Firmware Management

- Firmware Management for Cisco UCS S3260 Systems, on page 1
- Firmware Upgrades through Chassis Firmware Packages in Chassis Profiles , on page 2
- Direct Firmware Upgrade on S3260 Chassis and Server Endpoints, on page 8

Firmware Management for Cisco UCS S3260 Systems

Cisco UCS uses firmware obtained from and certified by Cisco to support the endpoints in a Cisco UCS domain. Each endpoint is a component in the Cisco UCS domain that requires firmware to function.

Cisco UCS Manager Firmware Management Guide, Release 3.2 provides detailed information about the complete firmware management process. Additionally, beginning with Cisco UCS Manager Release 3.1(2), you can upgrade the firmware of Cisco UCS S3260 chassis components by defining a chassis firmware policy and including it in the chassis profile associated with a Cisco UCS S3260 chassis.

You can upgrade a Cisco UCS domain with a S3260 chassis and servers through Cisco UCS Manager in the following ways:

- Upgrade infrastructure components through Auto Install—You can upgrade the infrastructure components, such as the Cisco UCS Manager software and the fabric interconnects, in a single step by using Auto Install. *Cisco UCS Manager Firmware Management Guide, Release 3.2* provides detailed information about the Auto Install process.
- Upgrade chassis through one of the following:
  - Upgrade chassis components through Auto Install—Beginning with Cisco UCS Manager Release 3.2(3), you can upgrade the firmware of Cisco UCS S3260 chassis components in a single step by using Auto Install.
  - Upgrade chassis through chassis firmware packages in chassis profiles—This option enables you to upgrade all chassis endpoints in a single step. The chassis endpoints that you can upgrade through a chassis firmware package are:
    - Chassis Adapter
    - Chassis Management Controller
    - Chassis Board Controller
    - Local Disk

Note You can upgrade local disks in the chassis through a chassis firmware package. Upgrade the local disks in a server through a host firmware package.

- SAS Expander

- Upgrade servers through firmware packages in service profiles—This option enables you to upgrade all server endpoints in a single step, reducing the amount of disruption caused by a server reboot. You can combine this option with the deferred deployment of service profile updates to ensure that server reboots occur during scheduled maintenance windows. The server endpoints that you can upgrade through a host firmware package are:
  - CIMC
  - BIOS
  - Board Controller
  - Storage Controller
  - Local Disk
  - NVMe in SIOC
  - Third-party adapter in SIOC

  Cisco UCS Manager Firmware Management Guide, Release 3.2 provides detailed information about upgrading server endpoints through host firmware packages.

You can also directly upgrade the firmware at each infrastructure, chassis, and server endpoint. This option enables you to upgrade many infrastructure, chassis, and server endpoints directly, including the fabric interconnects, SAS expanders, CMCs, chassis adapters, storage controllers, and board controllers. However, direct upgrade is not available for all endpoints, including the storage controller, HBA firmware, HBA option ROM and local disk.

This chapter explains the following newly introduced firmware management capabilities for the Cisco UCS S3260 system:

- Upgrading firmware through chassis firmware packages in chassis profiles
- Directly upgrading firmware on Cisco UCS S3260 chassis and server endpoints

Firmware Upgrades through Chassis Firmware Packages in Chassis Profiles

Cisco UCS Manager Release 3.1(2) introduces support for chassis profiles and chassis firmware packages on Cisco UCS S3260 chassis. You can upgrade the firmware of Cisco UCS S3260 chassis endpoints by defining a chassis firmware package and including it in the chassis profile associated with a chassis. You cannot manually upgrade the firmware of a chassis that is associated with a chassis profile.

Note If any chassis component is in the failed state, chassis profile association fails. Cisco recommends bringing the chassis component back up before continuing with chassis profile association. To continue association without bringing the chassis component back up, exclude the component before association.

You cannot upgrade the firmware on a server through chassis profiles. Upgrade the firmware on servers through service profiles.

Servers in a chassis are automatically powered down before the chassis upgrade process begins.

Chassis Firmware Package

This policy enables you to specify a set of firmware versions that make up the chassis firmware package (also known as the chassis firmware pack). The chassis firmware package includes the following firmware for chassis endpoints:

- **Chassis Adapter**
- **Chassis Management Controller**
- **Chassis Board Controller**
- **Local Disk**

Note **Local Disk** is excluded by default from the chassis firmware package.

- **SAS Expander**

Tip You can include more than one type of firmware in the same chassis firmware package. For example, a chassis firmware package can include both board controller firmware and chassis adapter firmware for two different models of adapters. However, you can only have one firmware version with the same type, vendor, and model number. The system recognizes which firmware version is required for an endpoint and ignores all other firmware versions.

