Firmware Management

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

Chassis Firmware Upgrade through Auto Install

Cisco UCS Manager Release 3.2(3) introduces support for upgrading chassis firmware through Auto Install on Cisco UCS S3260 chassis. This ability enables you to upgrade all chassis components in a Cisco UCS domain through a single chassis firmware package.

Upgrading the Chassis Firmware with Auto Install

You can upgrade chassis firmware by specifying a Chassis Firmware package.

If you staged the chassis firmware through **Prepare for Firmware Install**, and that backup version is the same as the selected chassis firmware version in this procedure, the backup version is set as the startup version.

If you did not set the backup version earlier, the selected firmware version is set as the backup version. This version is then set as the startup version.

Completing this stage will result in a reboot.

Note You cannot use Auto Install to upgrade the chassis in a Cisco UCS domain if Cisco UCS Manager in that domain is at a release prior to Cisco UCS Manager 3.2(3). For more information, see the *Cautions and Guidelines for Upgrading with Auto Install* section in the *Cisco UCS Manager Firmware Management Guide, Release 3.2*.

You cannot cancel a chassis firmware upgrade process after you complete the configuration in the **Install Chassis Firmware** wizard. Cisco UCS Manager applies the changes immediately.

Before you begin

- Complete all prerequisites listed in the *Prerequisites for Upgrading and Downgrading Firmware* section of the *Cisco UCS Manager Firmware Management Guide, Release 3.2*.
- Stage the Chassis firmware if using Cisco UCS Manager Release 3.2(3) or later releases. The *Preparing for Firmware Install* section of the *Cisco UCS Manager Firmware Management Guide, Release 3.2*, provides detailed information about staging the chassis firmware.

Note Although this is optional, it is also recommended.

Procedure

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

Step 2 Click the **Equipment** node.

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

Step 4 In the **Work** pane, click the **Firmware Auto Install** tab.

Step 5 In the **Actions** area, click **Install Chassis Firmware**.

Step 6 On the **Prerequisites** page of the **Install Chassis Firmware** wizard, carefully review the prerequisites and guidelines listed on this page and then do one of the following:

- If you have completed all of the prerequisites, click **Next**.
- If you have not completed all of the prerequisites, click **Cancel** and complete the prerequisites before you upgrade the chassis firmware.

Step 7 On the **Select Package Versions** page of the **Install Chassis Firmware** wizard, do the following:

a) Choose the software bundle to which you want to upgrade these chassis from the **New Version** drop-down list in the **Chassis Firmware** area.

b) To upgrade the chassis to a service pack firmware version, choose the service pack to which you want to upgrade these chassis from the **New Version** drop-down list in the **Service-Pack Firmware** area.

c) Click **Next**.

Step 8 On the **Select Firmware Packages** page of the **Install Chassis Firmware** wizard, do the following:

a) Expand the node for each organization that contains a chassis firmware package you want to update with the selected software.

If the firmware version for a chassis firmware package is staged, it appears as the **Backup Version** along with the name of the chassis firmware package.

b) Check the check box next to the name of each chassis firmware package that you want to update.

This step updates the selected chassis firmware package with the new version of firmware. You must choose the chassis firmware packages included in the chassis profiles associated with all chassis in the Cisco UCS domain to update all chassis.

c) Click **Next**.

Step 9 On the **Firmware Package Dependencies** page of the **Install Chassis Firmware** wizard, do the following:

a) Expand the node for each chassis firmware package listed in the table.
b) Review the list of chassis profiles that include the chassis firmware package.
c) If desired, click a link in one of the following columns:

- **Chassis Pack DN** column—Opens the navigator for the chassis firmware package.
- **Chassis Profile DN** column—Opens the navigator for the chassis profile.

d) Do one of the following:

- If you want to change one or more of the selected chassis firmware packages, click **Prev**.
- If you are satisfied that you have selected the appropriate chassis firmware packages and want to review the impact of the chassis firmware upgrade on the endpoints, click **Next**.
- If you want to start the chassis upgrade immediately, click **Install**.

Step 10 On the **Impacted Endpoints Summary** page of the **Install Chassis Firmware** wizard, do the following:

a) Click the appropriate check boxes to filter the results in the **Impacted Endpoints** table.

