Cisco UCS M-Series CLI 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 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.

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.

Options for Firmware Upgrades

You can upgrade Cisco UCS firmware through one or more of the following methods:

Note For a summary of steps and the required order in which to perform them in order to upgrade one or more Cisco UCS domains from one release to another, see the Cisco UCS upgrade guide for that upgrade path. If an upgrade guide is not provided for upgrading from a particular release, contact Cisco TAC as a direct upgrade from that release may not be supported.

Upgrading a Cisco UCS domain through Cisco UCS Manager

If you want to upgrade a Cisco UCS domain through the Cisco UCS Manager in that domain, you can choose one of the following upgrade options:

- Upgrade infrastructure and servers with Auto Install—This option upgrades all infrastructure components in the first stage. Then you can upgrade all server endpoints through host firmware packages in the second stage.

  Note You cannot use Auto Install to update a Cisco UCS M-Series chassis.

- Upgrade servers through firmware packages in service profiles—This option enables you to upgrade all server endpoints in a single step, reducing the amount of disruption caused by a server reboot. You can combine this option with the deferred deployment of service profile updates to ensure that server reboots occur during scheduled maintenance windows.
- Direct upgrades of infrastructure and server endpoints—This option enables you to upgrade many infrastructure and server endpoints directly, including the fabric interconnects, shared adapters, and board controllers. However, direct upgrade is not available for all endpoints, including the server BIOS, storage controller, and local disk. You must upgrade those endpoints through the host firmware package included in the service profile associated with the server.

Configuration Changes and Settings that Can Impact Upgrades

Depending upon the configuration of your Cisco UCS domain, the following changes may require you to make configuration changes after you upgrade. To avoid faults and other issues, we recommend that you make any required changes before you upgrade.

Impact of Upgrade to Cisco UCS, Release 2.1(2) and Higher on Initiator IQNs Defined at the Service Profile Level

If there are two iSCSI vNICs and both use the same initiator IQN (which is supported in Cisco UCS Release 2.0(1)), upgrading creates a single service profile level initiator IQN and resets the initiator IQNs on the iSCSI vNICs to have no value.

If the same initiator IQNs are used in iSCSI vNICs across service profiles in Cisco UCS Release 2.0(1), the upgrade creates duplicate initiator IQNs at the service profile level. This configuration generates faults for each iSCSI vNIC that has a duplicate initiator IQN defined at the service profile level. Changing the duplicate initiator IQNs at the service profile level clears these faults. You must clear these faults before you perform any service profile related operations, such as updating a host firmware package.

Default Maintenance Policy Should be Configured for User Acknowledgment

The default maintenance policy is configured to immediately reboot the server when disruptive changes are made to the service profile, such as server firmware upgrades through a host maintenance policy. We recommend that you change the reboot policy setting in the default maintenance policy to user acknowledgment to avoid unexpected disruption of server traffic.

When you configure the reboot policy in the default maintenance policy to User Ack, the list of disruptive changes are listed with the pending activities. You can then control when the servers are rebooted.

Overlapping FCoE VLAN IDs and Ethernet VLAN IDs Are No Longer Allowed with Cisco UCS Release 2.0 and Higher

Caution In Cisco UCS 1.4 and earlier releases, Ethernet VLANs and FCoE VLANs could have overlapping VLAN IDs. However, starting with Cisco UCS release 2.0, overlapping VLAN IDs are not allowed. If Cisco UCS Manager detects overlapping VLAN IDs during an upgrade, it raises a critical fault. If you do not reconfigure your VLAN IDs, Cisco UCS Manager raises a critical fault and drops Ethernet traffic on the overlapped VLANs. Therefore, we recommend that you ensure there are no overlapping Ethernet and FCoE VLAN IDs before you upgrade to Cisco UCS Release 2.2.

Be aware that when an uplink trunk is configured with VLAN ID 1 defined and set as the native VLAN, changing the Ethernet VLAN 1 ID to another value can cause network disruption and flapping on the fabric interconnects, resulting in an HA event that introduces a large amount of traffic and makes services temporarily unavailable.

If you did not explicitly configure the FCoE VLAN ID for a VSAN in Cisco UCS 1.4 and earlier releases, Cisco UCS Manager assigned VLAN 1 as the default FCoE VLAN for the default VSAN (with default VSAN ID 1). In those releases, VLAN 1 was also used as the default VLAN for Ethernet traffic. Therefore, if you accepted the default VLAN ID for the FCoE VLAN and one or more Ethernet VLANs, you must reconfigure the VLAN IDs for either the FCoE VLAN(s) on the VSAN(s) or the Ethernet VLAN(s).

For a new installation of Cisco UCS Release 2.2, the default VLAN IDs are as follows:

- The default Ethernet VLAN ID is 1.
- The default FCoE VLAN ID is 4048.

After an upgrade from Cisco UCS Release 1.4, where VLAN ID 4048 was used for FCoE storage port native VLAN, to release 2.0, the default VLAN IDs are as follows:

- The default Ethernet VLAN ID is 1.
- The current default FCoE VLAN ID is preserved. Cisco UCS Manager raises a critical fault on the conflicting Ethernet VLAN, if any. You must change one of the VLAN IDs to a VLAN ID that is not used or reserved.

Note If a Cisco UCS domain uses one of the default VLAN IDs, which results in overlapping VLANs, you can change one or more of the default VLAN IDs to any VLAN ID that is not used or reserved. From release 2.0 and higher, VLANs with IDs from 4030 to 4047 are reserved.

Important VSAN, FC and FCoE are not supported in Cisco UCS Release 2.5.

