Firmware Management

This chapter includes the following sections:

Overview of Firmware

Cisco UCS uses firmware obtained from and certified by Cisco to upgrade firmware on the following components:

- Servers, including the BIOS, storage controller, and server controller (BMC)
- Adapters, including NIC and HBA firmware, and Option ROM (where applicable)
- I/O modules
- Fabric interconnects
- Cisco UCS Manager

Cisco maintains a set of best practices for managing firmware images and updates in the following technical note: Unified Computing System Firmware Management Best Practices.

Image Management

Cisco delivers all firmware updates or packages to Cisco UCS components in images. These images can be the following:

- Component image, which contains the firmware for one component
- Package, which is a collection of component images

Cisco also provides release notes with each image, which you can obtain from the same website from which you obtained the image.

Cisco UCS Manager provides mechanisms to download both component images and packages to the fabric interconnect.

Image Headers

Every image has a header, which includes the following:

- Checksum
- Version information
- Compatibility information that the system can use to verify the compatibility of component images and any dependencies

Image Catalog

Cisco UCS Manager provides you with two views of the catalog of firmware images and their contents that have been downloaded to the fabric interconnect:

Packages This view provides you with a read-only representation of the packages that have been downloaded onto the fabric interconnect. This view is sorted by image, not by the contents of the image. For packages, you can use this view to see which component images are (were) in each downloaded package.

Images The images view lists the component images available on the system. You cannot use this view to see packages. The information available about each component image includes the name of the component, the image size, the image version, and the vendor and model of the component.

You can use this view to identify the firmware updates available for each component. You can also use this view to delete obsolete and unneeded images. Cisco UCS Manager deletes a package after all images in the package have been deleted.

Tip Cisco UCS Manager stores the images in bootflash on the fabric interconnect. In a cluster system, space usage in bootflash on both fabric interconnects is the same, because all images are synchronized between them. If Cisco UCS Manager reports that the bootflash is out of space, delete obsolete images to free up space.

Firmware Updates

You can use any of the Cisco UCS Manager interfaces to update firmware in the system, including Cisco UCS Manager GUI and the Cisco UCS Manager CLI.

You can use either of the following methods to update the firmware:

- Direct update at the endpoints.
- Updates to server components through service profiles that include a host firmware package policy and a management firmware package policy.

Note Direct update is not available for some server components, such as BIOS and storage controller.

Firmware Versions

The firmware versions on a component depend upon the type of component.

Firmware Versions in BMC, I/O Modules, and Adapters

Each BMC, I/O module, and adapter has two slots for firmware in flash. Each slot holds a version of firmware. One slot is active and the other is the backup slot. A component boots from whichever slot is designated as active.

The following firmware version terminology is used in the GUI and CLI:

Running Version	The running version is the firmware that is active and in use by the component.
Startup Version	The startup version is the firmware that will be used when the component next boots up. Cisco UCS Manager provides the activate operation to change the startup version.
Backup Version	The backup version is the firmware that is sitting in the other slot and is not in use by the component. This can be firmware that you have updated to the component but have not yet activated, or it can be an older firmware version that was replaced by a recent activate. Cisco UCS Manager provides the update operation to replace the image in the backup slot.

If the component cannot boot from the startup version, the component boots from the backup version.

Firmware Versions in the Fabric Interconnect and Cisco UCS Manager

You can update the fabric interconnect firmware and Cisco UCS Manager on the fabric interconnect. The fabric interconnect and Cisco UCS Manager firmware do not have backup versions, because all the images are stored on the fabric interconnect. As a result, the number of bootable fabric interconnect images is not limited to two, like the server BMC and adapters. Instead, the number of bootable fabric interconnect images is limited by the available space in the flash memory.

Note There are running and startup versions of the fabric interconnect and Cisco UCS Manager firmware, but there are no backup versions.

Direct Firmware Update at Endpoints

You can perform direct firmware updates on the following endpoints:

- Fabric interconnects
- Cisco UCS Manager
- I/O modules
- BMC
- Adapters

Note You cannot update the BIOS firmware directly. You must perform the BIOS firmware update through a host firmware package in a service profile. If the BIOS fails, you can use Cisco UCS Manager to recover the BIOS.

Stages of a Direct Firmware Update

Cisco UCS Manager separates the direct update process into stages to ensure that you can push the firmware to a component while the system is running without affecting uptime on the server or other components. Because you do not need to reboot the server until after you activate, you can perform that task overnight or during other maintenance periods.