You can also exclude firmware of specific components from a chassis firmware package either when creating a new chassis firmware package or when modifying an existing chassis firmware package. For example, if you do not want to upgrade the board controller firmware through the chassis firmware package, you can exclude board controller firmware from the list of firmware package components.

Important Each chassis firmware package is associated with one list of excluded components.

The chassis firmware package is pushed to all chassis associated with chassis profiles that include this policy.

This policy ensures that the chassis firmware is identical on all chassis associated with chassis profiles that use the same policy. Therefore, if you move the chassis profile from one chassis to another, the firmware

versions are maintained. Also, if you change the firmware version for an endpoint in the chassis firmware package, new versions are applied to all the affected chassis profiles immediately.

For a chassis firmware package to take effect, include this policy in a chassis profile, and associate that chassis profile with a chassis.

This policy is not dependent upon any other policies. Ensure that the appropriate firmware has been downloaded to the fabric interconnect. If the firmware image is not available when Cisco UCS Manager is associating a chassis with a chassis profile, Cisco UCS Manager ignores the firmware upgrade and completes the association.

Stages of a Firmware Upgrade through Chassis Firmware Packages in Chassis Profiles

You can use the chassis firmware package policies in chassis profiles to upgrade chassis firmware.

Caution If you modify a chassis firmware package by adding an endpoint or changing firmware versions for an existing endpoint, Cisco UCS Manager upgrades the endpoints after you acknowledge the change by clicking **Pending Activities**. This process disrupts data traffic to and from the chassis.

New Chassis Profile

For a new chassis profile, this upgrade takes place over the following stages:

Chassis Firmware Package Policy Creation

During this stage, you create the chassis firmware package.

Chassis Profile Association

During this stage, you include the chassis firmware package in a chassis profile, and then associate the chassis profile with a chassis. The system pushes the selected firmware versions to the endpoints. The chassis must be reacknowledged to ensure that the endpoints are running the versions specified in the firmware package.

Existing Chassis Profile

For chassis profiles that are associated with a chassis, Cisco UCS Manager upgrades the firmware after you acknowledge the change by clicking **Pending Activities**.

Effect of Updates to Firmware Packages in Chassis Profiles

To update firmware through a chassis firmware package in a chassis profile, you need to update the firmware in the package. What happens after you save the changes to a firmware package depends upon how the Cisco UCS domain is configured.

The following table describes the most common option for upgrading chassis with a firmware package in a chassis profile.

Chassis Profile	Maintenance Policy	Upgrade Actions
The chassis firmware package is included in one or more chassis profiles, and each chassis profile is associated with one chassis. OR The chassis firmware package is included in an updating chassis profile template, and the chassis profile created from that template is associated with one chassis.	Configured for user acknowledgment	The following occurs when you update the chassis firmware package: 1. Cisco UCS asks you to confirm your change and advises that a user-acknowledgement of the chassis is required. 2. Click the flashing **Pending Activities** button to select the chassis you want to reacknowledge, and apply the new firmware. 3. Cisco UCS verifies the model numbers and vendor against all chassis associated with chassis profiles that include this policy. If the model numbers and vendor match a firmware version in the policy, Cisco UCS reacknowledges the chassis and updates the firmware. A manual reacknowledgment of the chassis does not cause Cisco UCS to apply the chassis firmware package, nor does it cancel the pending activities. You must acknowledge or cancel the pending activity through the **Pending Activities** button.

Creating or Updating a Chassis Firmware Package

Tip You can include more than one type of firmware in the same chassis firmware package. For example, a chassis firmware package can include both board controller firmware and chassis adapter firmware for two different models of adapters. However, you can only have one firmware version with the same type, vendor, and model number. The system recognizes which firmware version is required for an endpoint and ignores all other firmware versions.

You can also exclude firmware of specific components from a chassis firmware package either when creating a new chassis firmware package or when modifying an existing chassis firmware package.

Important Each chassis firmware package is associated with one list of excluded components, which is common across all firmware packages.

Before you begin

Ensure that the appropriate firmware was downloaded to the fabric interconnect.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 2	UCS-A org/ # **create fw-chassis-pack** *pack-name*	Creates a chassis firmware package with the specified package name and enters organization firmware chassis package mode.
Step 3	(Optional) UCS-A org/fw-chassis-pack* # **set chassispack-vers** *version-num*	Specifies the package image version number. Changing this number triggers firmware updates on all components using the firmware through a chassis profile. Use this step only when updating a chassis firmware package, not when creating a package.
Step 4	(Optional) UCS-A org/fw-chassis-pack* # **set servicepack-vers** *servicepack-version-num*	Specifies the service pack version number. You cannot directly upgrade to a service pack without selecting a base chassis pack. The images from the service pack will take precedence over the images from Chassis Package.
Step 5	UCS-A org/fw-chassis-pack* # **create exclude-chassis-component** {**chassis-adaptor** | **chassis-board-controller** | **chassis-management-controller** | **local-disk** | **sas-expander**}	Excludes the specified component from the chassis firmware package. **Note** local-disk is excluded from the chassis firmware package by default.
Step 6	Required: UCS-A org/fw-chassis-pack* # **delete exclude-chassis-component** {**chassis-adapter** | **chassis-board-controller** | **chassis-management-controller** | **local-disk** | **sas-expander**}	Includes the specified component from the chassis firmware package.
Step 7	UCS-A org/fw-chassis-pack* # **commit-buffer**	Commits the transaction.