You can filter the results by the type of endpoint and by whether the impact of the upgrade is disruptive or not.

b) Review the list of impacted endpoints.
c) If desired, click the link in the **Maintenance Policy** column to open the navigator for that policy.
d) Do one of the following:

- If you want to change one or more of the selected chassis firmware packages, click **Prev**.
- If you are satisfied that you have selected the appropriate chassis firmware packages and want to start the chassis upgrade, click **Install**.

Step 11 (Optional) To check on the progress of the chassis firmware upgrade, check the **FSM** tab for each chassis that you are upgrading.

The **Firmware Installer** field on the **Firmware Auto Install** tab shows only the status of an infrastructure firmware upgrade.

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 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.

Before you begin

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

Procedure

Step 1 In the **Navigation** pane, click **Chassis**.

Step 2 Expand **Chassis** > **Policies**.

Step 3 Expand the node for the organization where you want to create the policy.

If the system does not include multi tenancy, expand the **root** node.

Step 4 Right-click **Chassis Firmware Packages** and choose **Create Chassis Firmware Package**.

Step 5 In the **Create Chassis Firmware Package** dialog box, enter a unique name and description for the package.

This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.

Step 6 From each drop-down list, **Chassis Package**, and **Service Pack**, select the firmware package.

The images from **Service Pack** will take precedence over the images from **Chassis Package**.

Step 7 In the **Excluded Components** area, check the check boxes corresponding to the components that you want to exclude from this chassis firmware package.

If you do not check any component check boxes, all the listed components are included in the chassis firmware package.

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

Step 8 Click **OK**.

What to do next

Include the policy in a chassis profile or chassis profile template

Updating a Chassis Firmware Package

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.

Before you begin

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

Procedure

Step 1 In the **Navigation** pane, click **Chassis**.

Step 2 Expand **Chassis** > **Policies**.

Step 3 Expand the node for the organization that includes the policy you want to update.

If the system does not include multi tenancy, expand the **root** node.

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

Step 5 In the **Work** pane, click the **General** tab.

Step 6 To modify the components in the chassis firmware package, click **Modify Package Versions**.

The **Modify Package Versions** window appears.

Step 7 To modify the chassis package, from the **Chassis Package** drop-down list, select the chassis package version.

Step 8 To modify the service pack, from the **Service Pack** drop-down list, select the service pack version.

To remove the service pack, select **<not set>**.

Step 9 In the **Excluded Components** area, check the check boxes corresponding to the components that you want to exclude from this chassis firmware package.

If you do not check any component check boxes, all the listed components are included in the chassis firmware package.

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

Step 10 Click **OK**.

Adding Chassis Firmware Packages to an Existing Chassis Profile

If the chassis profile is associated with a chassis, Cisco UCS Manager updates and activates the firmware in the chassis with the new versions after a user acknowledgment.

Procedure

Step 1 In the **Navigation** pane, click **Chassis**.

Step 2 Expand **Chassis** > **Chassis Profiles**.

Step 3 Expand the node for the organization that includes the chassis profile that you want to update.

If the system does not include multi tenancy, expand the **root** node.

Step 4 Click the chassis profile to which you want to add the chassis firmware package.

Step 5 In the **Work** pane, click the **Policies** tab.

Step 6 Click the down arrows to expand the **Chassis Firmware Package** section.

Step 7 To add a chassis firmware package, select the desired policy from the **Chassis Firmware Package** drop-down list.

Step 8 Click **Save Changes**.

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 Updating a Chassis Firmware Package, on page 9.
- 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 a Chassis Firmware Package, on page 8 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.

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:

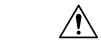
1. Upgrade infrastructure—Cisco UCS Manager software and the fabric interconnects
2. Upgrade chassis and server endpoints

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 the CMC Firmware on a S3260 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

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

Step 2 Expand **Equipment** > **Chassis** > ***Chassis Number***

Step 3 In the **Work** pane, click the **Installed Firmware** tab, select **Chassis Management Controller**, and then click **Update Firmware**.

Step 4 In the **Update Firmware** dialog box, do the following:

a) From the **Version** drop-down list, select the firmware version to update the endpoint.

b) Click **OK**.

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

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

Step 5 (Optional) Monitor the status of the update in the **Update Status** area.

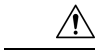
The update process can take several minutes. Do not activate the firmware until the selected firmware package displays in the **Backup Version** field in the **Installed Firmware** tab.

What to do next

Activate the firmware.

Updating the Chassis Adapter Firmware on a S3260 Chassis

If the adapter connectivity to both fabric interconnects is down, upgrade is skipped.