When you manually update firmware, the following stages occur:

Update

During this stage, the system pushes the selected firmware version to the component. The update process always overwrites the firmware in the backup slot on the component. The update stage applies only to I/O modules, BMCs, and adapters.

Activate

During this stage, the system sets the specified image version (normally the backup version) as active and reboots the endpoint. When the endpoint is rebooted, the backup slot becomes the active slot, and the active slot becomes the backup slot. The firmware in the new active slot becomes the startup version and the running version.

If the component cannot boot from the startup firmware, it defaults to the backup version and raises an alarm.

Recommended Order of Components for Firmware Activation

If you upgrade firmware by individual components in a Cisco UCS instance, we recommend that you activate the updates in the following order for quicker activation:

1. Adapter
2. BMC
3. I/O module

4 Fabric interconnect or Cisco UCS Manager

Note Consider the following when activating the firmware:

- You can update all components in parallel.
- While activating adapters and I/O modules, you can use the set-startup-only option to set the startup version and skip the reset.
- Activating a fabric interconnect resets the fabric interconnect and all I/O modules connected to it.

Outage Impacts of Direct Firmware Updates

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

Outage Impact of a Fabric Interconnect Firmware Update

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

- The fabric interconnect restarts.
- The corresponding I/O modules restart.

Outage Impact of a Cisco UCS Manager Firmware Update

A firmware update to Cisco UCS Manager disrupts Cisco UCS Manager GUI, but not Cisco UCS Manager CLI. The following disruptions occur in Cisco UCS Manager GUI during a firmware update:

- All users logged into Cisco UCS Manager GUI are logged out and their sessions ended.
- Any unsaved work in progress is lost.

Outage Impact of an I/O Module Firmware Update

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

- I/O modules restart when the corresponding fabric interconnect is updated.
- An I/O module can take a few minutes to become available after a firmware update.

Outage Impact of a BMC Firmware Update

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

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

Outage Impact of an Adapter Firmware Update

When you activate the firmware for an adapter, you cause the following outage impacts and disruptions:

- The server resets.
- Server traffic is disrupted.

Firmware Updates through Service Profiles

You can use service profiles to update the server and adapter firmware, including the BIOS on the server, by defining the following policies and including them in the service profile associated with a server:

- Host Firmware Package policy
- Management Firmware Package policy

Note You cannot update the firmware on an I/O module, fabric interconnect, or Cisco UCS Manager through service profiles. You must update the firmware on those components directly.

Host Firmware Pack

This policy enables you to specify a common set of firmware versions that make up the host firmware pack. The host firmware includes the following server and adapter components:

- BIOS
- SAS controller
- Emulex Option ROM (applicable only to Emulex-based Converged Network Adapters [CNAs])
- Emulex firmware (applicable only to Emulex-based CNAs)
- QLogic option ROM (applicable only to QLogic-based CNAs)
- Adapter firmware

The firmware pack is pushed to all servers associated with service profiles that include this policy.

This policy ensures that the host firmware is identical on all servers associated with service profiles which use the same policy. Therefore, if you move the service profile from one server to another, the firmware versions are maintained. Also, if you change the firmware version of the component in the firmware pack, new versions are applied to all the affected service profiles immediately, which could cause server reboots.

You must include this policy in a service profile, and that service profile must be associated with a server for it to take effect.

Prerequisites

This policy is not dependent upon any other policies. However, you must 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 server with a service profile, Cisco UCS Manager ignores the firmware update and completes the association.

Management Firmware Pack

This policy enables you to specify a common set of firmware versions that make up the management firmware pack. The management firmware includes the server controller (BMC) on the server.

The firmware pack is pushed to all servers associated with service profiles that include this policy.

This policy ensures that the BMC firmware is identical on all servers associated with service profiles which use the same policy. Therefore, if you move the service profile from one server to another, the firmware versions are maintained.

You must include this policy in a service profile, and that service profile must be associated with a server for it to take effect.

Prerequisites

This policy is not dependent upon any other policies. However, you must ensure that the appropriate firmware has been downloaded to the fabric interconnect.

Stages of a Firmware Update through Service Profiles

If you use policies in service profiles to update server and adapter firmware, you must complete the following stages:

Firmware Package Policy Creation

During this stage, you create the host and/or management firmware packages and include them in the appropriate firmware policies.

Associate

During this stage, you include a firmware policy in a service profile, and then associate the service profile with a server. The system pushes the selected firmware versions to the endpoints and reboots to ensure that the endpoints are running the versions specified in the firmware pack.

When the firmware versions in the policies change, the system performs firmware updates (wherever necessary), activates, and reboots the endpoints.

Caution As this type of update requires a reboot of the endpoints, it can be disruptive.