Example

The following example creates the cp1 chassis firmware package, includes the local disk component, and commits the transaction:

```
UCS-A# scope org
UCS-A /org # create fw-chassis-pack cp1
UCS-A /org/fw-chassis-pack* # delete exclude-chassis-component local-disk
UCS-A /org/fw-chassis-pack/exclude-chassis-component* # commit-buffer
UCS-A /org/fw-chassis-pack/exclude-chassis-component #
```

The following example excludes the chassis board controller component from the cp1 chassis firmware package, and commits the transaction:

```
UCS-A# scope org
UCS-A /org # enter fw-chassis-pack cp1
UCS-A /org/fw-chassis-pack* # create exclude-chassis-component chassis-board
-controller
UCS-A /org/fw-chassis-pack/exclude-chassis-component* # commit-buffer
UCS-A /org/fw-chassis-pack/exclude-chassis-component #
```

The following example adds a service pack to the cp1 chassis firmware package, and commits the transaction:

```
UCS-A# scope org
UCS-A /org # scope fw-chassis-pack cp1
UCS-A /org/fw-chassis-pack # set servicepack-vers 3.1(3)SP1
UCS-A /org/fw-chassis-pack* # commit-buffer
UCS-A /org/fw-chassis-pack #
```

Upgrading a UCS Domain with Cisco UCS S3260 Servers

Before you begin

- Ensure that all the servers nodes are shut down.
- Ensure that the UCS domain has an assigned chassis policy that references a chassis firmware package policy and a chassis maintenance policy.

Procedure

Step 1 Upgrade infrastructure firmware through Auto Install. See Upgrading the Infrastructure Firmware with Auto Install.

Step 2 Update the chassis firmware package policy.

- If you are using the default chassis firmware package policy, update the **default** chassis firmware package policy with the new package version. See Creating or Updating a Chassis Firmware Package, on page 5.
- You can create a new chassis firmware package policy using the new chassis package version, and configure the existing or assigned chassis profile (accept any UserAck). See Creating or Updating a Chassis Firmware Package, on page 5 to create a new chassis firmware package policy.

This process may take 1-2 hours. You can monitor the status in the chassis FSM tab.

Step 3 Update the host firmware. See Upgrading the Server Firmware with Auto Install.

Note Updating the host firmware is possible only through Cisco UCS Manager GUI.

Direct Firmware Upgrade on S3260 Chassis and Server Endpoints

The following sections provide detailed information about upgrading S3260 Chassis and Server endpoints.

S3260 Chassis Endpoints

To trigger firmware upgrade on S3260 Chassis components, use the following order:

1. Update CMC 1 firmware
2. Update CMC 2 firmware
3. Update Chassis Adapter 1 firmware
4. Update Chassis Adapter 2 firmware
5. Update SAS Expander 1 firmware
6. Update SAS Expander 2 firmware
7. Activate SAS Expander 1 firmware
8. Activate SAS Expander 2 firmware
9. Activate CMC 1 firmware
10. Activate CMC 2 firmware
11. Activate Chassis Adapter 1 firmware
12. Activate Chassis Adapter 2 firmware
13. Activate Chassis Board Controller

Note You cannot manually update the firmware for local disk in a chassis. The local disk firmware is updated when you explicitly include it in a chassis firmware package.

Cisco UCS S3260 Server Node Endpoints

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

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

While upgrading firmware, Cisco recommends that you use the following order:

1. Upgrade infrastructure—Cisco UCS Manager software and the fabric interconnects
2. Upgrade chassis and server endpoints

While downgrading firmware, Cisco recommends that you use the following order:

1. Downgrade chassis and server endpoints
2. Downgrade infrastructure—Cisco UCS Manager software and the fabric interconnects

Direct Firmware Upgrade on Chassis Endpoints

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 mode.
Step 2	UCS-A /chassis # **scope sioc** {**1** | **2**}	Enters the specified SIOC.
Step 3	UCS-A /chassis/sioc # **scope cmc**	Enters chassis CMC mode.
Step 4	UCS-A /chassis/sioc/cmc # **update firmware** *version-num*	Updates the selected firmware version on the CMC in the chassis.
Step 5	(Optional) UCS-A /chassis/sioc/cmc* # **commit-buffer**	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 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.

