Cisco UCS M-Series GUI Firmware Management Guide, Release 2.5

First Published: April 07, 2015

Last Modified: August 21, 2015

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

Preface

This preface includes the following sections:

Audience

This guide is intended primarily for data center administrators with responsibilities and expertise in one or more of the following:

- Server administration
- Storage administration
- Network administration
- Network security

Conventions

Text Type	Indication
GUI elements	GUI elements such as tab titles, area names, and field labels appear in **this font**. Main titles such as window, dialog box, and wizard titles appear in **this font**.
Document titles	Document titles appear in *this font*.
TUI elements	In a Text-based User Interface, text the system displays appears in `this font`.
System output	Terminal sessions and information that the system displays appear in `this font`.

Text Type	Indication
CLI commands	CLI command keywords appear in **this font**. Variables in a CLI command appear in *this font*.
[ ]	Elements in square brackets are optional.
{x | y | z}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the document.

Tip Means *the following information will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

Caution Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Warning IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Related Cisco UCS Documentation

Documentation Roadmaps

For a complete list of all B-Series documentation, see the *Cisco UCS B-Series Servers Documentation Roadmap* available at the following URL: http://www.cisco.com/go/unifiedcomputing/b-series-doc.

For a complete list of all C-Series documentation, see the *Cisco UCS C-Series Servers Documentation Roadmap* available at the following URL: http://www.cisco.com/go/unifiedcomputing/c-series-doc.

For a complete list of all M-Series documentation, see the *Cisco UCS M-Series Servers Documentation Roadmap* available at the following URL: https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/overview/guide/UCS_M_Series_Servers_Documentation_Roadmap.html

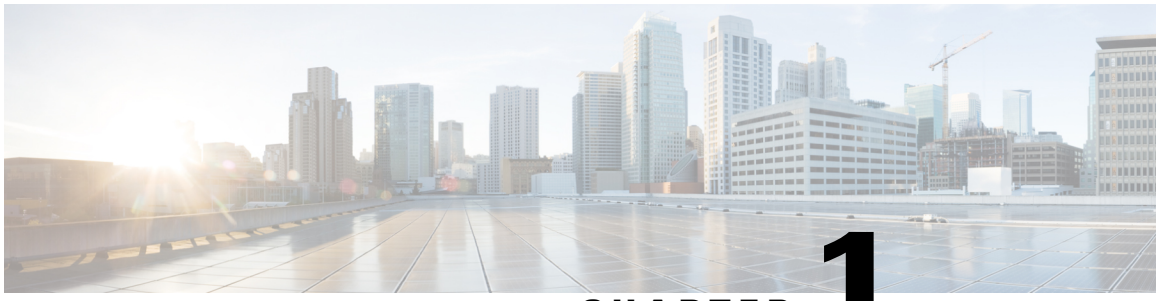
For information on supported firmware versions and supported UCS Manager versions for the rack servers that are integrated with the UCS Manager for management, refer to Release Bundle Contents for Cisco UCS Software.

Other Documentation Resources

Follow Cisco UCS Docs on Twitter to receive document update notifications.

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to ucs-docfeedback@cisco.com. We appreciate your feedback.



CHAPTER 1

Overview

This chapter includes the following sections:

Overview of Firmware

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.

This document uses the following definitions for managing firmware:

Upgrade

Changes the firmware running on an endpoint to another image, such as a release or patch. Upgrade includes both update and activation.

Update

Copies the firmware image to the backup partition on an endpoint.

Activate

Sets the firmware in the backup partition as the active firmware version on the endpoint. Activation can require or cause the reboot of an endpoint.

For Management Extensions and Capability Catalog upgrades, update and activate occur simultaneously. You only need to update or activate those upgrades. You do not need to perform both steps.

Important Cisco UCS Manager Release 2.5 supports only Cisco UCS M-Series Servers. It does not support Cisco UCS B-Series Servers and Cisco C-Series Servers.

Components That Support Firmware Upgrade

The following components support firmware upgrade:

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

Firmware Versions

The firmware version terminology used depends upon the type of endpoint, as follows:

Firmware Versions in CIMC, BIOS, CMC and Shared Adapters

Each CIMC, BIOS, Shared Adapter, and CMC has two flashes for firmware. 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 Cisco UCS Manager:

Running Version

The running version is the firmware that is active and in use by the endpoint.

Startup Version

The startup version is the firmware that will be used when the endpoint next boots up. Cisco UCS Manager uses the activate operation to change the startup version.

Backup Version

The backup version is the firmware in the other slot and is not in use by the endpoint. This version can be firmware that you have updated to the endpoint but have not yet activated, or it can be an older firmware version that was replaced by a recently activated version. Cisco UCS Manager uses the update operation to replace the image in the backup slot.

If the endpoint cannot boot from the startup version, it boots from the backup version.

The board controller and the storage controller do not have backup versions. Therefore, you can only activate them.

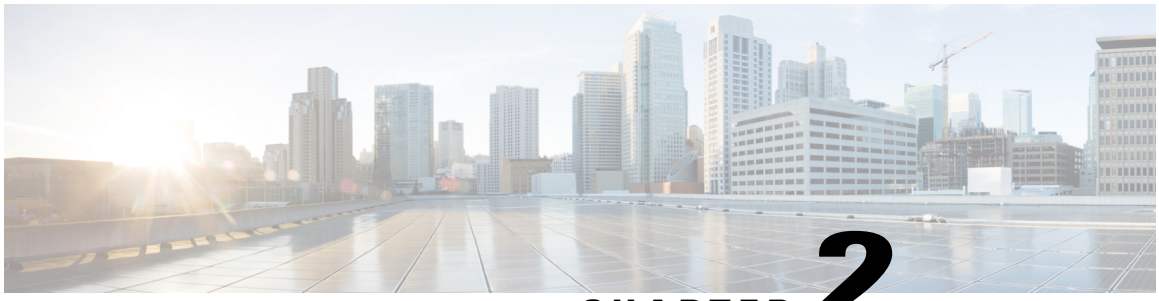
Firmware Versions in the Fabric Interconnect and Cisco UCS Manager

You can only activate 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 CIMC and adapters. Instead, the number of bootable fabric interconnect images is limited by the available space in the memory of the fabric interconnect and the number of images stored there.

The fabric interconnect and Cisco UCS Manager firmware have running and startup versions of the kernel and system firmware. The kernel and system firmware must run the same versions of firmware.

PART I

Managing Firmware through Cisco UCS Manager



CHAPTER 2

Downloading and Managing Firmware in Cisco UCS Manager

This chapter includes the following sections:

Firmware Image Management

Cisco delivers all firmware updates to Cisco UCS components in bundles of images. Cisco UCS firmware updates are available to be downloaded to fabric interconnects in a Cisco UCS domain in the following bundles:

Cisco UCS Infrastructure Software Bundle

This bundle includes the following firmware images that are required to update the following components:

- Cisco UCS Manager software
- Kernel and system firmware for the fabric interconnects

Cisco UCS M-Series Modular Server Software Bundle

This bundle includes the following firmware images that are required to update the firmware for the modular servers in a Cisco UCS domain.

- Chassis:
  - CMC firmware
  - Shared Adapter firmware
  - Board controller firmware
  - Storage controller firmware
- Server:
  - CIMC firmware
  - BIOS firmware
  - Board controller firmware

Cisco also provides release notes, which you can obtain on the same website from which you obtained the bundles.

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

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

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

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

Firmware Image Headers

Every firmware 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

Firmware 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 firmware bundles 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 in each downloaded firmware bundle.

Images

The images view lists the component images available on the system. You cannot use this view to see complete firmware bundles or to group the images by bundle. 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.

Obtaining M-Series Software Bundles from Cisco

The Cisco UCS M-Series Modular Server Software Bundle contains firmware for M-Series chassis and cartridge components.

Procedure

Step 1 In a web browser, navigate to Cisco.com.

Step 2 Under **Support**, click **All Downloads**.

Step 3 In the center pane, click **Servers - Unified Computing**.

Step 4 If prompted, enter your Cisco.com username and password to log in.

Step 5 In the right pane, click the link for the software bundles you require, as follows:

Bundle	Navigation Path
Cisco UCS M-Series Modular Server Software Bundle	Click **Cisco UCS M-Series Modular Server Software** > **Unified Computing System (UCS) Server Software Bundle**.

