapter # show update status
Status: Ready
UCS-A# /chassis/adapter # activate firmware 4.0(2S33)
UCS-A# /chassis/adapter* # commit-buffer
UCS-A# /chassis/adapter # show activate status
Status: Ready
UCS-A# /chassis/adapter # show firmware
Adapter:
    Running-Vers: 4.0(2S33)
    Package-Vers: 2.5(0.210)M
    Update-Status: Ready
    Activate-Status: Ready
```

Activating the Storage Controller Firmware on a Chassis

Before You Begin

Gracefully power down the servers.

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 raid-controller** *raid-id* {**sas** | **sd** | **flash** | **sata** | **unknown**	Enters storage controller mode for the chassis.
Step 3	UCS-A /chassis/raid-controller # **activate firmware** *version-num*	Activates the selected firmware version on the storage controller in the chassis.
Step 4	UCS-A /chassis/raid-controller # **commit-buffer**	Commits the transaction to the system configuration.
Step 5	UCS-A /chassis/raid-controller # **show activate status**	Displays the status of the firmware activation.

The following example shows how to activate the storage controller firmware:

```
UCS-A# scope chassis 1
UCS-A# /chassis # scope raid-controller 1 sas
UCS-A# /chassis/raid-controller # activate firmware 24.5.1.1
Warning: When committed, this command will soft shutdown the servers and reset the endpoint.
Associated servers power state will be restored after endpoint reset.
UCS-A# /chassis/raid-controller* # commit-buffer
UCS-A# /chassis/raid-controller* # show activate status
Activate-Status: Ready
```

Activating the Board Controller Firmware on a Chassis

Before You Begin

Gracefully power down the servers.

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 boardcontroller**	Enters board controller mode for the chassis.
Step 3	UCS-A /chassis/boardcontroller # **activate firmware** *version-num*	Activates the selected firmware version on the board controller in the chassis.
Step 4	UCS-A /chassis/boardcontroller # **commit-buffer**	Commits the transaction to the system configuration.
Step 5	UCS-A /chassis/boardcontroller # **show firmware**	Displays the running firmware version and the Activate status.

The following example shows how to activate the board controller firmware on a chassis:

```
UCS-A# scope chassis 1
UCS-A /chassis # scope boardcontroller
UCS-A /chassis/boardcontroller # activate firmware 1.0.4
Warning: When committed, this command will soft shutdown the servers and may power cycle
the chassis while activating the board controller.
Associated servers power state will be restored after chassis power cycle.
UCS-A# /chassis/boardcontroller # commit-buffer
UCS-A /chassis/boardcontroller* # show firmware
Board Controller:
    Running-Vers: 1.0.4
    Package-Vers: 2.5(0.210)M
    Activate-Status: Ready
UCS-A /chassis/boardcontroller* #
```

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.

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* / *cartridge-id* / *server-id*	Enters chassis server mode for the specified server.
Step 2	UCS-A /chassis/cartridge/server # **scope bios**	Enters chassis server BIOS mode.
Step 3	UCS-A /chassis/cartridge/server/bios # **update firmware** *version-num*	Updates the selected BIOS firmware for the server.
Step 4	UCS-A /chassis/cartridge/server/bios # **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 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/cartridge/server/bios # **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.

	Command or Action	Purpose
Step 6	UCS-A /chassis/cartridge/server/bios # **activate firmware** *version-num*	Activates the selected server BIOS firmware version.
Step 7	UCS-A /chassis/cartridge/server/bios # **commit-buffer**	Commits the transaction.
Step 8	UCS-A /chassis/cartridge/server/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 1/2/1
UCS-A# /chassis/cartridge/server # scope bios
UCS-A# /chassis/cartridge/server/bios # update firmware UCSME.142M4.2.0.100.52.122920140321
UCS-A# /chassis/cartridge/server/bios # activate firmware UCSME.142M4.2.0.100.52.122920140321
UCS-A# /chassis/cartridge/server/bios* # commit-buffer
```

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 / cartridge-id / server-id*	Enters chassis server mode for the specified server.
Step 2	UCS-A /chassis/cartridge/server # **scope cimc**	Enters chassis server CIMC mode.