	Command or Action	Purpose
Step 6	(Optional) UCS-A /chassis/sioc/cmc # **show update status**	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 7	UCS-A /chassis/sioc/cmc # **activate firmware** *version-num*	Activates the selected firmware version on the CMC in the server.
Step 8	UCS-A /chassis/sioc/cmc* # **commit-buffer**	Commits the transaction.
Step 9	(Optional) UCS-A /chassis/sioc/cmc # **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	(Optional) CS-A /chassis/sioc/cmc # **show firmware**	Displays the running firmware version, the Update status and the Activate status.

Example

The following example updates and activates the CMC firmware to version 2.0(8.13) in the same transaction, without verifying that the firmware update and firmware activation completed successfully:

```
UCS-A# scope chassis 2
UCS-A# /chassis # scope sioc 1
UCS-A# /chassis/sioc # scope cmc
UCS-A# /chassis/sioc/cmc # update firmware 2.0(8.13)
UCS-A# /chassis/sioc/cmc* # activate firmware 2.0(8.13)
UCS-A# /chassis/sioc/cmc* # commit-buffer
UCS-A# /chassis/sioc/cmc # show firmware
CMC:
    Running-Vers: 2.0(8.13)
    Package Vers: 3.1(2.222)C
    Update-Status: Ready
    Activate-Status: Ready
```

The following example updates the CMC firmware to version 2.0(8.13), 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 sioc 1
UCS-A# /chassis/sioc # scope cmc
UCS-A# /chassis/sioc/cmc # update firmware 2.0(8.13)
UCS-A# /chassis/sioc/cmc* # commit-buffer
UCS-A# /chassis/sioc/cmc # show update status
Status: Ready
UCS-A# /chassis/sioc/cmc # activate firmware 2.0(8.13)
UCS-A# /chassis/sioc/cmc* # commit-buffer
UCS-A# /chassis/sioc/cmc # show activate status
Status: Ready
UCS-A# /chassis/sioc/cmc # show firmware
CMC:
    Running-Vers: 2.0(8.13)
    Package Vers: 3.1(0.344)M
    Update-Status: Ready
    Activate-Status: Ready
```

Updating and Activating the Chassis Adapter Firmware on a Chassis

Updating and activating the chassis 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 sioc** {**1** | **2**}	Enters the specified SIOC.
Step 3	UCS-A /chassis/sioc # **scope adapter**	Enters chassis adapter mode.
Step 4	UCS-A /chassis/sioc/adapter # **show image**	Displays the available software images for the chassis adapter.
Step 5	UCS-A /chassis/sioc/adapter # **update firmware** *version-num*	Updates the selected firmware version on the chassis adapter.
Step 6	(Optional) UCS-A /chassis/sioc/adapter* # **commit-buffer**	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**

	Command or Action	Purpose
		commands in the same transaction; however, if the firmware update does not complete successfully, the firmware activation does not start.
Step 7	(Optional) UCS-A /chassis/sioc/adapter # **show update status**	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 8	UCS-A /chassis/sioc/adapter # **activate firmware** *version-num*	Activates the selected firmware version on the chassis adapter.
Step 9	UCS-A /chassis/sioc/adapter* # **commit-buffer**	Commits the transaction.
Step 10	UCS-A /chassis/sioc/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 11	(Optional) UCS-A /chassis/sioc/adapter # **show firmware**	Displays the running firmware version, the **Update** status and the **Activate** status.

Example

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

```
UCS-A# scope chassis 1
UCS-A# /chassis # scope sioc 2
UCS-A# /chassis/sioc # scope adapter
UCS-A# /chassis/sioc/adapter # show image
Name                                       Type                Version
------------------------------------------ ------------------- -------
ucs-2200.3.1.2.222.gbin                    Chassis Adaptor     3.1(2b)
ucs-2200.3.1.300.102.gbin                  Chassis Adaptor     3.1(300.102)
ucs-m83-8p40-vic.4.1.1.58.gbin             Chassis Adaptor     4.1(1.58)
ucs-pcie-c40q-03.4.1.1.58.gbin             Chassis Adaptor     4.1(1.58)
```

```
UCS-A# /chassis/sioc/adapter # update firmware 3.1(2b)
UCS-A# /chassis/sioc/adapter* # activate firmware 3.1(2b)
UCS-A# /chassis/sioc/adapter* # commit-buffer
UCS-A# /chassis/sioc/adapter # show firmware
Adapter:
    Running-Vers: 3.1(2b)
    Package-Vers:
    Update-Status: Ready
    Activate-Status: Ready
```

The following example updates the chassis adapter firmware, verifies that the firmware update completed successfully before starting the firmware activation, activates the chassis adapter firmware, and verifies that the firmware activation completed successfully:

```
UCS-A# scope chassis 1
UCS-A# /chassis # scope sioc 2
UCS-A# /chassis/sioc # scope adapter
UCS-A# /chassis/sioc/adapter # show image
Name                                       Type                Version
------------------------------------------ ------------------- -------
ucs-2200.3.1.2.222.gbin                    Chassis Adaptor     3.1(2b)
ucs-2200.3.1.300.102.gbin                  Chassis Adaptor     3.1(300.102)
ucs-m83-8p40-vic.4.1.1.58.gbin             Chassis Adaptor     4.1(1.58)
ucs-pcie-c40q-03.4.1.1.58.gbin             Chassis Adaptor     4.1(1.58)

UCS-A# /chassis/sioc/adapter # update firmware 3.1(2b)
UCS-A# /chassis/sioc/adapter* # commit-buffer
UCS-A# /chassis/sioc/adapter # show update status
Status: Ready
UCS-A# /chassis/sioc/adapter # activate firmware 3.1(2b)
UCS-A# /chassis/sioc/adapter* # commit-buffer
UCS-A# /chassis/sioc/adapter # show activate status
Status: Ready
UCS-A# /chassis/sioc/adapter # show firmware
Adapter:
    Running-Vers: 3.1(2b)
    Package-Vers:
    Update-Status: Ready
    Activate-Status: Ready
```

Updating and Activating the SAS Expander 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 mode.
Step 2	UCS-A /chassis # **scope sas-expander** *sas-id*	Enters chassis SAS expander mode for the specified SAS expander.
Step 3	UCS-A /chassis/sas-expander # **update firmware** *version-num*	Updates the selected firmware version on the specified SAS expander in the chassis.
Step 4	(Optional) UCS-A /chassis/sas-expander* # **commit-buffer**	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 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	(Optional) UCS-A /chassis/sas-expander # **show update status**	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/sas-expander # **activate firmware** *version-num*	Activates the selected firmware version on the specified SAS expander in the chassis.
Step 7	UCS-A /chassis/sas-expander* # **commit-buffer**	Commits the transaction.
Step 8	(Optional) UCS-A /chassis/sas-expander # **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.

	Command or Action	Purpose
Step 9	(Optional) UCS-A /chassis/sas-expander # **show firmware**	Displays the running firmware version, the Update status and the Activate status.

Example

The following example updates and activates the SAS expander firmware to version 3.1(2b) in the same transaction, without verifying that the firmware update and firmware activation completed successfully:

```
UCS-A# scope chassis 2
UCS-A# /chassis # scope sas-expander
UCS-A# /chassis/sas-expander # update firmware 3.1(2b)
UCS-A# /chassis/sas-expander* # activate firmware 3.1(2b)
UCS-A# /chassis/sas-expander* # commit-buffer
UCS-A# /chassis/sas-expander # show firmware
Running-Vers    Package-Vers    Activate-Status
--------------- --------------- ---------------
3.1(2b)                         Ready
```

The following example updates the SAS expander firmware to version 3.1(2b), verifies that the firmware update completed successfully before starting the firmware activation, activates the SAS expander firmware, and verifies that the firmware activation completed successfully:

```
UCS-A# scope chassis 2
UCS-A# /chassis # scope sas-expander
UCS-A# /chassis/sas-expander # update firmware 3.1(2b)
UCS-A# /chassis/sas-expander* # commit-buffer
UCS-A# /chassis/sas-expander # show update status
Status: Ready
UCS-A# /chassis/sas-expander # activate firmware 3.1(2b)
UCS-A# /chassis/sas-expander* # commit-buffer
UCS-A# /chassis/sas-expander # show activate status
Status: Ready
UCS-A# /chassis/sas-expander # show firmware
    Running-Vers: 3.1(2b)
    Package Vers: 3.1(2b)
    Update-Status: Ready
    Activate-Status: Ready
```

Activating the Board Controller Firmware on a Chassis

Note Cisco UCS Manager does not support activation of board controller firmware to earlier versions.

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 sioc** {1 | 2}	Enters the specified SIOC in the chassis.
Step 3	UCS-A /chassis/sioc #**scope boardcontroller**	Enters board controller mode for the chassis.
Step 4	UCS-A /chassis/sioc/boardcontroller # **activate firmware** *version-num*	Activates the selected firmware version on the board controller in the chassis.
Step 5	UCS-A /chassis/sioc/boardcontroller* # **commit-buffer**	Commits the transaction to the system configuration.
Step 6	UCS-A /chassis/sioc/boardcontroller # **show firmware**	Displays the running firmware version and the activate status.

Example

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