Tip The Unified Computing System (UCS) Documentation Roadmap Bundle, which is accessible through these paths, is a downloadable ISO image of all Cisco UCS documentation.

Step 6 On the first page from which you download a software bundle, click the **Release Notes** link to download the latest version of the Release Notes.

Step 7 For each software bundle that you want to download, do the following:

a) Click the link for the software release bundle.
The release number is followed by a number and a letter in parentheses. The number identifies the maintenance release level, and the letter differentiates between patches of that maintenance release. For more information about what is in each maintenance release and patch, see the latest version of the Release Notes.

b) Click one of the following buttons and follow the instructions provided:

- **Download Now—**Allows you to download the software bundle immediately.
- **Add to Cart—**Adds the software bundle to your cart to be downloaded at a later time.

c) Follow the prompts to complete your download of the software bundle(s).

Step 8 Read the Release Notes before upgrading your Cisco UCS domain.

What to Do Next

Download the software bundles to the fabric interconnect.

Downloading Firmware Images to the Fabric Interconnect from a Remote Location

Note In a cluster setup, the image file for the firmware bundle is downloaded to both fabric interconnects, regardless of which fabric interconnect is used to initiate the download. Cisco UCS Manager maintains all firmware packages and images in both fabric interconnects in sync. If one fabric interconnect is down, the download finishes successfully. The images are synced to the other fabric interconnect when it comes back online.

Before You Begin

Obtain the required firmware bundles from Cisco.

Procedure

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

Step 2 On the **Equipment** tab, 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, click the **Remote File System** radio button in the **Location of the Image File** field and fill in the required fields.

Step 7 Click **OK**.
Cisco UCS Manager GUI begins downloading the firmware bundle to the fabric interconnect.

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

Note If Cisco UCS Manager reports that the bootflash is out of space, delete obsolete bundles on the **Packages** tab 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.

Step 9 Repeat this task until all the required firmware bundles have been downloaded to the fabric interconnect.

What to Do Next

After the image file for the firmware bundles downloaded completes, update the firmware on the endpoints.

Downloading Firmware Images to the Fabric Interconnect from the Local File System

Note In a cluster setup, the image file for the firmware bundle is downloaded to both fabric interconnects, regardless of which fabric interconnect is used to initiate the download. Cisco UCS Manager maintains all firmware packages and images in both fabric interconnects in sync. If one fabric interconnect is down, the download finishes successfully. The images are synced to the other fabric interconnect when it comes back online.

Before You Begin

Obtain the required firmware bundles from Cisco.

Procedure

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

Step 2 On the **Equipment** tab, 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, click the **Local File System** radio button in the **Location of the Image File** field.

Step 7 In the **Filename** field, type the full path and and name of the image file.
If you do not know the exact path to the folder where the firmware image file is located, click **Browse** and navigate to the file.

Step 8 Click **OK**.
Cisco UCS Manager GUI begins downloading the firmware bundle to the fabric interconnect.

Step 9 (Optional) Monitor the status of the firmware bundle download on the **Download Tasks** tab.

Note If Cisco UCS Manager reports that the bootflash is out of space, delete obsolete bundles on the **Packages** tab 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.

Step 10 Repeat this task until all the required firmware bundles have been downloaded to the fabric interconnect.

What to Do Next

After the image file for the firmware bundles downloaded completes, update the firmware on the endpoints.

Canceling an Image Download

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

Procedure

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

Step 2 Expand the **Equipment** node.

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

Step 4 On the **Download Tasks** tab, right-click the task you want to cancel and select **Delete**.

Determining the Contents of a Firmware Package

Procedure

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

Step 2 On the **Equipment** tab, click the **Equipment** node.

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

Step 4 On the **Packages** subtab, click the + icon next to a package to view its contents.

Step 5 To take a snapshot of the package contents, do the following:

a) Highlight the rows that include the image name and its contents.

b) Right-click and choose **Copy**.

c) Paste the contents of your clipboard into a text file or other document.

Checking the Available Space on a Fabric Interconnect

If an image download fails, check whether the bootflash on the fabric interconnect or fabric interconnects in the Cisco UCS has sufficient available space.

Procedure

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

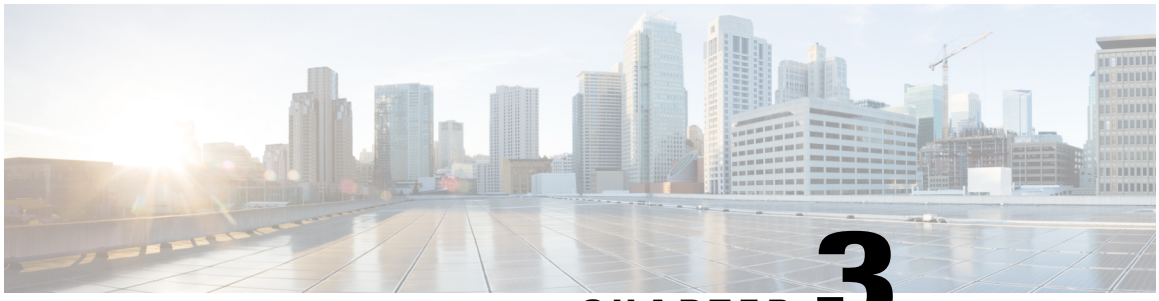
Step 2 On the **Equipment** tab, expand **Equipment** > **Fabric Interconnects**.

Step 3 Click the fabric interconnect on which you want to check the available space.

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

Step 5 Expand the **Local Storage Information** area.

When you download a firmware image bundle, a fabric interconnect needs at least twice as much available space as the size of the firmware image bundle. If the bootflash does not have sufficient space, delete the obsolete firmware, core files, and other unneeded objects from the fabric interconnect.



CHAPTER 3

Upgrading Firmware through Auto Install

This chapter includes the following sections:

Firmware Upgrades through Auto Install

Auto Install enables you to upgrade a Cisco UCS domain to the firmware versions contained in a single package in the following two stages:

- Install Infrastructure Firmware—Uses the Cisco UCS Infrastructure Software Bundle to upgrade the infrastructure components, such as the fabric interconnects, and Cisco UCS Manager.
- Install Server Firmware—Uses the Cisco UCS M-Series Server Software Bundle to upgrade all servers in the Cisco UCS domain.

These two stages are independent and can be run or scheduled to run at different times.

You can use Auto Install to upgrade the infrastructure components to one version of Cisco UCS and server components to a different version.

Install Infrastructure Firmware

Install Infrastructure Firmware upgrades all infrastructure components in a Cisco UCS domain, including Cisco UCS Manager, and all fabric interconnects. All components are upgraded to the firmware version included in the selected Cisco UCS Infrastructure Software Bundle.

Install Infrastructure Firmware does not support a partial upgrade to only some infrastructure components in a Cisco UCS domain domain.

You can schedule an infrastructure upgrade for a specific time to accommodate a maintenance window. However, if an infrastructure upgrade is already in progress, you cannot schedule another infrastructure upgrade. You must wait until the current upgrade is complete before scheduling the next one.

Note You can cancel an infrastructure firmware upgrade if it is scheduled to occur at a future time. However, you cannot cancel an infrastructure firmware upgrade after the upgrade has begun.

Install Server Firmware

Install Server Firmware uses host firmware packages to upgrade all servers and their components in a Cisco UCS domain. All servers whose service profiles include the selected host firmware packages are upgraded to the firmware versions in the selected software bundles, as follows:

- Cisco UCS M-Series Server Software Bundle for all servers.

Note You cannot cancel a server firmware upgrade process after you complete the configuration in the **Install Server Firmware** wizard. Cisco UCS Manager applies the changes immediately. However, when the actual reboot of servers occurs depends upon the maintenance policy in the service profile associated with the server.

Required Order of Steps for Auto Install

If you want to upgrade all components in a Cisco UCS domain to the same package version, you must run the stages of Auto Install in the following order:

1. Install Infrastructure Firmware
2. Install Server Firmware

This order enables you to schedule the server firmware upgrades during a different maintenance window than the infrastructure firmware upgrade.

Upgrading the Infrastructure Firmware with Auto Install

The **Firmware Auto Install** tab is not available if the Cisco UCS Manager GUI is at a release lower than 2.1(1).