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

Procedure

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

Step 2 Expand **Equipment** > **Chassis** > **Chassis** ***Number***

Step 3 In the **Installed Firmware** tab, select **Chassis Adapter** and click **Update Firmware**.

Step 4 In the **Update Firmware** dialog box, do the following:

a) From the **Version** drop-down list, select the firmware version to update the endpoint.

b) Click **OK**.

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

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

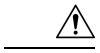
Step 5 (Optional) Monitor the status of the update in the **Update Status** area.

The update process can take several minutes. Do not activate the firmware until the selected firmware package displays in the **Backup Version** field in the **Installed Firmware** tab.

What to do next

Activate the firmware.

Updating the SAS Expander Firmware on a S3260 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

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

Step 2 Expand **Equipment** > **Chassis** > **Chassis** ***Number***

Step 3 In the **Installed Firmware** tab, select the SAS expander that you want to update and click **Update Firmware**.

Step 4 In the **Update Firmware** dialog box, do the following:

a) From the **Version** drop-down list, select the firmware version to update the endpoint.

b) Click **OK**.

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

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

Step 5 (Optional) Monitor the status of the update in the **Update Status** area.

The update process can take several minutes. Do not activate the firmware until the selected firmware package displays in the **Backup Version** field in the **Installed Firmware** tab.

What to do next

Activate the firmware.

Activating the SAS Expander Firmware on a S3260 Chassis

Procedure

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

Step 2 Expand **Equipment** > **Chassis** > **Chassis** ***Number***

Step 3 In the **Installed Firmware** tab, select the SAS Expander that you want to update and click **Activate Firmware**.

Step 4 In the **Activate Firmware** dialog box, do the following:

a) Select the appropriate version from the **Set Version** drop-down list.

If one or more of the selected endpoints are not configured with the version that you want as the backup version, the version does not display in the **Set Version** drop-down list. You must select the version from the **Startup Version** column for each individual endpoint.

b) Click **OK**.

Activating the CMC Firmware on a S3260 Chassis

Procedure

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

Step 2 Expand **Equipment** > **Chassis** > **Chassis** ***Number***

Step 3 In the **Installed Firmware** tab, select **Chassis Management Controller** and then click **Activate Firmware**.

Step 4 In the **Activate Firmware** dialog box, do the following:

a) Select the appropriate version from the **Set Version** drop-down list.

If one or more of the selected endpoints are not configured with the version that you want as the backup version, the version does not display in the **Set Version** drop-down list. You must select the version from the **Startup Version** column for each individual endpoint.

b) Click **OK**.

Activating the Chassis Adapter Firmware on a S3260 Chassis

Procedure

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

Step 2 Expand **Equipment** > **Chassis** > **Chassis** ***Number***

Step 3 In the **Installed Firmware** tab, select **Chassis Adapter** and then click **Activate Firmware**.

Step 4 In the **Activate Firmware** dialog box, do the following:

a) Select the appropriate version from the **Set Version** drop-down list.

If one or more of the selected endpoints are not configured with the version that you want as the backup version, the version does not display in the **Set Version** drop-down list. You must select the version from the **Startup Version** column for each individual endpoint.

b) Click **OK**.

Activating the Chassis Board Controller Firmware on a S3260 Chassis

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

Procedure

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

Step 2 Expand **Equipment** > **Chassis** > **Chassis** ***Number***

Step 3 In the **Installed Firmware** tab, select **Board Controller** and then click **Activate Firmware**.

Step 4 In the **Activate Firmware** dialog box, do the following:

a) Select the appropriate version from the **Set Version** drop-down list.

If one or more of the selected endpoints are not configured with the version that you want as the backup version, the version does not display in the **Set Version** drop-down list. You must select the version from the **Startup Version** column for each individual endpoint.

b) Click **OK**.

Direct Firmware Upgrade on Server Endpoints

Updating the CIMC Firmware on a Cisco UCS S3260 Server Node

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

Procedure

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

Step 2 Expand **Equipment** > **Chassis** > ***Chassis Number*** > **Servers**.

Step 3 Expand the node for the server for which you want to update the CIMC.

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

Step 5 Click the **CIMC** tab.

Step 6 In the **Actions** area, click **Update Firmware**.

Step 7 In the **Update Firmware** dialog box, do the following:

a) From the **Version** drop-down list, select the firmware version to update the endpoint.

b) Click **OK**.