```
UCS-A# scope chassis 1
UCS-A /chassis # scope sioc 1
UCS-A /chassis/sioc # scope boardcontroller
UCS-A /chassis/sioc/boardcontroller # activate firmware 3.1.211
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/sioc/boardcontroller* # commit-buffer
UCS-A /chassis/sioc/boardcontroller # show firmware
Board Controller:
    Running-Vers: NA
    Package-Vers: 3.1(2b)C
    Activate-Status: Ready
UCS-A /chassis/boardcontroller* #
```

Direct Firmware Upgrade on Server Endpoints

Updating and Activating the CIMC Firmware on a Cisco UCS S3260 Storage 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* / *server-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	(Optional) UCS-A /chassis/server/cimc* # **commit-buffer**	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	(Optional) UCS-A /chassis/server/cimc # **show firmware**	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.

	Command or Action	Purpose
Step 8	UCS-A /chassis/server/cimc* # **commit-buffer**	Commits the transaction.
Step 9	(Optional) UCS-A /chassis/server/cimc # **show firmware**	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.

Example

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

```
UCS-A# scope server 3/1
UCS-A# /chassis/server # scope cimc
UCS-A# /chassis/server/cimc # show image
Name                                       Type               Version
------------------------------------------ ------------------ -------
ucs-b200-m1-k9-cimc.3.1.20.26.gbin         CIMC               3.1(20.26)
ucs-b200-m3-k9-cimc.3.1.20.26.gbin         CIMC               3.1(20.26)
ucs-b200-m4-k9-cimc.3.1.20.26.gbin         CIMC               3.1(20.26)
ucs-b22-m3-k9-cimc.3.1.20.26.gbin          CIMC               3.1(20.26)
ucs-b230-m2-k9-cimc.3.1.20.26.gbin         CIMC               3.1(20.26)
ucs-b250-m1-k9-cimc.3.1.20.26.gbin         CIMC               3.1(20.26)
ucs-b420-m3-k9-cimc.3.1.20.26.gbin         CIMC               3.1(20.26)
ucs-b420-m4-k9-cimc.3.1.20.26.gbin         CIMC               3.1(20.26)
ucs-b440-m2-k9-cimc.3.1.20.26.gbin         CIMC               3.1(20.26)
ucs-c22-k9-cimc.2.0.12.73.gbin             CIMC               2.0(12.73)
ucs-c220-k9-cimc.2.0.12.73.gbin            CIMC               2.0(12.73)
ucs-c220-m4-k9-cimc.2.0.12.73.gbin         CIMC               2.0(12.73)
ucs-c240-k9-cimc.2.0.12.73.gbin            CIMC               2.0(12.73)
ucs-c240-m4-k9-cimc.2.0.12.73.gbin         CIMC               2.0(12.73)
ucs-c3260-m3-k9-cimc.2.0.12.73.gbin        CIMC               2.0(12.73)
ucs-c3260-m4-k9-cimc.2.0.12.73.gbin        CIMC               2.0(12.73)
ucs-c460-m4-k9-cimc.2.0.12.73.gbin         CIMC               2.0(12.73)
ucs-EXM4-1-k9-cimc.3.1.20.26.gbin          CIMC               3.1(20.26)
ucs-EXM4-2-k9-cimc.3.1.20.26.gbin          CIMC               3.1(20.26)


...