PART I

Managing Firmware through Cisco UCS Manager

CHAPTER 2

Downloading and Managing Firmware in Cisco UCS Manager

This chapter includes the following sections:

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 M-Series 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

	Command or Action	Purpose
Step 1	UCS-A# **scope firmware**	Enters firmware mode.
Step 2	UCS-A /firmware # **download image** *URL*	Downloads the firmware bundle. Using the download path provided by Cisco, specify the URL with one of the following syntax: • **ftp:**// *server-ip-addr* / *path* • **scp:**// *username@server-ip-addr* / *path* • **sftp:**// *username@server-ip-addr* / *path* • **tftp:**// *server-ip-addr* **:** *port-num* / *path* **Note** TFTP has a file size limitation of 32 MB. Because firmware bundles can be much larger than that, we recommend that you do not select TFTP for firmware downloads. If you use a hostname rather than an IP address, configure a DNS server in Cisco UCS Manager.
Step 3	Enter the password for the remote server.	The password for the remote server username. This field does not apply if the protocol is tftp.
Step 4	UCS-A /firmware # **show download-task**	Displays the status for your download task. When your image is completely downloaded, the task state changes from Downloading to Downloaded. The CLI does not automatically refresh, so you may have to enter the **show download-task** command multiple times until the task state displays Downloaded.
Step 5	Repeat this task until all of the firmware bundles have been downloaded to the fabric interconnect.	

The following example uses SCP to download the firmware package.

```
UCS-A# scope firmware
UCS-A /firmware # download image
scp://user1@192.168.10.10/images/ucs-k9-bundle-m-series.2.5.0.224.M.bin
UCS-A /firmware # show download-task
UCS-A /firmware #
```

What to Do Next

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

Displaying the Firmware Package Download Status

After a firmware download operation has been started, you can check the download status to see if the package is still downloading or if it has completely downloaded.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope firmware**	Enters firmware mode.
Step 2	UCS-A /firmware # **show download-task**	Displays the status for your download task. When your image is completely downloaded, the task state changes from Downloading to Downloaded. The CLI does not automatically refresh, so you may have to enter the **show download-task** command multiple times until the task state displays Downloaded.

The following example displays the download status for the firmware package. The **show download-task** command is entered multiple times until the download state indicates that the firmware package has been downloaded:

```
UCS-A# scope firmware
UCS-A /firmware # show download-task

Download task:
File Name                                    Protocol     Server          Userid      State
---------                                    --------     --------------- ---------   -----
ucs-k9-bundle-m-series.2.5.0.224.M.bin         Scp          10.193.32.11    user1
Downloading

UCS-A /firmware # show download-task

Download task:
File Name                                    Protocol     Server          Userid      State
---------                                    --------     --------------- ---------   -----
ucs-k9-bundle-m-series.2.5.0.224.M.bin         Scp          10.193.32.11    user1
Downloaded
```

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

	Command or Action	Purpose
Step 1	UCS-A# **scope firmware**	Enters firmware mode.

	Command or Action	Purpose
Step 2	UCS-A /firmware # **delete download-task** *image_filename*	Deletes the specified image file.
Step 3	UCS-A /firmware # **commit-buffer**	Commits the transaction to the system configuration.

The following example cancels an image download:

```
UCS-A# scope firmware
UCS-A /firmware # delete download-task ucs-k9-bundle-m-series.2.5.0.202.M.bin
UCS-A /firmware* # commit-buffer
UCS-A /firmware* #
```

Displaying All Available Software Images on the Fabric Interconnect

This procedure is optional and displays the available software images on the fabric interconnect for all endpoints. You can also use the **show image** command in each endpoint mode to display the available software images for that endpoint.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope firmware**	Enters firmware mode.
Step 2	UCS-A /firmware # **show image**	Displays all software images downloaded onto the fabric interconnect. **Note** You must provide the software version number when directly updating an endpoint. If you intend to directly update firmware at an endpoint, note its version number in the right column.

The following example displays all available software images on the fabric interconnect:

```
UCS-A# scope firmware
UCS-A /firmware # show image
Name                                          Type                 Version
--------------------------------------------- -------------------- -------
ucs-4308-brdprog.1.0.6.bin                    Board Controller     1.0.6
ucs-4308.2.0.2.45.bin                         Chassis Management Controller
                                                                   2.0(2.45)
ucs-6100-k9-kickstart.5.2.3.N2.2.50.225.bin   Fabric Interconnect Kernel
                                                                   5.2(3)N2(2.50.225)
ucs-6100-k9-system.5.2.3.N2.2.50.225.bin      Fabric Interconnect System
                                                                   5.2(3)N2(2.50.225)
ucsme-142-m4-bios.UCSME.142M4.2.0.100.54.011620150100.bin
                                              Server BIOS
UCSME.142M4.2.0.100.54.011620150100
ucsme-142-m4-k9-cimc.2.0.100.59.bin           CIMC                 2.0(100.59)
```

Displaying All Available Packages on the Fabric Interconnect

This procedure is optional and displays the available software packages on the fabric interconnect for all endpoints.. You can also use the **show package** command in each endpoint mode to display the available software images for that endpoint.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope firmware**	Enters firmware mode.
Step 2	UCS-A /firmware # **show package**	Displays all software packages downloaded onto the fabric interconnect. **Note** You must provide the software version number when directly updating an endpoint. If you intend to directly update firmware at an endpoint, note its version number in the right column.

The following example displays all available software packages on the fabric interconnect:

```
UCS-A# scope firmware
UCS-A /firmware # show package
```

Determining the Contents of a Firmware Package

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope firmware**	Enters firmware mode.
Step 2	UCS-A /firmware # **show package** *package-name* **expand**	Displays the contents of the specified firmware package.