Before You Begin

If your Cisco UCS domain does not use an NTP server to set the time, make sure that the clocks on the primary and secondary fabric interconnects are in sync. You can do this by configuring an NTP server in Cisco UCS Manager or by syncing the time manually.

Procedure

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

Step 2 On the **Equipment** tab, 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 Infrastructure Firmware**.

Step 6 In the **Prerequisites** page of the **Install Infrastructure Firmware** dialog box, ensure that you address the warnings before proceeding.
Warnings are given in the following categories:

- Whether there are any current critical or major faults.
- Whether a configuration backup has been taken recently.
- Whether the management interface monitoring policy is enabled.
- Whether there is pending fabric interconnect reboot activity.
- Whether NTP is configured.

You can click the hyperlinks for each warning to address them directly. Check the checkbox for each warning that you have addressed, or check the **Ignore All** checkbox to continue without addressing the warnings.

Step 7 In the **Properties** area of the **Install Infrastructure Firmware** dialog box, complete the following fields:

Name	Description
Name field	The name of the infrastructure pack created and maintained by Cisco UCS. You cannot change the default name in this field or create a custom infrastructure pack.
Description field	A user-defined description of the infrastructure pack. This field is completed by default. However, you can enter your own description if you prefer. Enter up to 256 characters. You can use any characters or spaces except ` (accent mark), \ (backslash), ^ (carat), " (double quote), = (equal sign), > (greater than), < (less than), or ' (single quote).
Version drop-down list	A list of the software bundles from that are available for you to upgrade the firmware on the infrastructure components.
Force check box	If checked, Cisco UCS attempts the installation even if a previous attempt to install the selected version failed or was interrupted.

Step 8 In the **Infrastructure Schedule** area of the **Install Infrastructure Firmware** dialog box, do one of the following:

Option	Description
Start Time field	The date and time that the occurrence will run. Click the down arrow at the end of the field to select the date from a calendar.
Upgrade Now check box	If checked, Cisco UCS Manager ignores the **Start Time** field and upgrades the infrastructure firmware as soon as you click **OK**.

Step 9 Click **OK**.
The **Firmware Installer** field on the **Firmware Auto Install** tab displays the status of the infrastructure firmware upgrade.

Note If there is not enough space under bootflash, a warning will display and the upgrade process will stop.

What to Do Next

Acknowledge the reboot of the primary fabric interconnect. If you do not acknowledge that reboot, Cisco UCS Manager cannot complete the infrastructure upgrade and the upgrade remains pending indefinitely.

Acknowledging the Reboot of the Primary Fabric Interconnect

Before You Begin

Caution To upgrade with minimal disruption, you must confirm the following:

- Ensure that all the IOMs that are attached to the Fabric Interconnect are up before you acknowledge the reboot of the Fabric Interconnect. If all IOMs are not up, all the servers connected to the Fabric Interconnect will immediately be re-discovered and cause a major disruption.
- Ensure that both of the Fabric Interconnects and the service profiles are configured for failover.
- Verify that the data path has been successfully restored from the secondary Fabric Interconnect before you acknowledge the reboot of the primary Fabric Interconnect. For more information, see Verifying that the Data Path is Ready, on page 57.

After you upgrade the infrastructure firmware, Install Infrastructure Firmware automatically reboots the secondary fabric interconnect in a cluster configuration. However, you must acknowledge the reboot of the primary fabric interconnect. If you do not acknowledge the reboot, Install Infrastructure Firmware waits indefinitely for that acknowledgment rather than completing the upgrade.

Procedure

Step 1 On the toolbar, click **Pending Activities**.

Step 2 In the **Pending Activities** dialog box, click the **User Acknowledged Activities** tab.

Step 3 In the table, locate the row for the pending reboot of the primary fabric interconnect.

Step 4 In the **Reboot Now** column for that row, check the **Acknowledge All** check box.

Step 5 Click **OK**.
Cisco UCS Manager immediately reboots the primary fabric interconnect. You cannot stop this reboot after you click **OK**.

Canceling an Infrastructure Firmware Upgrade

Note You can cancel an infrastructure firmware upgrade if it is scheduled to occur at a future time. However, you cannot cancel an infrastructure firmware upgrade after the upgrade has begun.

Procedure

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

Step 2 On the **Equipment** tab, 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 Infrastructure Firmware**.

Step 6 In the **Actions** area of the **Install Infrastructure Firmware** dialog box, click **Cancel Infrastructure Upgrade**.

Step 7 If the Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Step 8 Click **OK**.

Upgrading the Server Firmware with Auto Install

The **Firmware Auto Install** tab is not available if the Cisco UCS Manager GUI is at a release lower than 2.1(1).

Note You cannot cancel a server firmware upgrade process after you complete the configuration in the **Install Server Firmware** wizard. Cisco UCS Manager applies the changes immediately. However, when the actual reboot of servers occurs depends upon the maintenance policy in the service profile associated with the server.

Procedure

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

Step 2 On the **Equipment** tab, 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 Server Firmware**.

Step 6 On the **Prerequisites** page of the **Install Server 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 server firmware.

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

a) If the Cisco UCS domain contains blade servers, choose the software bundle to which you want to upgrade these servers from the **New Version** drop-down list in the **B-Series Blade Server Software** area.

b) If the Cisco UCS domain contains rack-mount servers, choose the software bundle to which you want to upgrade these servers from the **New Version** drop-down list in the **C-Series Rack-Mount Server Software** area.
If the Cisco UCS domain includes both blade servers and rack servers, we recommend that you choose a new firmware version for the B-Series blade servers and C-Series rack-mount servers in the **Select Package Versions** page and upgrade all servers in the domain.

Note If you update the default host firmware package, you might cause the upgrade of firmware on unassociated servers and on servers with associated service profiles that do not include a host firmware package. This firmware upgrade may cause the reboot of those servers according to the maintenance policy defined in the service profile.

c) If the Cisco UCS domain contains M-Series servers, choose the software bundle to which you want to upgrade these servers from the **New Version** drop-down list in the **M-Series Server Software** area

d) Click **Next**.

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

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

b) Check the check box next to the name of each host firmware package that you want to update.
This step updates the selected host firmware package with the new version of firmware. You must choose the host firmware packages included in the service profiles associated with all servers in the Cisco UCS domain to update all servers.

c) Click **Next**.

Step 9 On the **Host Firmware Package Dependencies** page of the **install Server Firmware** wizard, do the following:

a) Expand the node for each host firmware package listed in the table.

b) Review the list of service profiles that include the host firmware package.

c) If desired, click a link in one of the following columns:

- **Host Pack DN** column—Opens the navigator for the host firmware package.

- **Service Profile DN** column—Opens the navigator for the service profile.

d) Do one of the following:

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

Step 10 On the **Impacted Endpoints Summary** page of the **install Server 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.

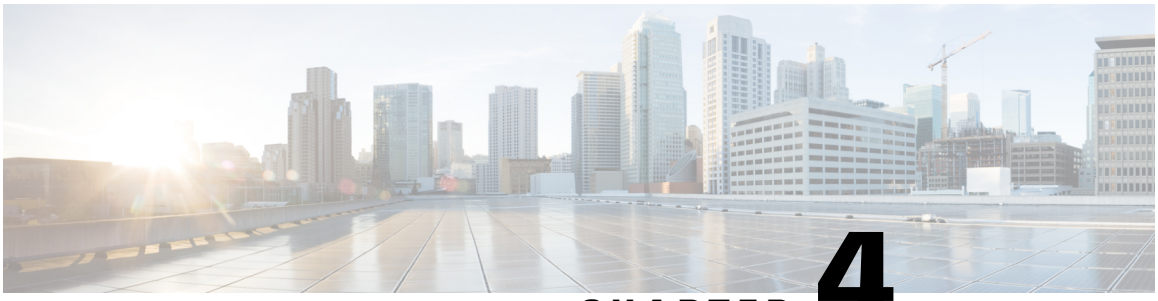
b) Review the list of impacted endpoints.

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 host firmware packages, click **Prev**.
- If you are satisfied that you have selected the appropriate host firmware packages and want to start the server upgrade, click **Install**.

Step 11 (Optional) To check on the progress of the server firmware upgrade, check the **FSM** tab for each server that you are upgrading.
The **Firmware Installer** field on the **Firmware Auto Install** tab shows only the status of an infrastructure firmware upgrade.