UCS-A# /chassis/server/cimc # update firmware 2.0(12.73)
UCS-A# /chassis/server/cimc* # activate firmware 2.0(12.73)
UCS-A# /chassis/server/cimc* # commit-buffer
UCS-A# /chassis/server/cimc #
```

The following example updates the CIMC firmware, 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 3/1
```

```
UCS-A# /chassis/server # scope cimc
UCS-A# /chassis/server/cimc # show image
Name                                       Type                Version
------------------------------------------ ------------------- -------
ucs-b200-m1-k9-cimc.3.1.20.26.gbin          CIMC                3.1(20.26)
ucs-b200-m3-k9-cimc.3.1.20.26.gbin          CIMC                3.1(20.26)
ucs-b200-m4-k9-cimc.3.1.20.26.gbin          CIMC                3.1(20.26)
ucs-b22-m3-k9-cimc.3.1.20.26.gbin           CIMC                3.1(20.26)
ucs-b230-m2-k9-cimc.3.1.20.26.gbin          CIMC                3.1(20.26)
ucs-b250-m1-k9-cimc.3.1.20.26.gbin          CIMC                3.1(20.26)
ucs-b420-m3-k9-cimc.3.1.20.26.gbin          CIMC                3.1(20.26)
ucs-b420-m4-k9-cimc.3.1.20.26.gbin          CIMC                3.1(20.26)
ucs-b440-m2-k9-cimc.3.1.20.26.gbin          CIMC                3.1(20.26)
ucs-c22-k9-cimc.2.0.12.73.gbin              CIMC                2.0(12.73)
ucs-c220-k9-cimc.2.0.12.73.gbin             CIMC                2.0(12.73)
ucs-c220-m4-k9-cimc.2.0.12.73.gbin          CIMC                2.0(12.73)
ucs-c240-k9-cimc.2.0.12.73.gbin             CIMC                2.0(12.73)
ucs-c240-m4-k9-cimc.2.0.12.73.gbin          CIMC                2.0(12.73)
ucs-c3260-m3-k9-cimc.2.0.12.73.gbin         CIMC                2.0(12.73)
ucs-c3260-m4-k9-cimc.2.0.12.73.gbin         CIMC                2.0(12.73)
ucs-c460-m4-k9-cimc.2.0.12.73.gbin          CIMC                2.0(12.73)
ucs-EXM4-1-k9-cimc.3.1.20.26.gbin           CIMC                3.1(20.26)
ucs-EXM4-2-k9-cimc.3.1.20.26.gbin           CIMC                3.1(20.26)
...

UCS-A# /chassis/server/cimc # update firmware 2.0(12.73)
UCS-A# /chassis/server/cimc* # commit-buffer
UCS-A# /chassis/server/cimc # show firmware
Running-Vers    Update-Status   Activate-Status
--------------- --------------- ---------------
2.0(12.73)      Updating        Ready

UCS-A# /chassis/server/cimc # show firmware
Running-Vers    Update-Status   Activate-Status
--------------- --------------- ---------------
2.0(12.73)      Ready           Ready

UCS-A# /chassis/server/cimc # activate firmware 2.0(12.73)
UCS-A# /chassis/server/cimc* # commit-buffer
UCS-A# /chassis/server/cimc # show firmware
Running-Vers    Update-Status   Activate-Status
--------------- --------------- ---------------
2.0(12.73)      Ready           Activating

UCS-A# /chassis/server/cimc # show firmware
Running-Vers    Update-Status   Activate-Status
--------------- --------------- ---------------
2.0(12.73)      Ready           Ready
```

Updating and Activating the BIOS Firmware on a Cisco UCS S3260 Storage Server

Important You can update and activate BIOS firmware on a server using the Cisco UCS Manager CLI on all servers.

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* / *server-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	(Optional) UCS-A /chassis/server/bios* # **commit-buffer**	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	(Optional) UCS-A /chassis/server/bios # **show firmware**	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/bios # **activate firmware** *version-num*	Activates the selected server BIOS firmware version.

	Command or Action	Purpose
Step 8	UCS-A /chassis/server/bios* # **commit-buffer**	Commits the transaction.
Step 9	(Optional) UCS-A /chassis/bios # **show firmware**	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.

Example

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 3/1
UCS-A# /chassis/server # scope bios
UCS-A# /chassis/server/bios # show image
Name                                        Type          Version
------------------------------------------- ------------- -------
ucs-b200-m2-bios.S5500.2.1.3c.0.0151437.bin   Server BIOS   S5500.2.1.3c.
                                                                  0.081120151437
ucs-b200-m3-bios.B200M3.2.2.6d.0.160055.bin   Server BIOS   B200M3.2.2.6d

.0.062220160055
ucs-b200-m4-bios.B200M4.3.1.3c.0.161459.bin   Server BIOS   B200M4.3.1.3c

.0.080120161459
ucs-b200-m4-bios.B200M4.3.1.3e.0.161737.bin   Server BIOS   B200M4.3.1.3e