The following example displays the contents of a firmware package:

```
UCS-A# scope firmware
UCS-A /firmware # show package ucs-k9-bundle-m-series.2.5.0.224.M.bin expand
Package ucs-k9-bundle-m-series.2.5.0.224.M.bin:

  Images:
      ucs-4308-brdprog.1.0.6.bin
      ucs-4308.2.0.2.45.bin
      ucs-m-lsi-mrsas-9361-8i.24.5.1.9.bin
      ucs-m83-8p40-vic.4.0.2S47.bin
      ucsme-142-m4-bios.UCSME.142M4.2.0.100.54.011620150100.bin
      ucsme-142-m4-k9-cimc.2.0.100.59.bin

UCS-A /firmware #
```

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

	Command or Action	Purpose
Step 1	UCS-A# **scope fabric-interconnect** {**a** | **b**}	Enters fabric interconnect mode for the specified fabric.
Step 2	UCS-A /fabric-interconnect # **show storage** [**detail** | **expand**}	Displays the available space for the specified fabric. **Note** 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.

The following example displays the available space for a fabric interconnect:

```
UCS-A# scope fabric-interconnect a
UCS-A /fabric-interconnect # show storage
Storage on local flash drive of fabric interconnect:
    Partition        Size (MBytes)    Used Percentage
    ---------------- ---------------- ---------------
    bootflash        8658             50
    opt              1917             2
    workspace        277              4
UCS-A /fabric-interconnect #
```

Deleting Firmware Packages from a Fabric Interconnect

Use this procedure if you want to delete an entire package. If you prefer, you can also delete only a single image from a package.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope firmware**	Enters firmware mode.
Step 2	UCS-A /firmware # **delete package** *package-name*	Deletes the specified firmware package.
Step 3	UCS-A /firmware # **commit-buffer**	Commits the transaction to the system configuration.

Cisco UCS Manager deletes the selected package or packages and all images contained within each package.

The following example deletes a firmware package and commits the transaction:

```
UCS-A# scope firmware
UCS-A /firmware # delete package ucs-k9-bundle-infra.2.5.0.224.A.bin
UCS-A /firmware* # commit-buffer
UCS-A /firmware #
```

Deleting Firmware Images from a Fabric Interconnect

Use this procedure if you want to delete only a single image from a package.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope firmware**	Enters firmware mode.
Step 2	UCS-A /firmware # **delete image** *image-name*	Deletes the specified firmware image.
Step 3	UCS-A /firmware # **commit-buffer**	Commits the transaction to the system configuration.

The following example deletes a firmware image and commits the transaction:

```
UCS-A# scope firmware
UCS-A /firmware # delete image ucs-m-lsi-mrsas-9361-8i.24.5.1.8.bin
UCS-A /firmware* # commit-buffer
UCS-A /firmware #
```

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.

Cautions, Guidelines, and Limitations for Upgrading with Auto Install

Before you use Auto Install to upgrade the firmware for any endpoint in a Cisco UCS domain, consider the following cautions, guidelines, and limitations:

Note These guidelines are specific to Auto Install and are in addition to those listed in Cautions, Guidelines, and Limitations for Firmware Upgrades.

State of the Endpoints

Before you begin an upgrade, all affected endpoints must be in the following state:

- For a cluster configuration, verify that the high availability status of the fabric interconnects shows that both are up and running.
- For a standalone configuration, verify that the Overall Status of the fabric interconnect is Operable.

- For all endpoints to be upgraded, verify that they are in an Operable state.
- For all servers to be upgraded, verify that all the servers have been discovered and that discovery did not fail. Install Server Firmware will fail if any server endpoints cannot be upgraded.

Recommendations for the Default Host Firmware Policy

After you upgrade Cisco UCS Manager, a new host firmware policy named "default" is created, and assigned to all service profiles that did not already include a host firmware policy. The default host firmware policy is blank. It does not contain any firmware entries for any components. This default policy is also configured for an immediate reboot rather than waiting for user acknowledgment before rebooting the servers.

During the upgrade of server firmware, you can add firmware for the servers in the Cisco UCS domain to the default host firmware policy. To complete the upgrade, all servers must be rebooted.

Every service profile that is assigned the default host firmware policy reboots the associated server according to the maintenance policy included in the service profile. If the maintenance policy is set to immediate reboot, you cannot cancel the upgrade or prevent the servers from rebooting after you complete the configuration in the **Install Server Firmware** wizard. We recommend that you verify the maintenance policy associated with these service profiles to ensure that they are set for a timed reboot or for user acknowledgment.

Time, Date, and Time Zone on Fabric Interconnects Must Be Identical

To ensure that the fabric interconnects in a cluster configuration are in sync, you must ensure that they are configured for the same date, time, and time zone. We recommend that you configure an NTP server and the correct time zone in both fabric interconnects. If the date, time or time zone in the fabric interconnects are out of sync, the Auto Install might fail.

Cannot Upgrade Infrastructure and Server Firmware Simultaneously

You cannot upgrade the infrastructure firmware at the same time as you upgrade server firmware. We recommend that you upgrade the infrastructure firmware first and then upgrade the server firmware. Do not begin the server firmware upgrade until the infrastructure firmware upgrade is completed.