CHAPTER 4

Using Firmware Automatic Synchronization Server Policy

This chapter includes the following sections:

Firmware Automatic Synchronization

You can use the **Firmware Auto Sync Server** policy in Cisco UCS Manager to determine when and how firmware versions on recently discovered servers must be upgraded. With this policy, you can upgrade the firmware versions of recently discovered unassociated servers to match the firmware version defined in the default host firmware pack. In addition, you can determine if the firmware upgrade process should run immediately after the server is discovered or run at a later time.

Important The firmware automatic synchronization is dependent on the default host firmware pack. If you delete the default host firmware pack, a major fault is raised in Cisco UCS Manager. If you have configured a default host firmware pack, but not specified or configured a server firmware in it, then a minor fault is raised. Irrespective of the severity of the fault raised, you must resolve these faults prior to setting the **Firmware Auto Sync Server** policy.

Following are the values for the **Firmware Auto Sync Server** policy:

- **Auto Acknowledge—**Firmware on the server is automatically synchronized after it is discovered by Cisco UCS Manager. This option is selected by default.
- **User Acknowledge—**Firmware on the server is not synchronized until the administrator acknowledges the upgrade in the **Pending Activities** dialog box.
- **No Action—**no firmware upgrade is initiated on the server.

You can set this policy either from the Cisco UCS Manager GUI or Cisco UCS Manager CLI. The firmware for a server is automatically triggered when the following conditions occur:

- The firmware version on a server or the endpoint on a server differs from the firmware version configured in the default host firmware pack.
- The value for the **Firmware Auto Sync Server** policy has been modified. For example, if you had initially set it as **Auto Acknowledge** and you change it to **User Acknowledge**.

Important If Cisco UCS Manager is registered as a Cisco UCS domain with Cisco UCS Central, then this policy runs as a local policy. If the default host firmware pack is not defined in or is deleted from Cisco UCS Manager, then this policy will not run.

Setting the Firmware Auto-Sync Server Policy

Use this policy to determine when and how the firmware version of a recently discovered unassociated server must be updated.

If the firmware version of a specific endpoint of a server differs from the version in the default host firmware pack, the FSM state in Cisco UCS Manager displays the update status for that specific endpoint only. The firmware version of the server is not updated.

Before You Begin

- You should have created a default host firmware pack prior to setting this policy.
- You should have logged in as an administrator to complete this task.

Procedure

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

Step 2 On the **Equipment** tab, click the **Equipment** node.

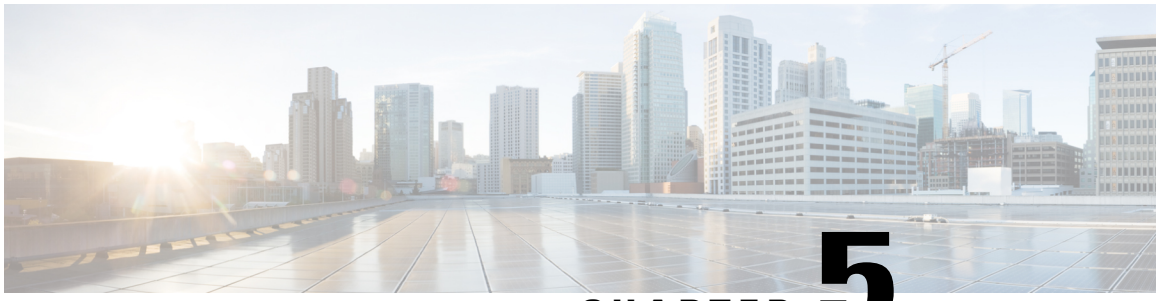
Step 3 In the Work pane, click the **Policies** tab.

Step 4 Click the **Global Policies** subtab.

Step 5 In the **Firmware Auto Sync Server Policy** area, select one of the following values as the **Sync State**:

- **Auto Acknowledge—**Firmware on the server is automatically synchronized after it is discovered by Cisco UCS Manager. This option is selected by default.
- **User Acknowledge—**Firmware on the server is not synchronized until the administrator acknowledges the upgrade in the **Pending Activities** dialog box.
- **No Action—**no firmware upgrade is initiated on the server.

Step 6 Click **Save Changes**.



CHAPTER 5

Directly Upgrading Firmware at Endpoints

This chapter includes the following sections:

Direct Firmware Upgrade at Endpoints

If you follow the correct procedure and apply the upgrades in the correct order, a direct firmware upgrade and the activation of the new firmware version on the endpoints is minimally disruptive to traffic in a Cisco UCS domain.

You can directly upgrade the firmware on the following endpoints:

- Chassis:
  - CMC
  - Shared Adapter
  - Storage Controller
  - Board controller
- Server:
  - CIMC
  - BIOS
  - Board Controller
- Infrastructure:
  - Fabric interconnects
  - Cisco UCS Manager

The CIMC and BIOS firmware can also be upgraded through the host firmware package in the service profile. If you use a host firmware package to upgrade this firmware, you can reduce the number of times a server needs to be rebooted during the firmware upgrade process.

Note You cannot directly upgrade an endpoint if the service profile associated with the server includes a firmware package. To perform a direct upgrade, you must remove the firmware package from the service profile.

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

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

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

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

Stages of a Direct Firmware Upgrade

Cisco UCS Manager separates the direct upgrade process into two stages to ensure that you can push the firmware to an endpoint while the system is running without affecting uptime on the server or other endpoints.

Update

During this stage, the system copies the selected firmware version from the primary fabric interconnect to the backup partition in the endpoint and verifies that the firmware image is not corrupt. The update process always overwrites the firmware in the backup slot.

The update stage applies only to the following endpoints:

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

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

Activate

During this stage, the system sets the specified image version (normally the backup version) as the startup version and, if you do not specify **Set Startup Version Only**, immediately reboots the endpoint. When the endpoint is rebooted, the backup partition becomes the active partition, and the active partition becomes the backup partition. The firmware in the new active partition becomes the startup version and the running version.

The following endpoints only require activation because the specified firmware image already exists on the endpoint:

- Cisco UCS Manager
- Fabric interconnects
- CMC
- Shared Adapter
- Board controllers for chassis and server
- Storage controller
- CIMC
- BIOS

When the firmware is activated, the endpoint is rebooted and the new firmware becomes the active kernel version and system version. If the endpoint cannot boot from the startup firmware, it defaults to the backup version and raises a fault.

Outage Impacts of Direct Firmware Upgrades

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

Outage Impact of a Fabric Interconnect Firmware Upgrade

When you upgrade the firmware for a fabric interconnect, you cause the fabric interconnect reboot.

Outage Impact of a Cisco UCS Manager Firmware Upgrade

A firmware upgrade to Cisco UCS Manager causes the following disruptions:

- Cisco UCS Manager GUI—All users logged in to Cisco UCS Manager GUI are logged out and their sessions ended.

  Any unsaved work in progress is lost.

- Cisco UCS Manager CLI—All users logged in through telnet are logged out and their sessions ended.

Outage Impact of a CMC Firmware Upgrade

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

Outage Impact of a Shared Adapter Firmware Upgrade

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

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

Outage Impact of a Storage Controller Firmware Upgrade

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

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

Outage Impact of a Board Controller Firmware Upgrade

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

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

- The storage controller reboots.

Outage Impact of a BIOS Firmware Upgrade

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

Outage Impact of a CIMC Firmware Upgrade

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

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

Outage Impact of a Board Controller Firmware Upgrade on a Server

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

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

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

Updating the Firmware on Multiple Endpoints

You can use this procedure to update the firmware on the following endpoints:

- BIOS
- CIMC
- CMC
- Shared Adapter

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

Procedure

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

Step 2 On the **Equipment** tab, click the **Equipment** node.

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

Step 4 On the **Installed Firmware** tab, click **Update Firmware**.
Cisco UCS Manager GUI opens the **Update Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS domain. This step take a few minutes, based on the number of chassis and servers.