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

Step 8 (Optional) Monitor the status of the update in the **Update Status** area.

The update process can take several minutes. Do not activate the firmware until the selected firmware package displays in the **Backup Version** field in the **Firmware** area of the **General** tab.

What to do next

Activate the firmware.

Activating the CIMC Firmware on a Cisco UCS S3260 Server Node

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

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

Procedure

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

Step 2 Expand **Equipment** > **Chassis** > ***Chassis Number*** > **Servers**.

Step 3 Expand the node for the server that includes the CIMC for which you want to activate the updated firmware.

Step 4 On the **Work** pane, click the **Inventory** tab.

Step 5 Click the **CIMC** tab.

Step 6 In the **Actions** area, click **Activate Firmware**.

Step 7 In the **Activate Firmware** dialog box, do the following:

a) Select the appropriate version from the **Version To Be Activated** drop-down list.

If one or more of the selected endpoints are not configured with the required version as the backup version, that version does not display in the **Set Version** drop-down list. You must select the version from the **Startup Version** column for each individual endpoint.

b) If you want to set the startup version and not change the version running on the endpoint, check the **Set Startup Version Only** check box.

If you configure **Set Startup Version Only**, the activated firmware moves to the pending-next-reboot state and the endpoint is not immediately rebooted. The activated firmware does not become the running version of firmware until the endpoint reboots.

c) Click **OK**.

Updating the BIOS Firmware on a Cisco UCS S3260 Server Node

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

Procedure

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

Step 2 Expand **Equipment** > **Chassis** > ***Chassis Number*** > **Servers**.

Step 3 Expand the node for the server for which you want to update the BIOS firmware.

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

Step 5 Click the **Motherboard** tab.

Step 6 In the **Actions** area, click **Update BIOS Firmware**.

Step 7 In the **Update Firmware** dialog box, do the following:

a) From the **Version** drop-down list, select the firmware version to which you want to update the server BIOS.

b) (Optional) If you want to update the firmware regardless of any possible incompatibilities or currently executing tasks, check the **Force** check box.

c) Click **OK**.

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

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

What to do next

Activate the firmware.

Activating the BIOS Firmware on a Cisco UCS S3260 Server Node

Procedure

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

Step 2 Expand **Equipment** > **Chassis** > ***Chassis Number*** > **Servers**.

Step 3 Expand the node for the server for which you want to activate the updated BIOS firmware.

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

Step 5 Click the **Motherboard** tab.

Step 6 In the **Actions** area, click **Activate BIOS Firmware**.

Step 7 In the **Activate Firmware** dialog box, do the following:

a) Select the appropriate server BIOS version from the **Version To Be Activated** drop-down list.

b) If you want to set the startup version and not change the version running on the server, check the **Set Startup Version Only** check box.

If you configure **Set Startup Version Only**, the activated firmware moves into the pending-next-reboot state and the server is not immediately rebooted. The activated firmware does not become the running version of firmware until the server is rebooted.

c) Click **OK**.

Activating the Board Controller Firmware on a Cisco UCS S3260 Server Node

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

Procedure

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

Step 2 Click the **Equipment** node.

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

Step 4 On the **Installed Firmware** tab, click **Activate Firmware**.

Cisco UCS Manager GUI opens the **Activate Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS domain. This step might take a few minutes, based on the number of chassis and servers.

Step 5 From the **Filter** drop-down list on the menu bar of the **Activate Firmware** dialog box, select **Board Controller**.

Cisco UCS Manager GUI displays all servers that have board controllers in the **Activate Firmware** dialog box.

Step 6 For the board controller you want to update, select a version from the **Startup Version** drop-down list.

Step 7 Click **OK**.

Step 8 (Optional) You can also use the **Force Board Controller Activation** option to update the firmware version when you upgrade CPUs with different architectures.

Activating the Storage Controller Firmware on a Cisco UCS S3260 Server Node

Procedure

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

Step 2 Expand **Equipment** > **Chassis** > ***Chassis Number*** > **Servers**.

Step 3 Select the server on which you want to activate the storage controller.

Step 4 In the **Installed Firmware** tab, select **Storage Controller** and then click **Activate Firmware**.

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

a) Select the appropriate version from the **Set Version** drop-down list.

If one or more of the selected endpoints are not configured with the version that you want as the backup version, the version does not display in the **Set Version** drop-down list. You must select the version from the **Startup Version** column for each individual endpoint.

b) Click **OK**.