Required Privileges

Users must have the following privileges to upgrade endpoints with Auto Install:

Privileges	Upgrade Tasks User Can Perform
admin	• Run Install Infrastructure Firmware • Run Install Server Firmware • Add, delete, and modify host firmware packages
Service profile compute (ls-compute)	Run Install Server Firmware
Service profile server policy (ls-server-policy)	Add, delete, and modify host firmware packages
Service profile config policy (ls-config-policy)	Add, delete, and modify host firmware packages

Impact of Host Firmware Packages and Management Firmware Packages on Install Server Firmware

Because Install Server Firmware uses host firmware packages to upgrade the servers, you do not have to upgrade all servers in a Cisco UCS domain to the same firmware versions. However, all servers which have associated service profiles that include the host firmware packages you selected when you configured Install Server Firmware are upgraded to the firmware versions in the specified software bundles.

If the service profiles associated with servers include a management firmware package as well as a host firmware package, Install Server Firmware uses the firmware version in the management firmware package to upgrade the CIMC on the servers. The CIMC is not upgraded to the firmware version in the host firmware package, even if it is a more recent version of the CIMC than the one in the management firmware package. If you want to use the host firmware packages to upgrade the CIMC in the servers, you must remove the management firmware packages from the associated service profiles.

Effect of Using Install Server Firmware on Servers Whose Service Profiles Do Not Include a Host Firmware Package

If you use Install Server Firmware to upgrade server endpoints on servers that have associated service profiles without host firmware packages, Install Server Firmware uses the default host firmware package to upgrade the servers. You can only update the default host firmware package through Install Server Firmware.

If you want to upgrade the CIMC or BIOS in a server with an associated service profile that has previously been updated through the default host firmware package in Install Server Firmware, you must use one of the following methods:

- Use Install Server Firmware to modify the default host firmware package and then upgrade the server through Install Server Firmware.
- Create a new host firmware package policy, assign it to the service profile associated with the server, and then upgrade the server through that host firmware package policy.
- Disassociate the service profile from the service profile and then directly upgrade the server endpoints.

Upgrading Server Firmware on Newly Added Servers

If you add a server to a Cisco UCS domain after you run Install Server Firmware, the firmware on the new server is not automatically upgraded by Install Server Firmware. If you want to upgrade the firmware on a newly added server to the firmware version used when you last ran Install Server Firmware, you must manually upgrade the endpoints to upgrade the firmware on that server. Install Server Firmware requires a change in firmware version each time. You cannot rerun Install Server Firmware to upgrade servers to the same firmware version.

Note After you finish the upgrade to Release 2.2, you can use the **Firmware Auto Sync Server** policy in Cisco UCS Manager to automatically update newly discovered servers.

Upgrading the Infrastructure Firmware

The **auto-install** scope is not available if the Cisco UCS Manager CLI 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

	Command or Action	Purpose
Step 1	UCS-A# **scope firmware**	Enters firmware mode.
Step 2	UCS-A /firmware # **scope auto-install**	Enters auto-install mode for infrastructure firmware upgrades.
Step 3	UCS-A /firmware/auto-install # **install infra infra-vers** *infrastructure-bundle-version* [**starttime** *mon dd yyyy hh min sec*] [**force**]	Updates and activates the infrastructure firmware. You must use **starttime** to schedule the infrastructure firmware upgrade, if you do not want the upgrade to start as soon as you commit the transaction. If you use **starttime**, enter the following information to specify when you want to schedule the upgrade: • *mon*—The first three letters of the desired month, such as jan or feb. • *dd*—The number of the desired day of the month, from 1 to 31. • *yyyy*—The four numbers of the desired year, such as 2012. • *hh*—The hour when you want the upgrade to start, from 0 to 23. • *min*—The minute when you want the upgrade to start, from 0 to 60. • *sec*—The second when you want the upgrade to start, from 0 to 60. Use the **force** keyword to activate the firmware regardless of any possible incompatibilities or currently executing tasks. **Caution** Review the checklist that displays and ensure you have met all the requirements before you continue with the upgrade.
Step 4	UCS-A /firmware/auto-install # **commit-buffer**	Commits the transaction to the system configuration. **Note** If there is not enough space under bootflash, a warning will display and the upgrade process will stop.

This example shows how to upgrade the infrastructure to the firmware in the Cisco UCS Infrastructure Software Bundle and commit the transaction:

```
UCS-A# scope firmware
UCS-A /firmware # scope auto-install
```

```
UCS-A /firmware/auto-install # install infra infra-vers ucs-k9-bundle-infra.2.5.0.225.A.bin
This operation upgrades firmware on UCS Infrastructure Components
(UCS manager, Fabric Interconnects and IOMs).
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup
(3) Check if Management Interface Monitoring Policy is enabled
(4) Check if there is a pending Fabric Interconnect Reboot activitiy
(5) Ensure NTP is configured
Do you want to proceed? (yes/no): yes
UCS-A /firmware/auto-install* # commit-buffer
UCS-A /firmware/auto-install #
```

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.

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

	Command or Action	Purpose
Step 1	UCS-A# **scope firmware**	Enters firmware mode.
Step 2	UCS-A /firmware # **scope auto-install**	Enters auto-install mode for infrastructure firmware upgrades.
Step 3	UCS-A /firmware/auto-install # **acknowledge primary fabric-interconnect reboot**	Acknowledges the pending reboot of the primary fabric interconnect.

	Command or Action	Purpose
Step 4	UCS-A /firmware/auto-install # **commit-buffer**	Commits the transaction to the system configuration. Cisco UCS Manager immediately reboots the primary fabric interconnect. You cannot stop this reboot after you commit the transaction.