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

a) From the **Filter** drop-down list on the menu bar, select **ALL**.
If you want to update all endpoint firmware of a specific type, such as the shared adapter or server BIOS, select that type from the drop-down list.

b) In the **Select** field, do one of the following:

- To activate all endpoints to the same version, click the **Version** radio button and select the appropriate version from the **Set Version** drop-down list.
- To activate all endpoints to the firmware version included in a specific bundle, click the **Bundle** radio button and select the appropriate bundle from the **Set Bundle** drop-down list .

c) 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 image to the backup memory partition and verifies that the image is not corrupt. The image remains as the backup version until you activate it. Cisco UCS Manager begins all updates at the same time. However, some updates might complete at different times.

The update is complete when the **Update Firmware** dialog box displays **ready** in the **Update Status** column for all updated endpoints.

Step 6 (Optional) To monitor the progress of the update to a specific endpoint, right-click the endpoint and choose **Show Navigator**.
Cisco UCS Manager displays the progress in the **Update Status** area on the **General** tab. If the navigator has an **FSM** tab, you can also monitor the progress there. An entry in the **Retry #** field might not indicate that the update failed. The retry count also includes retries that occur when Cisco UCS Manager retrieves the update status.

What to Do Next

Activate the firmware.

Updating 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

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

Step 2 On the **Equipment** tab, expand **Equipment** > **Chassis** > ***Chassis Number***

Step 3 In 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 which you want 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 CMC Firmware on a Chassis

Procedure

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

Step 2 On the **Equipment** tab, 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 desired version as the backup version, Cisco UCS Manager GUI does not display that version in the **Set Version** drop-down list. You must select the version from the **Startup Version** column for each individual endpoint.

b) Click **OK**.

Updating the Shared Adapter 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.

Before You Begin

Gracefully power down the servers.

Procedure

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

Step 2 On the **Equipment** tab, expand **Equipment** > **Chassis** > **Chassis** *Number*

Step 3 In the **Installed Firmware** tab, select **Shared 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 which you want 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 Shared Adapter Firmware on a Chassis

Procedure

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

Step 2 On the **Equipment** tab, expand **Equipment** > **Chassis** > **Chassis** *Number*

Step 3 In the **Installed Firmware** tab, select **Shared 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 desired version as the backup version, Cisco UCS Manager GUI does not display that version 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 Storage Controller Firmware on a Chassis

Procedure

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

Step 2 On the **Equipment** tab, expand **Equipment** > **Chassis** > **Chassis** *Number*

Step 3 In the **Installed Firmware** tab, select the storage controller 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 desired version as the backup version, Cisco UCS Manager GUI does not display that version 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 Board Controller Firmware on a Chassis

Before You Begin

Gracefully power down the servers.

Procedure

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

Step 2 On the **Equipment** tab, 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 desired version as the backup version, Cisco UCS Manager GUI does not display that version in the **Set Version** drop-down list. You must select the version from the **Startup Version** column for each individual endpoint.

b) Click **OK**.

Updating the BIOS Firmware on a 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 the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment** > **Chassis** > **Chassis** *Number* > **Cartridges** > **Cartridge** *Number* > **Servers**

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

Step 4 In the **Installed Firmware** tab, select **BIOS** and click **Update Firmware**.

Step 5 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.

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 **Installed Firmware** tab.

What to Do Next

Activate the firmware.

Activating the BIOS Firmware on a Server

Procedure

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

Step 2 On the **Equipment** tab, expand **Equipment** > **Chassis** > **Chassis** *Number* > **Cartridges** > **Cartridge** *Number* > **Servers**

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

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

Step 5 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 start up 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**.

Updating the CIMC Firmware on a 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 the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment** > **Chassis** > **Chassis** *Number* > **Cartridges** > **Cartridge** *Number* > **Servers**

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

Step 4 In the **Installed Firmware** tab, select CIMC Controller and click **Update Firmware**.

Step 5 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 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 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 **Installed Firmware** tab.

What to Do Next

Activate the firmware.

Activating the CIMC Firmware on a Server

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

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

Procedure

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

Step 2 On the **Equipment** tab, expand **Equipment** > **Chassis** > **Chassis** *Number* > **Cartridges** > **Cartridge** *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 **Installed Firmware** tab, select **CIMC Controller** and 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 desired version as the backup version, Cisco UCS Manager GUI does not display that version 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 Board Controller Firmware on a Server

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

Before You Begin

Gracefully power down the servers.

Procedure

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

Step 2 On the **Equipment** tab, expand **Equipment** > **Chassis** > **Chassis** *Number* > **Cartridges** > **Cartridge** *Number* > **Servers**

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

Step 4 In the **Installed Firmware** tab, select **Board 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 desired version as the backup version, Cisco UCS Manager GUI does not display that version 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 Cisco UCS Manager Software

Procedure

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

Step 2 On the **Equipment** tab, 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 On the **UCS Manager** row of the **Activate Firmware** dialog box, do the following:

a) From the drop-down list in the **Startup Version** column, select the version to which you want to update the software.

b) Click **OK**.

Cisco UCS Manager disconnects all active sessions, logs out all users, and activates the software. When the upgrade is complete, you are prompted to log back in. If you are prompted to re-login immediately after being disconnected, the login will fail. You must wait until the activation of Cisco UCS Manager is completed, which takes a few minutes.

Cisco UCS Manager makes the selected version the startup version and schedules the activation to occur when the fabric interconnects are upgraded.

Activating the Firmware on a Subordinate Fabric Interconnect

Before You Begin

Determine which fabric interconnect in the cluster is the subordinate fabric interconnect.

Procedure

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

Step 2 On the **Equipment** tab, 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, choose **Fabric Interconnects**.

Step 6 On the row of the **Activate Firmware** dialog box for the subordinate fabric interconnect, do the following:

a) In the **Kernel** row, choose the firmware version to which you want to upgrade from the drop-down list in the **Startup Version** column.

b) In the **System** row, choose the firmware version to which you want to upgrade from the drop-down list in the **Startup Version** column.

Step 7 Click **Apply**.
Cisco UCS Manager updates and activates the firmware and reboots the fabric interconnect, disrupting data traffic to and from that fabric interconnect. However, assuming the Cisco UCS domain is configured to permit traffic and port failover, data traffic fails over to the primary fabric interconnect and is not disrupted.

Step 8 Verify the high availability status of the subordinate fabric interconnect.
If the **High Availability Details** area for the fabric interconnect does not show the following values, contact Cisco Technical Support immediately. Do not continue to update the primary fabric interconnect.

Field Name	Required Value
Ready field	**Yes**
State field	**Up**

What to Do Next

If the high availability status of the subordinate fabric interconnect contains the required values, update and activate the primary fabric interconnect.

Activating the Firmware on a Primary Fabric Interconnect

This procedure continues directly from Activating the Firmware on a Subordinate Fabric Interconnect, on page 38 and assumes you are on the **Firmware Management** tab.

Before You Begin

Activate the subordinate fabric interconnect.

Procedure

Step 1 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 2 From the **Filter** drop-down list on the menu bar, choose **Fabric Interconnects**.

Step 3 On the row of the **Activate Firmware** dialog box for the subordinate fabric interconnect, do the following:

a) In the **Kernel** row, choose the firmware version to which you want to upgrade from the drop-down list in the **Startup Version** column.

b) In the **System** row, choose the firmware version to which you want to upgrade from the drop-down list in the **Startup Version** column.

Step 4 Click **Apply**.
Cisco UCS Manager updates and activates the firmware and reboots the fabric interconnect, disrupting data traffic to and from that fabric interconnect. However, assuming the Cisco UCS domain is configured to permit traffic and port failover, data traffic fails over to the other fabric interconnect, which becomes the primary. When it comes back up, this fabric interconnect is the subordinate fabric interconnect.

Step 5 Verify the high availability status of the fabric interconnect.
If the **High Availability Details** area for the fabric interconnect does not show the following values, contact Cisco Technical Support immediately.

Field Name	Required Value
Ready field	**Yes**
State field	**Up**

Activating the Firmware on a Standalone Fabric Interconnect

For a standalone configuration with a single fabric interconnect, you can minimize the disruption to data traffic when you perform a direct firmware upgrade of the endpoints. However, you must reboot the fabric interconnect to complete the upgrade and, therefore, cannot avoid disrupting traffic.

Tip If you ever need to recover the password to the admin account that was created when you configured the fabric interconnects for the Cisco UCS domain, you must know the running kernel version and the running system version. If you do not plan to create additional accounts, Cisco recommends that you save the path to these firmware versions in a text file so that you can access them if required.