.0.081120161737
ucs-b22-m3-bios.B22M3.2.2.6d.0.20160114.bin   Server BIOS   B22M3.2.2.6d.
                                                                  0.062220160114
ucs-b230-m2-bios.B230.2.1.3a.0.20151410.bin   Server BIOS   B230.2.1.3a.0
                                                                   .022420151410
ucs-b250-m2-bios.S5500.2.1.3d.0.0161035.bin   Server BIOS   S5500.2.1.3d.
                                                                  0.032520161035
ucs-b420-m3-bios.B420M3.2.2.6e.0.160138.bin   Server BIOS   B420M3.2.2.6e.0.062220160138
ucs-b420-m4-bios.B420M4.3.1.2a.0.161234.bin   Server BIOS   B420M4.3.1.2a.0.072520161234
ucs-b420-m4-bios.B420M4.3.1.2d.0.161622.bin   Server BIOS   B420M4.3.1.2d.0.081120161622
ucs-b440-m2-bios.B440.2.1.3a.0.20151142.bin   Server BIOS   B440.2.1.3a.0.022420151142
ucs-c22-bios.C22M3.2.0.13a.0.0713160955.bin   Server BIOS   C22M3.2.0.13a.0.0713160955
ucs-c220-bios.C220M3.2.0.13a.0.13160937.bin   Server BIOS   C220M3.2.0.13a.0.0713160937
ucs-c220-m4-bios.C220M4.2.0.13a.0.62332.bin   Server BIOS   C220M4.2.0.13a.0.0725162332
ucs-c220-m4-bios.C220M4.2.0.13b.0.61705.bin   Server BIOS   C220M4.2.0.13b.0.0805161705
ucs-c240-bios.C240M3.2.0.13a.0.13160947.bin   Server BIOS   C240M3.2.0.13a.0.0713160947
ucs-c240-m4-bios.C240M4.2.0.13a.0.62345.bin   Server BIOS   C240M4.2.0.13a.0.0725162345
ucs-c240-m4-bios.C240M4.2.0.13b.0.61722.bin   Server BIOS   C240M4.2.0.13b.0.0805161722
ucs-c3260-m3-bios.C3X60M3.2.0.13a.0.044.bin   Server BIOS   C3X60M3.2.0.13a.0.0722160044
ucs-c3260-m4-bios.C3X60M4.2.0.13a.0.350.bin   Server BIOS   C3X60M4.2.0.13a.0.0801162350
ucs-c460-m4-bios.C460M4.2.0.13a.0.60447.bin   Server BIOS   C460M4.2.0.13a.0.072720160447
ucs-c460-m4-bios.C460M4.2.0.13b.0.62321.bin   Server BIOS   C460M4.2.0.13b.0.080320162321
ucs-EXM4-1-bios.EXM4.2.2.7.0.1520161539.bin   Server BIOS   EXM4.2.2.7.0.021520161539
ucs-EXM4-2-bios.EXM4.2.2.7.0.1520161539.bin   Server BIOS   EXM4.2.2.7.0.021520161539
ucs-EXM4-3-bios.EXM4.3.1.2b.0.020161506.bin   Server BIOS   EXM4.3.1.2b.0.062020161506
```

```
UCS-A# /chassis/server/bios # update firmware C3X60M4.2.0.12.11.041320162312
UCS-A# /chassis/server/bios* # activate firmware C3X60M4.2.0.12.11.041320162312
UCS-A# /chassis/server/bios* # commit-buffer
UCS-A# /chassis/server/bios #
```

Activating the Board Controller Firmware on a Cisco UCS S3260 Storage 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	(Optional) UCS-A /chassis/server/boardcontroller # **show image**	Displays the available software images for the board controller.
Step 4	(Optional) UCS-A /chassis/server/boardcontroller # **show firmware**	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.

Example

The following example activates the board controller firmware:

```
UCS-A# scope server 3/1
UCS-A# /chassis/server # scope boardcontroller
UCS-A# /chassis/server/boardcontroller # show image
Name                                       Type                 Version
------------------------------------------ -------------------- -------
ucs-4308-brdprog.1.0.12.gbin               Chassis Board Controller
                                                                1.0.12
ucs-b200-m3-brdprog.15.0.gbin              Board Controller     15.0
```

```
ucs-b200-m4-brdprog.12.0.gbin                Board Controller     12.0
ucs-b22-m3-brdprog.17.0.gbin                 Board Controller     17.0
ucs-b230-m2-pld.B230100D.gbin                Board Controller     B230100D
ucs-b250-m1-pld.111026-111026.gbin           Board Controller     111026-111026

ucs-b420-m3-brdprog.12.0.gbin                Board Controller     12.0
ucs-b420-m4-brdprog.6.0.gbin                 Board Controller     6.0
ucs-b440-m2-pld.B440100C-B4402008.gbin       Board Controller     B440100C-B440
                                                                                2008
ucs-c22-m3-brdprog.5.0.gbin                  Board Controller     5.0
ucs-c220-m3-brdprog.5.0.gbin                 Board Controller     5.0
ucs-c220-m4-brdprog.27.0.gbin                Board Controller     27.0
ucs-c240-m3-brdprog.5.0.gbin                 Board Controller     5.0
ucs-c240-m4-brdprog.24.0.gbin                Board Controller     24.0
ucs-c3260-brdprog.1.0.11.gbin                Board Controller     1.0.11
ucs-c3260-m3-brdprog.2.0.gbin                Board Controller     2.0
ucs-c460-m4-brdprog.16.0.gbin                Board Controller     16.0
ucs-EXM4-1-brdprog.7.0.gbin                  Board Controller     7.0
ucs-EXM4-2-brdprog.5.0.gbin                  Board Controller     5.0


UCS-A# /chassis/server/boardcontroller # show firmware
BoardController:
    Running-Vers: 1.0.11
    Package-Vers: 3.1(2)B
    Activate-Status: Ready

UCS-A# /chassis/server/boardcontroller # activate firmware 1.0.11
UCS-A# /chassis/server/boardcontroller* # commit-buffer
```