This example shows how to acknowledge the reboot of the primary fabric interconnect and commit the transaction:

```
UCS-A# scope firmware
UCS-A /firmware # scope auto-install
UCS-A /firmware/auto-install # acknowledge primary fabric-interconnect reboot
UCS-A /firmware/auto-install* # commit-buffer
UCS-A /firmware/auto-install #
```

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

	Command or Action	Purpose
Step 1	UCS-A# **scope firmware**	Enters firmware mode.
Step 2	UCS-A /firmware # **scope auto-install**	Enters auto-install mode for infrastructure firmware upgrades.
Step 3	UCS-A /firmware/auto-install # **cancel install infra**	Cancels the scheduled infrastructure firmware upgrade.
Step 4	UCS-A /firmware/auto-install # **commit-buffer**	Commits the transaction to the system configuration.

The following example cancels a scheduled infrastructure firmware upgrade and commits the transaction:

```
UCS-A# scope firmware
UCS-A /firmware # scope auto-install
UCS-A /firmware/auto-install # cancel install infra
UCS-A /firmware/auto-install* # commit-buffer
UCS-A /firmware/auto-install #
```

CHAPTER 4

Directly Upgrading Firmware at Endpoints

This chapter includes the following sections:

Direct Firmware Upgrade at Endpoints

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

You can directly upgrade the firmware on the following endpoints:

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

- CIMC
- BIOS
- Board Controller

- Infrastructure:
  - Fabric interconnects
  - Cisco UCS Manager

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

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

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

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

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

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

Stages of a Direct Firmware Upgrade

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

Update

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

The update stage applies only to the following endpoints:

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

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

Activate

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

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

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

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

Outage Impacts of Direct Firmware Upgrades

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

Outage Impact of a Fabric Interconnect Firmware Upgrade

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

Outage Impact of a Cisco UCS Manager Firmware Upgrade

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

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

  Any unsaved work in progress is lost.
- Cisco UCS Manager CLI—All users logged in through telnet are logged out and their sessions ended.

Outage Impact of a CMC Firmware Upgrade

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

Outage Impact of a Shared Adapter Firmware Upgrade

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

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

Outage Impact of a Storage Controller Firmware Upgrade

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

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

Outage Impact of a Board Controller Firmware Upgrade

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

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

Outage Impact of a BIOS Firmware Upgrade

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

Outage Impact of a CIMC Firmware Upgrade

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

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

Outage Impact of a Board Controller Firmware Upgrade on a Server

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

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

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

Updating and Activating the CMC Firmware on a Chassis

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

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope chassis** *chassis-id*	Enters chassis server mode for the specified server.
Step 2	UCS-A /chassis # **scope cmc**	Enters chassis CMC mode.
Step 3	UCS-A /chassis/cmc # **update firmware** *version-num*	Updates the selected firmware version on the CMC in the chassis.
Step 4	UCS-A /chassis/cmc # **commit-buffer**	(Optional) Commits the transaction. Use this step only if you intend to use the **show update status** command in Step 5 to verify that the firmware update completed successfully before activating the firmware in Step 6. You can skip this step and commit the **update firmware** and **activate firmware** commands in the same transaction; however, if the

	Command or Action	Purpose
		firmware update does not complete successfully, the firmware activation does not start. Cisco UCS Manager copies the selected firmware image to the backup memory partition and verifies that image is not corrupt. The image remains as the backup version until you explicitly activate it.
Step 5	UCS-A /chassis/cmc # **show update status**	(Optional) Displays the status of the firmware update. Use this step only if you want to verify that the firmware update completed successfully. The firmware update is complete when the update status is Ready. The CLI does not automatically refresh, so you may have to enter the **show update status** command multiple times until the task state changes from Updating to Ready. Continue to Step 6 when the update status is Ready.
Step 6	UCS-A /chassis/cmc # **activate firmware** *version-num*	Activates the selected firmware version on the CMC in the server.
Step 7	UCS-A /chassis/cmc # **commit-buffer**	Commits the transaction.
Step 8	UCS-A /chassis/cmc # **show activate status**	(Optional) Displays the status of the firmware activation. Use this step only if you want to verify that the firmware activation completed successfully. The CLI does not automatically refresh, so you may have to enter the **show activate status** command multiple times until the task state changes from Activating to Ready.
Step 9	CS-A /chassis/cmc # **show firmware**	(Optional) Displays the running firmware version, the Update status and the Activate status.

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

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

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

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

Updating and Activating the Shared Adapter Firmware on a Chassis

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

Before You Begin

Gracefully power down the servers.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope chassis** *chassis-id*	Enters chassis mode for the specified chassis.
Step 2	UCS-A /chassis # **scope adapter**	Enters chassis adapter mode.
Step 3	UCS-A /chassis/adapter # **show image**	Displays the available software images for the shared adapter.
Step 4	UCS-A /chassis/adapter # **update firmware** *version-num*	Updates the selected firmware version on the shared adapter.
Step 5	UCS-A /chassis/adapter # **commit-buffer**	(Optional) Commits the transaction. Use this step only if you intend to use the **show update status** command in Step 6 to verify that the firmware update completed successfully before activating the firmware in Step 7. You can skip this step and commit the **update firmware** and **activate firmware** commands in the same transaction; however, if the firmware update does not complete successfully, the firmware activation does not start.

	Command or Action	Purpose
Step 6	UCS-A /chassis/adapter # **show update status**	(Optional) Displays the status of the firmware update. Use this step only if you want to verify that the firmware update completed successfully. The firmware update is complete when the update status is Ready. The CLI does not automatically refresh, so you may have to enter the **show update status** command multiple times until the task state changes from Updating to Ready. Continue to Step 7 when the update status is Ready.
Step 7	UCS-A /chassis/adapter # **activate firmware** *version-num*	Activates the selected firmware version on the shared adapter.
Step 8	UCS-A /chassis/adapter # **commit-buffer**	Commits the transaction.
Step 9	UCS-A /chassis/adapter # **show activate status**	Displays the status of the firmware activation. Use this step only if you want to verify that the firmware activation completed successfully. The CLI does not automatically refresh, so you may have to enter the **show activate status** command multiple times until the task state changes from Activating to Ready.
Step 10	UCS-A /chassis/adapter # **show firmware**	(Optional) Displays the running firmware version, the Update status and the Activate status.