Procedure

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

Step 2 On the **Equipment** tab, click the **Equipment** node.

Step 3 Expand the **Fabric Interconnects** node and click the standalone fabric interconnect.

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.
Force check box	If checked, Cisco UCS attempts the installation even if a previous attempt to install the selected version failed or was interrupted.
System Version drop-down list	Choose the version you want to use for the system.
Force check box	If checked, Cisco UCS attempts the installation even if a previous attempt to install the selected version failed or was interrupted.

Step 6 Click **OK**.

Cisco UCS Manager activates the firmware and reboots the fabric interconnect. For a standalone fabric interconnect, this disrupts all data traffic in the Cisco UCS domain.

Verifying Firmware Versions on Components

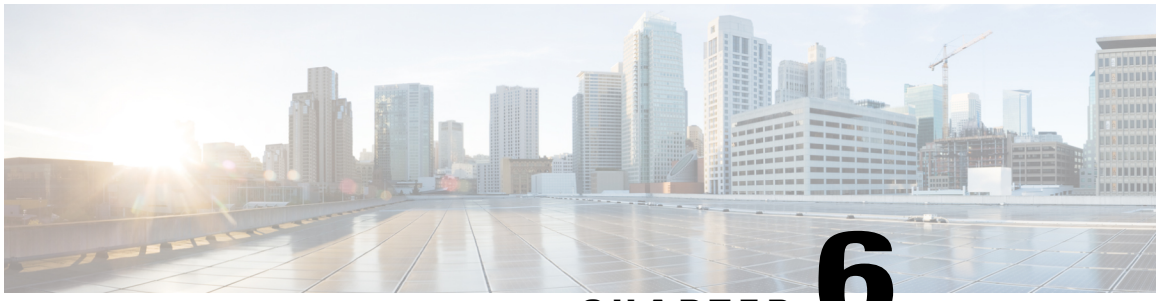
Procedure

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

Step 2 On the **Equipment** tab, click the **Equipment** node.

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

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



CHAPTER 6

UpgradingFirmwarethroughFirmwarePackages in Service Profiles

This chapter includes the following sections:

Firmware Upgrades through Firmware Packages in Service Profiles

You can use firmware packages in service profiles to upgrade the server firmware, including the BIOS on the server, by defining a host firmware policy and including it in the service profile associated with a server.

You cannot upgrade the firmware on the CMC, shared adapter, storage controller, board controller, fabric interconnect, or Cisco UCS Manager through service profiles. You must upgrade the firmware on those endpoints directly.

Note Cisco UCS no longer supports the creation of new management firmware packages. You can modify and update existing management firmware packages, if desired. However, we recommend that you remove the management firmware packages from all service profiles and use host firmware packages to update the Cisco Integrated Management Controller (CIMC) on the servers.

Host Firmware Package

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

- CIMC
- BIOS
- Board controller

Tip You can include more than one type of firmware in the same host firmware package. For example, a host firmware package can include the BIOS firmware, CIMC firmware, and board controller firmware. The system recognizes which firmware version is required for an endpoint and ignores all other firmware versions.

The firmware package 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 for an endpoint in the firmware package, 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.

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 upgrade and completes the association.

Management Firmware Package

Note Cisco UCS no longer supports the creation of new management firmware packages. You can modify and update existing management firmware packages, if desired. However, we recommend that you remove the management firmware packages from all service profiles and use host firmware packages to update the Cisco Integrated Management Controller (CIMC) on the servers.

This policy enables you to specify a set of firmware versions that make up the management firmware package (also known as a management firmware pack). The management firmware package includes the Cisco Integrated Management Controller (CIMC) on the server. You do not need to use this package if you upgrade the CIMC directly.

The firmware package is pushed to all servers associated with service profiles that include this policy. This policy ensures that the CIMC 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.

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 Upgrade through Firmware Packages in Service Profiles

You can use the host firmware package policies in service profiles to upgrade server and adapter firmware.

Caution Unless you have configured and scheduled a maintenance window, if you modify a host firmware package by adding an endpoint or changing firmware versions for an existing endpoint, Cisco UCS Manager upgrades the endpoints and reboots all servers associated with that firmware package as soon as the changes are saved, disrupting data traffic to and from the servers.

New Service Profile

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

Firmware Package Policy Creation

During this stage, you create the host firmware packages.

Service Profile Association

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

Existing Service Profile

For service profiles that are associated with servers, Cisco UCS Manager upgrades the firmware and reboots the server as soon as you save the changes to the firmware packages unless you have configured and scheduled a maintenance window. If you configure and schedule a maintenance window, Cisco UCS Manager defers the upgrade and server reboot until then.

Effect of Updates to Firmware Packages in Service Profiles

To update firmware through a firmware package in a service 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 options for upgrading servers with a firmware package in a service profile.

Service Profile	Maintenance Policy	Upgrade Actions
Firmware package is not included in a service profile or an updating service profile template. OR You want to upgrade the firmware without making any changes to the existing service profile or updating service profile template.	No maintenance policy	After you update the firmware package, do one of the following: • To reboot and upgrade some or all servers simultaneously, add the firmware package to one or more service profiles that are associated with servers or to an updating service profile template. • To reboot and upgrade one server at a time, do the following for each server: **1** Create a new service profile and include the firmware package in that service profile. **2** Dissociate the server from its service profile. **3** Associate the server with the new service profile. **4** After the server has been rebooted and the firmware upgraded, disassociate the server from the new service profile and associate it with its original service profile. **Caution** If the original service profile includes a scrub policy, disassociating a service profile may result in data loss when the disk or the BIOS is scrubbed upon association with the new service profile.
The firmware package is included in one or more service profiles, and the service profiles are associated with one or more servers. OR The firmware package is included in an updating service profile template, and the service profiles created from that template are associated with one or more servers.	No maintenance policy OR A maintenance policy configured for immediate updates.	The following occurs when you update the firmware package: **1** The changes to the firmware package take effect as soon as you save them. **2** Cisco UCS verifies the model numbers and vendor against all servers associated with service profiles that include this policy. If the model numbers and vendor match a firmware version in the policy, Cisco UCS reboots the servers and updates the firmware. All servers associated with service profiles that include the firmware package are rebooted at the same time.

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

Creating a Host Firmware Package

Tip You can include more than one type of firmware in the same host firmware package. For example, a host firmware package can include both BIOS firmware and storage controller firmware or 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.

Before You Begin

Ensure that the appropriate firmware was 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 multitenancy, expand the **root** node.

Step 4 Right-click **Host Firmware Packages** and choose **Create Host Firmware 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 32 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 Select **Advanced** Host Firmware Package configuration.

Step 7 On each subtab, do the following for each type of firmware you want to include in the package:

a) In the **Select** column, ensure that the check box for the appropriate lines are checked.

b) In the **Vendor**, **Model**, and **PID** columns, verify that the information matches the servers you want to update with this package.
The model and model number (PID) must match the servers that are associated with this firmware package. If you select the wrong model or model number, Cisco UCS Manager cannot install the firmware update.

c) In the **Version** column, choose the firmware version to which you want to update the firmware.

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

What to Do Next

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

Updating a Host Firmware Package

If the policy is included in one or more service profiles associated with a server and those service profiles do not include maintenance policies, Cisco UCS Manager updates and activates the firmware in the server and

adapter with the new versions and reboots the server as soon as you save the host firmware package policy unless you have configured and scheduled a maintenance window.

Before You Begin

Ensure that the appropriate firmware was 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 multitenancy, expand the **root** node.

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

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

Step 6 On each subtab, do the following for each type of firmware you want to include in the package:

a) In the **Select** column, ensure that the check box for the appropriate lines are checked.

b) In the **Vendor**, **Model**, and **PID** columns, verify that the information matches the servers you want to update with this package.
The model and model number (PID) must match the servers that are associated with this firmware package. If you select the wrong model or model number, Cisco UCS Manager cannot install the firmware update.

c) In the **Version** column, choose the firmware version to which you want to update the firmware.

Step 7 Click **Save Changes**.
Cisco UCS Manager verifies the model numbers and vendor against all servers associated with service profiles that include this policy. If the model numbers and vendor match a firmware version in the policy, Cisco UCS Manager updates the firmware according to the settings in the maintenance policies included in the service profiles.