Firmware Downgrades

You downgrade firmware in a Cisco UCS instance in the same way that you upgrade firmware. The package or version that you select when you update the firmware determines whether you are performing an upgrade or a downgrade.

Downloading and Managing Images

Obtaining Images from Cisco

Procedure

Step 1 In a web browser, navigate to the web link provided by Cisco to obtain firmware images for Cisco UCS.

Step 2 Choose one or more firmware images and copy them to a network server.

Step 3 Read the release notes provided with the image or images.

What to Do Next

Download the firmware image to the fabric interconnect.

Checking the Available Space on a Fabric Interconnect

You cannot download new firmware images if the bootflash on the fabric interconnect or fabric interconnects in the Cisco UCS does not have sufficient available space. In a cluster system, the available space is the same on both fabric interconnects because Cisco UCS mirrors the configuration on both fabric interconnects.

Procedure

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

Step 2 On the **Equipment** tab, expand **Equipment ➤ Fabric Interconnects**.

Step 3 In the **Work** pane, click the **General** tab.

Step 4 Expand the **Local Storage Information** area.
If the bootflash area does not have sufficient available space, you can delete obsolete images through the **Firmware Management** tab on the **Equipment** node.

Downloading Images to the Fabric Interconnect

Note In a cluster setup, the firmware image is automatically downloaded to both fabric interconnects, regardless of which fabric interconnect is used to initiate the download. Cisco UCS Manager always keeps the images in both fabric interconnects in sync. If one fabric interconnect is down while dowloading, the download still finishes successfully. The images are synced to the other fabric interconnect when it comes back online.

Before You Begin

Obtain the firmware images from Cisco.

Procedure

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

Step 2 Click the **Equipment** node.

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

Step 4 Click the **Installed Firmware** tab.

Step 5 Click **Download Firmware**.

Step 6 In the **Download Firmware** dialog box, complete the following fields:

Name	Description
Protocol field	The protocol to use when communicating with the remote server. This can be: • **FTP** • **SCP** • **SFTP** • **TFTP**
Server field	The IP address or hostname of the remote server on which the files resides.
Filename field	The name of the firmware executable you want to download.
Remote Path field	The absolute path to the file on the remote server, if required. If you use SCP, the absolute path is always required. If you use any other protocol, you may not need to specify a remote path if the file resides in the default download folder. For details about how your file server is configured, contact your system administrator.
User field	The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP.
Password field	The password for the remote server username. This field does not apply if the protocol is TFTP.

Cisco UCS Manager GUI begins downloading the firmware bundle to the fabric interconnect.

Step 7 Click **OK**.

Step 8 (Optional) Monitor the status of the image download on the **Download Tasks** tab.

Note If Cisco UCS Manager reports that the bootflash is out of space, delete obsolete images to free up space. To view the available space in bootflash, navigate to the fabric interconnect on the **Equipment** tab and expand the **Local Storage Information** area on the **General** tab.

What to Do Next

Update the firmware on the components.

Canceling an Image Download

You can cancel an image download only while it is in progress. After the image has downloaded, deleting the download task does not delete the image that was downloaded.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.
Step 2 Expand the **Equipment** node.
Step 3 In the **Work** pane, select the **Firmware Management** tab.
Step 4 On the **Download Tasks** tab, right-click the task you want to cancel and select **Delete**.

Directly Updating Firmware at Endpoints

Updating the Firmware on Multiple Components

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.
Step 2 In the **Equipment** tab, select the **Equipment Node**.
Step 3 In the **Work** pane, select the **Firmware Management** tab.
Step 4 In the **Installed Firmware** tab, select **Update Firmware**.
Step 5 In the **Update Firmware** dialog box:
a) For each component whose firmware you want to update, select the appropriate version from the drop-down list in the **Backup Version** column.
b) Click **OK**.

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

What to Do Next

Activate the firmware.

Activating the Firmware on Multiple Components

After you activate the firmware, you may need to reboot the server.

Procedure

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

Step 2 In the **Equipment** tab, select the **Equipment Node**.

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

Step 4 In the **Installed Firmware** tab, select **Activate Firmware**.

Step 5 In the **Activate Firmware** dialog box:

a) For each component whose firmware you want to update, select the appropriate version from the drop-down list in the **Startup Version** column.

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

c) If you only want to set the start up version and not change the version running on the component, check the **Set Startup Version Only** check box.

d) Click **OK**.

Updating the Firmware on an Adapter

Procedure

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

Step 2 On the **Equipment** tab, expand **Equipment ➤ Chassis ➤** ***Chassis Number*** **➤ Servers**.