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

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

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

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

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

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

Activating the Storage Controller Firmware on a Chassis

Before You Begin

Gracefully power down the servers.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope chassis** *chassis-id*	Enters chassis mode for the specified chassis.
Step 2	UCS-A /chassis # **scope raid-controller** *raid-id* {**sas** | **sd** | **flash** | **sata** | **unknown**	Enters storage controller mode for the chassis.
Step 3	UCS-A /chassis/raid-controller # **activate firmware** *version-num*	Activates the selected firmware version on the storage controller in the chassis.
Step 4	UCS-A /chassis/raid-controller # **commit-buffer**	Commits the transaction to the system configuration.
Step 5	UCS-A /chassis/raid-controller # **show activate status**	Displays the status of the firmware activation.

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

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

Activating the Board Controller Firmware on a Chassis

Before You Begin

Gracefully power down the servers.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope chassis** *chassis-id*	Enters chassis mode for the specified chassis.
Step 2	UCS-A /chassis #**scope boardcontroller**	Enters board controller mode for the chassis.
Step 3	UCS-A /chassis/boardcontroller # **activate firmware** *version-num*	Activates the selected firmware version on the board controller in the chassis.
Step 4	UCS-A /chassis/boardcontroller # **commit-buffer**	Commits the transaction to the system configuration.
Step 5	UCS-A /chassis/boardcontroller # **show firmware**	Displays the running firmware version and the Activate status.

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

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

Updating and Activating the BIOS Firmware on a Server

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

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

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope server** *chassis-id / cartridge-id / server-id*	Enters chassis server mode for the specified server.
Step 2	UCS-A /chassis/cartridge/server # **scope bios**	Enters chassis server BIOS mode.
Step 3	UCS-A /chassis/cartridge/server/bios # **update firmware** *version-num*	Updates the selected BIOS firmware for the server.
Step 4	UCS-A /chassis/cartridge/server/bios # **commit-buffer**	(Optional) Commits the transaction. Use this step only if you intend to use the **show firmware** command in Step 5 to verify that the firmware update completed successfully before activating the firmware in Step 6. You can skip this step and commit the **update firmware** and **activate firmware** commands in the same transaction; however, if the firmware update does not complete successfully, the firmware activation does not start. Cisco UCS Manager copies the selected firmware image to the backup memory partition and verifies that image is not corrupt. The image remains as the backup version until you explicitly activate it.
Step 5	UCS-A /chassis/cartridge/server/bios # **show firmware**	(Optional) Displays the status of the firmware update. Use this step only if you want to verify that the firmware update completed successfully. The firmware update is complete when the update status is Ready. The CLI does not automatically refresh, so you may have to enter the **show firmware** command multiple times until the task state changes from Updating to Ready. Continue to Step 6 when the update status is Ready.

	Command or Action	Purpose
Step 6	UCS-A /chassis/cartridge/server/bios # **activate firmware** *version-num*	Activates the selected server BIOS firmware version.
Step 7	UCS-A /chassis/cartridge/server/bios # **commit-buffer**	Commits the transaction.
Step 8	UCS-A /chassis/cartridge/server/bios # **show firmware**	(Optional) Displays the status of the firmware activation. Use this step only if you want to verify that the firmware activation completed successfully. The CLI does not automatically refresh, so you may have to enter the **show firmware** command multiple times until the task state changes from Activating to Ready.

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

```
UCS-A# scope server 1/2/1
UCS-A# /chassis/cartridge/server # scope bios
UCS-A# /chassis/cartridge/server/bios # update firmware UCSME.142M4.2.0.100.52.122920140321
UCS-A# /chassis/cartridge/server/bios # activate firmware UCSME.142M4.2.0.100.52.122920140321
UCS-A# /chassis/cartridge/server/bios* # commit-buffer
```

Updating and Activating the CIMC Firmware on a Server

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

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

Procedure

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

	Command or Action	Purpose
Step 3	UCS-A /chassis/cartridge/server/cimc # **show image**	Displays the available software images for the adapter.
Step 4	UCS-A /chassis/cartridge/server/cimc # **update firmware** *version-num*	Updates the selected firmware version on the CIMC in the server.
Step 5	UCS-A /chassis/cartridge/server/cimc # **commit-buffer**	(Optional) Commits the transaction. Use this step only if you intend to use the **show firmware** command in Step 6 to verify that the firmware update completed successfully before activating the firmware in Step 7. You can skip this step and commit the **update-firmware** and **activate-firmware** commands in the same transaction; however, if the firmware update does not complete successfully, the firmware activation does not start. Cisco UCS Manager copies the selected firmware image to the backup memory partition and verifies that image is not corrupt. The image remains as the backup version until you explicitly activate it.
Step 6	UCS-A /chassis/cartridge/server/cimc # **show firmware**	(Optional) Displays the status of the firmware update. Use this step only if you want to verify that the firmware update completed successfully. The firmware update is complete when the update status is Ready. The CLI does not automatically refresh, so you may have to enter the **show firmware** command multiple times until the task state changes from Updating to Ready. Continue to Step 7 when the update status is Ready.
Step 7	UCS-A /chassis/cartridge/server/cimc # **activate firmware** *version-num*	Activates the selected firmware version on the CIMC in the server.
Step 8	UCS-A /chassis/cartridge/server/cimc # **commit-buffer**	Commits the transaction.
Step 9	UCS-A /chassis/cartridge/server/cimc # **show firmware**	(Optional) Displays the status of the firmware activation. Use this step only if you want to verify that the firmware activation completed successfully. The CLI does not automatically refresh, so you may have to enter the **show firmware** command multiple times until the task state changes from Activating to Ready.