Updating a Management Firmware Package

Note Cisco UCS no longer supports the creation of new management firmware packages. You can modify and update existing management firmware packages, if desired. However, we recommend that you remove the management firmware packages from all service profiles and use host firmware packages to update the Cisco Integrated Management Controller (CIMC) on the servers.

If the policy is included in one or more service profiles associated with a server and those service profiles do not include maintenance policies, Cisco UCS Manager updates and activates the management firmware in the server with the new versions and reboots the server as soon as you save the management firmware package policy unless you have configured and scheduled a maintenance window.

Before You Begin

Ensure that the appropriate firmware was 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 multitenancy, expand the **root** node.

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

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

Step 6 In the firmware table, do the following:

a) In the **Select** column, ensure that the check box for the appropriate lines are checked.

b) In the **Vendor**, **Model**, and **PID** columns, verify that the information matches the servers you want to update with this package.
The model and model number (PID) must match the servers that are associated with this firmware package. If you select the wrong model or model number, Cisco UCS Manager cannot install the firmware update.

c) In the **Version** column, choose the firmware version to which you want to update the firmware.

Step 7 Click **Save Changes**.
Cisco UCS Manager verifies the model numbers and vendor against all servers associated with service profiles that include this policy. If the model numbers and vendor match a firmware version in the policy, Cisco UCS Manager updates the firmware according to the settings in the maintenance policies included in the service profiles.

Adding Firmware Packages to an Existing Service Profile

If the service profile does not include a maintenance policy and is associated with a server, Cisco UCS Manager updates and activates the firmware in the server with the new versions and reboots the server as soon as you save the changes to the service profile.

Procedure

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

Step 2 On the **Servers** tab, expand **Servers** > **Service Profiles**.

Step 3 Expand the node for the organization that includes the service profile that you want to update.
If the system does not include multitenancy, expand the **root** node.

Step 4 Click the service profile to which you want to add the firmware packages.

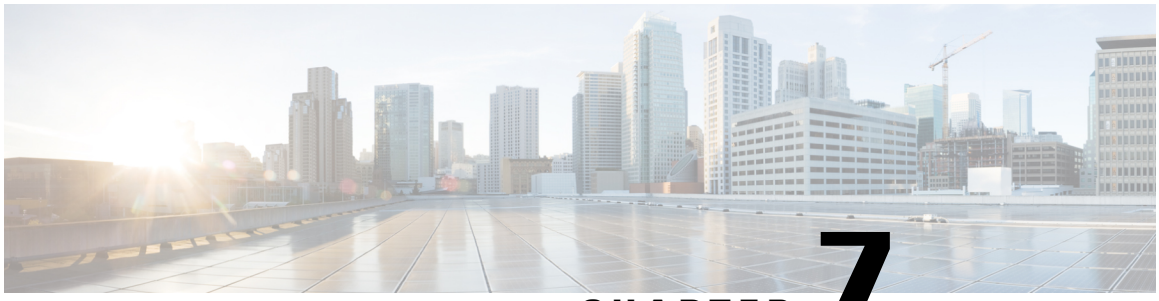
Step 5 In the **Work** pane, click the **Policies** tab.

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

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

Step 8 To add a management firmware package, select the desired policy from the **Management Firmware** drop-down list.

Step 9 Click **Save Changes**.



CHAPTER 7

Managing the Capability Catalog in Cisco UCS Manager

This chapter includes the following sections:

Capability Catalog

The Capability Catalog is a set of tunable parameters, strings, and rules. Cisco UCS uses the catalog to update the display and configurability of components such as newly qualified DIMMs and disk drives for servers.

The catalog is divided by hardware components, such as the chassis, CPU, local disk, and I/O module. You can use the catalog to view the list of providers available for that component. There is one provider per hardware component. Each provider is identified by the vendor, model (PID), and revision. For each provider, you can also view details of the equipment manufacturer and the form factor.

Contents of the Capability Catalog

The contents of the Capability Catalog include the following:

Implementation-Specific Tunable Parameters

- Power and thermal constraints
- Slot ranges and numbering
- Adapter capacities

Hardware-Specific Rules

- Firmware compatibility for components such as the BIOS, CIMC, RAID controller, and adapters
- Diagnostics
- Hardware-specific reboot

User Display Strings

- Part numbers, such as the CPN, PID/VID
- Component descriptions
- Physical layout/dimensions
- OEM information

Updates to the Capability Catalog

Capability Catalog updates are included in each Cisco UCS Infrastructure Software Bundle. Unless otherwise instructed by Cisco TAC, you only need to activate the Capability Catalog update after you've downloaded, updated, and activated a Cisco UCS Infrastructure Software Bundle.

As soon as you activate a Capability Catalog update, Cisco UCS immediately updates to the new baseline catalog. You do not have to perform any further tasks. Updates to the Capability Catalog do not require you to reboot or reinstall any component in a Cisco UCS domain.

Each Cisco UCS Infrastructure Software Bundle contains a baseline catalog. In rare circumstances, Cisco releases an update to the Capability Catalog between Cisco UCS releases and makes it available on the same site where you download firmware images.

Note The Capability Catalog version is determined by the version of Cisco UCS that you are using. For information about Capability Catalog releases supported by specific Cisco UCS releases, see the *Release Notes for Cisco UCS Software*.

Activating a Capability Catalog Update

Procedure

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

Step 2 On the **Admin** tab, expand **All**.

Step 3 Click the **Capability Catalog** node.

Step 4 In the **Work** pane, click the **Catalog Update Tasks** tab.

Step 5 Click **Activate Catalog**.

Step 6 In the **Activate Catalog** dialog box, choose the capability catalog update that you want to activate from the **Version to be Activated** drop-down list.

Step 7 Click **OK**.

Verifying that the Capability Catalog Is Current

Before You Begin

Procedure

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

Step 2 On the **Admin** tab, expand **All**.

Step 3 Click the **Capability Catalog** node.

Step 4 In the **Work** pane, click the **Catalog Update Tasks** tab.
The current version of the capability catalog is located on the upper right of that tab.

Step 5 On Cisco.com, determine the most recent release of the capability catalog available.
For more information about the location of capability catalog updates, see Obtaining Capability Catalog Updates from Cisco, on page 54.

Step 6 If a more recent version of the capability catalog is available on Cisco.com, update the capability catalog with that version.

Viewing a Capability Catalog Provider

Procedure

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

Step 2 On the **Admin** tab, expand **All** > **Capability Catalog**.

Step 3 In the **Work** pane, click the tab for the provider you want to view.

Step 4 To view the details of a provider, do the following:

a) In the table, click the row with the vendor, model, and revision of the provider you want to view.

b) Click the **Expand** icon to the right of the heading to display the properties for the following areas:

- **Equipment Manufacturing** area
- **Form Factor** area

Downloading Individual Capability Catalog Updates

Obtaining Capability Catalog Updates from Cisco

Procedure

Step 1 In a web browser, navigate to Cisco.com.

Step 2 Under **Support**, click **All Downloads**.

Step 3 In the center pane, click **Unified Computing and Servers**.

Step 4 If prompted, enter your Cisco.com username and password to log in.

Step 5 In the right pane, click **Cisco UCS Infrastructure and UCS Manager Software** > **Unified Computing System (UCS) Manager Capability Catalog**.

Step 6 Click the link for the latest release of the Capability Catalog.

Step 7 Click one of the following buttons and follow the instructions provided:

- **Download Now—**Allows you to download the catalog update immediately
- **Add to Cart—**Adds the catalog update to your cart to be downloaded at a later time

Step 8 Follow the prompts to complete your download of the catalog update.

What to Do Next

Update the Capability Catalog.

Updating the Capability Catalog from a Remote Location

You cannot perform a partial update to the Capability Catalog. When you update the Capability Catalog, all components included in the catalog image are updated.

An M-Series server bundle includes the Capability Catalog update for that server. You do not need to download a separate Capability Catalog update. You only need to activate the Capability Catalog update.

Procedure

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

Step 2 On the **Admin** tab, expand **All**.

Step 3 Click the **Capability Catalog** node.

Step 4 In the **Work** pane, click the **Catalog Update Tasks** tab.

Step 5 Click **Update Catalog**.

Step 6 In the **Update Catalog** dialog box, click the **Remote File System** radio button in the **Location of the Image File** field and fill in the required fields.