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

Step 4 Expand **Interface Cards** and select the interface card for the adapter you want to upgrade.

Step 5 In the **General** tab, click **Update Firmware**.

Step 6 In the **Update Firmware** dialog box:

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

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 firmware package to the backup memory slot, where it remains until you explicitly activate it.

Step 7 (Optional) Monitor the status of the update in the **Update Status** area.
The update process can take several minutes. Do not activate the firmware until the selected firmware package displays in the **Backup Version** field in the **Firmware** area of the **General** tab.

What to Do Next

Activate the firmware.

Activating the Firmware on an Adapter

Procedure

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

Step 2 On the **Equipment** tab, expand **Equipment ➤ Chassis ➤** ***Chassis Number*** **➤ Servers**.

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

Step 4 Expand **Interface Cards** and select the interface card for the adapter.

Step 5 In the **General** tab, click **Activate Firmware**.

Step 6 In the **Activate Firmware** dialog box:

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

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

c) If you only want to set the start up version and not change the version running on the component, check the **Set Startup Version Only** check box.

d) Click **OK**.

Updating the Firmware on a BMC

Procedure

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

Step 2 On the **Equipment** tab, expand **Equipment ➤ Chassis ➤** ***Chassis Number*** **➤ Servers**.

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

Step 4 In the **General** tab, click the **Inventory** tab.

Step 5 Click the **BMC** tab.

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

Step 7 In the **Update Firmware** dialog box:

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

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 firmware package to the backup memory slot, where it remains until you explicitly activate it.

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

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

What to Do Next

Activate the firmware.

Activating the Firmware on a BMC

Procedure

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

Step 2 On the **Equipment** tab, expand **Equipment ➤ Chassis ➤** ***Chassis Number*** **➤ Servers**.

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

Step 4 On the **General** tab, click the **Inventory** tab.

Step 5 Click the **BMC** tab.

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

Step 7 In the **Activate Firmware** dialog box:

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

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

c) If you only want to set the start up version and not change the version running on the component, check the **Set Startup Version Only** check box.

d) Click **OK**.

Updating the Firmware on an IOM

Procedure

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

Step 2 On the **Equipment** tab, expand **Equipment ➤ Chassis ➤** ***Chassis Number*** **➤ IO Modules**.

Step 3 Click the I/O module that you want to update.

Step 4 In the **General** tab, click **Update Firmware**.

Step 5 In the **Update Firmware** dialog box:

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

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 firmware package to the backup memory slot, where it remains until you explicitly activate it.

Step 6 (Optional) Monitor the status of the update in the **Update Status** area.
The update process can take several minutes. Do not activate the firmware until the selected firmware package displays in the **Backup Version** field in the **Firmware** area of the **General** tab.

What to Do Next

Activate the firmware.

Activating the Firmware on an IOM

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.
Step 2 On the **Equipment** tab, expand **Equipment ➤ Chassis ➤ *Chassis Number* ➤ IO Modules**.
Step 3 Select the **IO Module** node that includes the I/O module for which you want to activate the updated firmware.
Step 4 In the **General** tab, click **Activate Firmware**.
Step 5 In the **Activate Firmware** dialog box:
a) Select the appropriate version from the **Version To Be Activated** drop-down list.
b) (Optional) If you want to activate the firmware regardless of any possible incompatibilities or currently executing tasks, check the **Ignore Compatibility Check** check box.
c) If you only want to set the start up version and not change the version running on the component, check the **Set Startup Version Only** check box.
d) Click **OK**.

Updating and Activating the Firmware on a Fabric Interconnect

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.
Step 2 In the **Equipment** tab, expand the **Equipment** node.
Step 3 Expand the **Fabric Interconnects** node and click the fabric interconnect for which you want to update and activate the firmware.
Step 4 On the **General** tab, click **Activate Firmware**.
Step 5 In the **Activate Firmware** dialog box, complete the following fields:

Name	Description
Kernel Version drop-down list	Choose the version that you want to use for the kernel.

Name	Description
System Version drop-down list	Choose the version you want to use for the system.
Ignore Compatibility Check check box	By default, Cisco UCS makes sure that the firmware version is compatible with everything running on the server before it activates that version. Check this check box if you want Cisco UCS to activate the firmware without making sure that it is compatible first. **Note** We recommend that you use this option only when explicitly directed to do so by a technical support representative.

Step 6 Click **OK**.
Cisco UCS Manager updates and activates the firmware, and then reboots the fabric interconnect.