The following example updates and activates the CIMC firmware to version 2.0(100.46) in the same transaction, without verifying that the firmware update and firmware activation completed successfully:

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

The following example updates the CIMC firmware to version 2.0(100.46), verifies that the firmware update completed successfully before starting the firmware activation, activates the CIMC firmware, and verifies that the firmware activation completed successfully:

```
UCS-A# scope server 1/1
UCS-A# /chassis/cartridge/server # scope cimc
UCS-A# /chassis/cartridge/server/cimc # update firmware 2.0(100.46)
UCS-A# /chassis/cartridge/server/cimc* # commit-buffer
UCS-A# /chassis/cartridge/server/cimc # show firmware
Running-Vers    Update-Status   Activate-Status
--------------- --------------- ---------------
2.0(100.46)     Updating        Ready

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

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

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

Activating the Board Controller Firmware on a Server

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

Before You Begin

Gracefully power down the servers.

Procedure

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

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

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

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

Activating the Cisco UCS Manager Software

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope system**	Enters system mode.
Step 2	UCS-A /system # **show image**	Displays the available software images for Cisco UCS Manager (system).
Step 3	UCS-A /system # **activate firmware** *version-num*	Activates the selected firmware version on the system. **Note** Activating Cisco UCS Manager does not require rebooting the fabric interconnect; however, management services will briefly go down and all VSH shells will be terminated as part of the activation.
Step 4	UCS-A /system # **commit-buffer**	Commits the transaction. Cisco UCS Manager makes the selected version the startup version and schedules the activation to occur when the fabric interconnects are upgraded.

The following example upgrades Cisco UCS Manager and commits the transaction:

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

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

Activating the Firmware on a Fabric Interconnect

When updating the firmware on two fabric interconnects in a high availability cluster configuration, you must activate the subordinate fabric interconnect before activating the primary fabric interconnect. For more information about determining the role for each fabric interconnect, see Verifying the High Availability Status and Roles of a Cluster Configuration.

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

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

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope fabric-interconnect** {**a** | **b**}	Enters fabric interconnect mode for the specified fabric interconnect.
Step 2	UCS-A /fabric-interconnect # **show image**	Displays the available software images for the fabric interconnect.
Step 3	UCS-A /fabric-interconnect # **activate firmware** {**kernel-version** *kernel-ver-num* | **system-version** *system-ver-num*}	Activates the selected firmware version on the fabric interconnect.
Step 4	UCS-A /fabric-interconnect # **commit-buffer**	Commits the transaction. Cisco UCS Manager updates and activates the firmware, and then reboots the fabric interconnect , disrupting data traffic to and from that fabric interconnect.

The following example upgrades the fabric interconnect to version 5.2(3)N2(2.21.92) and commits the transaction:

```
UCS-A# scope fabric-interconnect a
UCS-A /fabric-interconnect # show image
Name                                          Type                  Version
--------------------------------------------- -------------------- -----------------
ucs-6100-k9-kickstart.5.2.3.N2.2.50.225.bin   Fabric Interconnect Kernel
                                                                    5.2(3)N2(2.50.225)
ucs-6100-k9-system.5.2.3.N2.2.50.225.bin      Fabric Interconnect System
                                                                    5.2(3)N2(2.50.225)

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

CHAPTER 5

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 or 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.

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

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 2	UCS-A org/ # **create fw-host-pack** *pack-name*	Creates a host firmware package with the specified package name and enters organization firmware host package mode.
Step 3	UCS-A /org/fw-host-pack # **set descr** *description*	(Optional) Provides a description for the host firmware package. **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any **show** command output.
Step 4	UCS-A org/fw-host-pack # **create pack-image** *hw-vendor-name hw-model* {**adapter** | **board-controller** | **cimc** | **graphics-card** | **host-hba** | **host-hba-optionrom** | **host-nic** | **local-disk** | **raid-controller** | **server-bios**} *version-num*	Creates a package image for the host firmware package and enters organization firmware host package image mode. The *hw-vendor-name* must match the full name of the vendor, and must begin and end with quotation marks. The *hw-vendor-name* and *hw-model* values are labels that help you easily identify the package image when you enter the **show image detail** command. The *version-num* value specifies the version number of the firmware being used for the package image. **Important** The **host-hba** and **host-hba-optionrom** options are not supported by Cisco UCS M-Series Servers. 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.

	Command or Action	Purpose
		Note Only CIMC firmware and BIOS firmware are available for pack item creation.
Step 5	UCS-A org/fw-host-pack/pack-image # **set version** *version-num*	(Optional) Specifies the package image version number. Changing this number triggers firmware updates on all components using the firmware through a service profile. Use this step only when updating a host firmware package, not when creating a package. **Note** The host firmware package can contain multiple package images. Repeat 4, and 5, to create additional package images for other components.
Step 6	UCS-A org/fw-host-pack/pack-image # **commit-buffer**	Commits the transaction. 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.