Step 7 Click **OK**.

Cisco UCS Manager downloads the image and updates the Capability Catalog. You do not need to reboot any hardware components.

What to Do Next

Activate the Capability Catalog update.

Updating the Capability Catalog from the Local File System

You cannot perform a partial update to the Capability Catalog. When you update the Capability Catalog, all components included in the catalog image are updated.

An M-Series server bundle includes the Capability Catalog update for that server. You do not need to download a separate Capability Catalog update. You only need to activate the Capability Catalog update.

Procedure

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

Step 2 On the **Admin** tab, expand **All**.

Step 3 Click the **Capability Catalog** node.

Step 4 In the **Work** pane, click the **Catalog Update Tasks** tab.

Step 5 Click **Update Catalog**.

Step 6 In the **Download Firmware** dialog box, click the **Local File System** radio button in the **Location of the Image File** field.

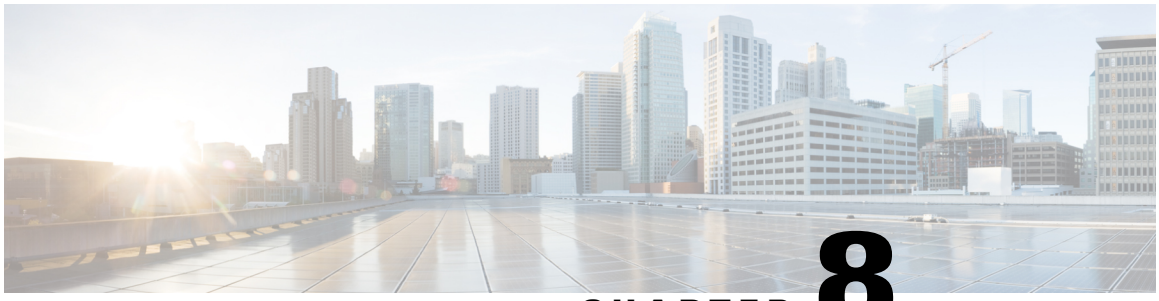
Step 7 In the **Filename** field, type the full path and and name of the image file.
If you do not know the exact path to the folder where the firmware image file is located, click **Browse** and navigate to the file.

Step 8 Click **OK**.

Cisco UCS Manager downloads the image and updates the Capability Catalog. You do not need to reboot any hardware components.

What to Do Next

Activate the Capability Catalog update.



CHAPTER 8

Verifying that the Data Path is Ready

This chapter includes the following sections:

Verifying that Dynamic vNICs Are Up and Running

When you upgrade a Cisco UCS that includes dynamic vNICs and an integration with VMware vCenter, you must verify that all dynamic VNICs are up and running on the new primary fabric interconnect before you activate the new software on the former primary fabric interconnect to avoid data path disruption.

Perform this step in the Cisco UCS Manager GUI.

Procedure

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

Step 2 On the **VM** tab, expand **All** > **VMware** > **Virtual Machines**.

Step 3 Expand the virtual machine for which you want to verify the dynamic vNICs and choose a dynamic vNIC.

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

Step 5 On the **VIF** tab, verify that the **Status** column for each VIF is **Online**.

Step 6 Repeat Steps 3 through 5 until you have verified that the VIFs for all dynamic vNICs on all virtual machines have a status of **Online**.

Verifying the Ethernet Data Path

Procedure

	Command or Action	Purpose
Step 1	UCS-A /fabric-interconnect # **connect nxos** {**a** | **b**}	Enters NX-OS mode for the fabric interconnect.
Step 2	UCS-A(nxos)# **show int br | grep -v down | wc –l**	Returns the number of active Ethernet interfaces. Verify that this number matches the number of Ethernet interfaces that were up prior to the upgrade.
Step 3	UCS-A(nxos)# **show platform fwm info hw-stm | grep '1.' | wc –l**	Returns the total number of MAC addresses. Verify that this number matches the number of MAC addresses prior to the upgrade.

The following example returns the number of active Ethernet interfaces and MAC addresses for subordinate fabric interconnect A so that you can verify that the Ethernet data path for that fabric interconnect is up and running:

```
UCS-A /fabric-interconnect # connect nxos a
UCS-A(nxos)# show int br | grep -v down  | wc -l
86
UCS-A(nxos)# show platform fwm info hw-stm | grep '1.' | wc -l
80
```

Verifying the Data Path for Fibre Channel End-Host Mode

For best results when upgrading a Cisco UCS domain, we recommend that you perform this task before you begin the upgrade and after you activate the subordinate fabric interconnect, and then compare the two results.

Procedure

	Command or Action	Purpose
Step 1	UCS-A /fabric-interconnect # **connect nxos** {**a** | **b**}	Enters NX-OS mode for the fabric interconnect.
Step 2	UCS-A(nxos)# **show npv flogi-table**	Displays a table of flogi sessions.
Step 3	UCS-A(nxos)# **show npv flogi-table | grep fc | wc -l**	Returns the number of servers logged into the fabric interconnect. The output should match the output you received when you performed this verification prior to beginning the upgrade.

The following example displays the flogi-table and number of servers logged into subordinate fabric interconnect A so that you can verify that the Fibre Channel data path for that fabric interconnect in Fibre Channel End-Host mode is up and running:

```
UCS-A /fabric-interconnect # connect nxos a
UCS-A(nxos)# show npv flogi-table
--------------------------------------------------------------------------------
SERVER                                                                  EXTERNAL
INTERFACE VSAN FCID            PORT NAME               NODE NAME       INTERFACE
--------------------------------------------------------------------------------
vfc705    700  0x69000a 20:00:00:25:b5:27:03:01 20:00:00:25:b5:27:03:00 fc3/1
vfc713    700  0x690009 20:00:00:25:b5:27:07:01 20:00:00:25:b5:27:07:00 fc3/1
vfc717    700  0x690001 20:00:00:25:b5:27:08:01 20:00:00:25:b5:27:08:00 fc3/1

Total number of flogi = 3.

UCS-A(nxos)# show npv flogi-table | grep fc | wc -l
3
```

Verifying the Data Path for Fibre Channel Switch Mode

For best results when upgrading a Cisco UCS domain, we recommend that you perform this task before you begin the upgrade and after you activate the subordinate fabric interconnect, and then compare the two results.

Procedure

	Command or Action	Purpose
Step 1	UCS-A /fabric-interconnect # **connect nxos** {**a** | **b**}	Enters NX-OS mode for the fabric interconnect.
Step 2	UCS-A(nxos)# **show flogi database**	Displays a table of flogi sessions.
Step 3	UCS-A(nxos)# **show flogi database | grep –I fc | wc –1**	Returns the number of servers logged into the fabric interconnect. The output should match the output you received when you performed this verification prior to beginning the upgrade.

The following example displays the flogi-table and number of servers logged into subordinate fabric interconnect A so that you can verify that the Fibre Channel data path for that fabric interconnect in Fibre Channel End-Host mode is up and running:

```
UCS-A /fabric-interconnect # connect nxos a
UCS-A(nxos)# show flogi database
--------------------------------------------------------------------------------
INTERFACE        VSAN    FCID           PORT NAME               NODE NAME
--------------------------------------------------------------------------------
vfc726           800   0xef0003  20:00:00:25:b5:26:07:02 20:00:00:25:b5:26:07:00
vfc728           800   0xef0007  20:00:00:25:b5:26:07:04 20:00:00:25:b5:26:07:00
vfc744           800   0xef0004  20:00:00:25:b5:26:03:02 20:00:00:25:b5:26:03:00
vfc748           800   0xef0005  20:00:00:25:b5:26:04:02 20:00:00:25:b5:26:04:00
vfc764           800   0xef0006  20:00:00:25:b5:26:05:02 20:00:00:25:b5:26:05:00
```

```
vfc768           800   0xef0002  20:00:00:25:b5:26:02:02 20:00:00:25:b5:26:02:00
vfc772           800   0xef0000  20:00:00:25:b5:26:06:02 20:00:00:25:b5:26:06:00
vfc778           800   0xef0001  20:00:00:25:b5:26:01:02 20:00:00:25:b5:26:01:00

Total number of flogi = 8.
UCS-A(nxos)# show flogi database | grep fc | wc -l
8
```