	Command or Action	Purpose
Step 3	UCS-A /chassis/cartridge/server/cimc # **show image**	Displays the available software images for the adapter.
Step 4	UCS-A /chassis/cartridge/server/cimc # **update firmware** *version-num*	Updates the selected firmware version on the CIMC in the server.
Step 5	UCS-A /chassis/cartridge/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/cartridge/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/cartridge/server/cimc # **activate firmware** *version-num*	Activates the selected firmware version on the CIMC in the server.
Step 8	UCS-A /chassis/cartridge/server/cimc # **commit-buffer**	Commits the transaction.
Step 9	UCS-A /chassis/cartridge/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 2.0(100.46) in the same transaction, without verifying that the firmware update and firmware activation completed successfully:

```
UCS-A# scope server 1/2/1
UCS-A# /chassis/cartridge/server # scope cimc
UCS-A# /chassis/cartridge/server/cimc # update firmware 2.0(100.46)
UCS-A# /chassis/cartridge/server/cimc* # activate firmware 2.0(100.46)
UCS-A# /chassis/cartridge/server/cimc* # commit-buffer
UCS-A# /chassis/cartridge/server/cimc #
```

The following example updates the CIMC firmware to version 2.0(100.46), 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/cartridge/server # scope cimc
UCS-A# /chassis/cartridge/server/cimc # update firmware 2.0(100.46)
UCS-A# /chassis/cartridge/server/cimc* # commit-buffer
UCS-A# /chassis/cartridge/server/cimc # show firmware
Running-Vers    Update-Status   Activate-Status
--------------- --------------- ---------------
2.0(100.46)     Updating        Ready

UCS-A# /chassis/cartridge/server/cimc # show firmware
Running-Vers    Update-Status   Activate-Status
--------------- --------------- ---------------
2.0(100.46)     Ready           Ready

UCS-A# /chassis/cartridge/server/cimc # activate firmware 2.0(100.46)
UCS-A# /chassis/cartridge/server/cimc* # commit-buffer
UCS-A# /chassis/cartridge/server/cimc # show firmware
Running-Vers    Update-Status   Activate-Status
--------------- --------------- ---------------
2.0(100.46)     Ready           Activating

UCS-A# /chassis/cartridge/server/cimc # show firmware
Running-Vers    Update-Status   Activate-Status
--------------- --------------- ---------------
2.0(100.46)     Ready           Ready
```

Activating the Board Controller Firmware on a Server

This can be done only on servers in the Cisco UCSME-2814 cartridge.

Before You Begin

Gracefully power down the servers.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope server** *chassis-id*/*cartridge-id*/*server-id*	Enters server mode for the specified server.
Step 2	UCS-A /chassis/cartridge/server #**scope boardcontroller**	Enters board controller mode for the server.

	Command or Action	Purpose
Step 3	UCS-A /chassis/cartridge/server/boardcontroller # **activate firmware** *version-num*	Activates the selected firmware version on the board controller on the server.
Step 4	UCS-A /chassis/cartridge/server/boardcontroller # **commit-buffer**	Commits the transaction to the system configuration.
Step 5	UCS-A /chassis/cartridge/server/boardcontroller # **show firmware**	Displays the running firmware version and the Activate status.

The following example shows how to activate the board controller firmware on a chassis:

```
UCS-A# scope chassis 1/3/1
UCS-A /chassis/cartridge/server # scope boardcontroller
UCS-A /chassis/cartridge/server/boardcontroller # activate firmware 2.0
Warning: When committed this command will reset the end-point
UCS-A# /chassis/cartridge/server/boardcontroller # commit-buffer
UCS-A /chassis/cartridge/server/boardcontroller* # show firmware
Board Controller:
    Running-Vers: 2.0
    Package-Vers: 2.5(1.89)M
    Activate-Status: Ready
UCS-A /chassis/cartridge/server/boardcontroller* #
```

Activating the Cisco UCS Manager Software

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope system**	Enters system mode.
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 and commits the transaction:

```
UCS-A# scope system
UCS-A# /system # show image
Name                                               Type              Version
-------------------------------------------------- ----------------- -----------
ucs-manager-k9.2.5.0.1a.bin                        System            2.5(1a)

UCS-A# /system # activate firmware 2.5(1a)
UCS-A# /system* # commit-buffer
UCS-A# /system #
```

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 , 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.N2.2.50.225.bin   Fabric Interconnect Kernel
                                                                  5.2(3)N2(2.50.225)
ucs-6100-k9-system.5.2.3.N2.2.50.225.bin      Fabric Interconnect System
                                                                  5.2(3)N2(2.50.225)

UCS-A /fabric-interconnect # activate firmware kernel-version 5.2(3)N2(2.50.224)
system-version 5.2(3)N2(2.50.224)
UCS-A /fabric-interconnect* # commit-buffer
UCS-A /fabric-interconnect #
```