Updating and Activating the Cisco UCS Manager Software

You can also update Cisco UCS Manager when you update and activate the fabric interconnect firmware.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.
Step 2 Click the **Equipment** tab, expand the **Equipment** node.
Step 3 Select the **Fabric Interconnects** node.
Step 4 In the **Work** pane, click the **Installed Firmware** tab.
Step 5 Click **Activate Firmware**.
Step 6 On the **UCS Manager** row of the **Activate Firmware** dialog box:
a) From the drop-down list in the **Startup Version** column, select the version to which you want to update the software.
b) (Optional) If you want to activate the firmware regardless of any possible incompatibilities or currently executing tasks, check the **Ignore Compatibility Check** check box.
c) Click **OK**.
Cisco UCS Manager disconnects, and then updates and activates the software.

Updating Firmware through Service Profiles

Creating a Host Firmware Package

Before You Begin

Ensure that the appropriate firmware has been downloaded to the fabric interconnect.

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ 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 **Host Firmware Packages** and select **Create Package**.

Step 5 In the **Create Host 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, and you cannot change this name after the object has been saved.

Step 6 Click the down arrows to expand one or more of the following sections on the left of the dialog box:

- **Adapter Firmware Packages**
- **Storage Controller Firmware Packages**
- **Fibre Channel Adapters Firmware Packages**
- **BIOS Firmware Packages**
- **HBA Option ROM Packages**

Step 7 In each section for the component to which you want to include firmware in the pack:

a) Select the line in the table which lists the firmware version that you want to add to the pack.
b) Drag the line to the table on the right.
c) Click **Yes** to confirm that you selected the correct version.

Step 8 When you have added all the desired firmware to the pack, click **OK**.

What to Do Next

Include the policy in a service profile and/or template.

Updating a Host Firmware Pack

If the policy is associated with a service profile, Cisco UCS Manager updates and activates the firmware in the server and adapter with the new versions and reboots the server.

Before You Begin

Ensure that the appropriate firmware has been downloaded to the fabric interconnect.

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ 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 **Host Firmware Packages** and select the policy you want to update.

Step 5 In the table on the right, delete the existing entries for the firmware you want to update:

a) Select the line in the table for the firmware version that you want to change.
b) Right-click and select **Delete**.
c) Click **Yes** to confirm that you want to delete that entry.

Step 6 On the **General** tab, click the down arrows to expand one or more of the following sections on the left:

- **Adapter Firmware Packages**
- **Storage Controller Firmware Packages**
- **Fibre Channel Adapters Firmware Packages**
- **BIOS Firmware Packages**
- **HBA Option ROM Packages**

Step 7 In each section for the component to which you want to include firmware in the pack:

a) Select the line in the table for the firmware version that you want to add to the pack.
b) Drag the line to the table on the right.
c) Click **Yes** to confirm that you selected the correct version.

Step 8 Click **Save Changes**.

Creating a Management Firmware Package

Before You Begin

Ensure that the appropriate firmware has been downloaded to the fabric interconnect.

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ 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 **Management Firmware Packages** and select **Create Package**.

Step 5 In the **Create Management 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, and you cannot change this name after the object has been saved.

Step 6 In the **BMC Firmware Packages** section on the left of the dialog box:

a) Click the down arrows to expand the section.
b) Select the line in the table which lists the firmware version that you want to add to the package.
c) Drag the line to the table on the right.
d) Click **Yes** to confirm that you selected the correct version.

Step 7 When you have added the desired firmware to the package, click **OK**.

What to Do Next

Include the policy in a service profile and/or template.

Updating a Management Firmware Pack

If the policy is associated with a service profile, Cisco UCS Manager updates and activates the firmware in the server and adapter with the new versions and reboots the server.

Before You Begin

Ensure that the appropriate firmware has been downloaded to the fabric interconnect.

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ 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 **Management Firmware Packages** and select the policy you want to update.

Step 5 In the table on the right, delete the existing entry for the firmware you want to update:

a) Select the line in the table for the firmware version that you want to change.
b) Right-click and select **Delete**.
c) Click **Yes** to confirm that you want to delete that entry.

Step 6 In the **BMC Firmware Packages** section on the left:

a) Click the down arrows to expand the section.
b) Select the line in the table which lists the firmware version that you want to add to the pack.
c) Drag the line to the table on the right.
d) Click **Yes** to confirm that you selected the correct version.

Step 7 Click **Save Changes**.

Verifying Firmware Versions on Components

Procedure

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

Step 2 On the **Equipment** tab, select the **Equipment Node**.

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

Step 4 On the **Installed Firmware** tab, review the firmware versions listed for each component.