The following example creates the app1 host firmware package, creates a BIOS package image, and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # create fw-host-pack app1
UCS-A /org/fw-host-pack* # set descr "This is a host firmware package example."
UCS-A /org/fw-host-pack* # create pack-image "Cisco Systems Inc" N20-AQ0102 bios
UCSME.142M4.2.0.100.52.122920140321
UCS-A /org/fw-host-pack/pack-image* # commit-buffer
UCS-A /org/fw-host-pack/pack-image #
```

What to Do Next

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

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

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 2	UCS-A org/ # **scope fw-mgmt-pack** *pack-name*	Scope to a management firmware package with the specified package name and enters organization firmware management package mode.
Step 3	UCS-A /org/fw-mgmt-pack # **set descr** *description*	(Optional) Provides a description for the management firmware package. **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any **show** command output.
Step 4	UCS-A org/fw-mgmt-pack # **create pack-image** "*hw-vendor-name*" "*hw-model*" **cimc** "*version-num*"	Creates a package image for the management firmware package and enters organization firmware management package image mode. The *hw-vendor-name* and *hw-model* values are labels that help you easily identify the package image when you enter the **show image detail** command. The *version-num* value specifies the version number of the firmware being used for the package image. 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.
Step 5	UCS-A org/fw-mgmt-pack/pack-image # **set version** *version-num*	(Optional) Specifies the package image version number. Changing this number triggers firmware updates on all components using the firmware through a service profile. Use this step only when updating a firmware package, not when creating a package.
Step 6	UCS-A org/fw-mgmt-pack/pack-image # **commit-buffer**	Commits the transaction. 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.

The following example updates the cimc1 host firmware package, creates a CIMC package image with version 1.0(0.988) firmware, and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # scope fw-mgmt-pack cimc1
UCS-A /org/fw-mgmt-pack* # set descr "This is a management firmware package example."
```

```
UCS-A /org/fw-mgmt-pack* # create pack-image "Cisco Systems Inc" "SB-1600-CTRL" cimc
"2.3(200.166)"
UCS-A /org/fw-mgmt-pack/pack-image* # commit-buffer
UCS-A /org/fw-mgmt-pack/pack-image #
```

What to Do Next

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

CHAPTER 6

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*.

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.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope system**	Enters system command mode.
Step 2	UCS-A /system # **scope capability**	Enters capability command mode.
Step 3	UCS-A /system/capability # **update catalog** *URL*	Imports and applies the specified Capability Catalog file. Specify the URL for the operation using one of the following syntax: • **ftp:**// *username@hostname* / *path* • **scp:**// *username@hostname* / *path* • **sftp:**// *username@hostname* / *path*

	Command or Action	Purpose
		• **tftp:**// *hostname* **:** *port-num* / *path* • **usbA:**/ *path* • **usbB:**/ *path* When a username is specified, you are prompted for a password.
Step 4	UCS-A /system/capability # **show version**	(Optional) Displays the catalog update version.
Step 5	UCS-A /system/capability # **show cat-updater** [*filename*]	(Optional) Displays the update history for a Capability Catalog file, if specified, or for all Capability Catalog file update operations.

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

The following example uses SCP to import a Capability Catalog file:

```
UCS-A# scope system
UCS-A /system # scope capability
UCS-A /system/capability # update catalog
scp://user1@192.0.2.111/catalogs/ucs-catalog.2.5.0.233.T.bin
Warning: This command is deprecated and will be removed in a future release. Replaced by:
activate catalog
Password:
UCS-A /system/capability # show version
Catalog:
    Running-Vers: 2.5(0.233)T
    Package-Vers:
    Activate-Status: Ready

UCS-A /system/capability # show cat-updater ucs-catalog.2.5.0.233.T.bin

Catalog Updater:
    File Name Protocol Server          Userid          Status
    --------- -------- --------------- --------------- ------
    ucs-catalog.2.5.0.233.T.bin
              Scp      192.0.2.111     user1           Success
UCS-A /system/capability #
```

Verifying that the Capability Catalog is Current

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope system**	Enters system mode.
Step 2	UCS-A /system # **scope capability**	Enters system capability mode.

	Command or Action	Purpose
Step 3	UCS-A /system/capability # **show version**	Displays the current Capability Catalog version.
Step 4	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 55.
Step 5	If a more recent version of the Capability Catalog is available on Cisco.com, update the Capability Catalog with that version.	

The following example displays the current Capability Catalog version:

```
UCS-A# scope system
UCS-A /system # scope capability
UCS-A /system/capability # show version
Catalog:
    Running-Vers: 1.0(8.35)
    2.5(0.233)
    Activate-Status: Ready
UCS-A /system/capability #
```

Activating a M-Series Capability Catalog Update

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope system**	Enters system mode.
Step 2	UCS-A /system # **scope capability**	Enters system capability mode.
Step 3	UCS-A /system/capability # **activate firmware** *firmware-version*	Activates the specified Capability Catalog version.
Step 4	UCS-A /system/capability # **commit-buffer**	Commits the transaction to the system configuration.

The following example activates a Capability Catalog update and commits the transaction:

```
UCS-A# scope system
UCS-A /system # scope capability
UCS-A /system/capability # activate firmware 2.5(0.233)
UCS-A /system/capability* # commit-buffer
UCS-A /system/capability #
```

Restarting a Capability Catalog Update

You can restart a failed Capability Catalog file update, modifying the update parameters if necessary.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope system**	Enters system command mode.
Step 2	UCS-A /system # **scope capability**	Enters capability command mode.
Step 3	UCS-A /system/capability # **show cat-updater** [*filename*]	(Optional) Displays the update history for Capability Catalog file update operations.
Step 4	UCS-A /system/capability # **scope cat-updater** *filename*	Enters the command mode for the Capability Catalog file update operation.
Step 5	UCS-A /system/capability/cat-updater # **set userid** *username*	(Optional) Specifies the username for the remote server.
Step 6	UCS-A /system/capability/cat-updater # **set password** *password*	(Optional) Specifies the password for the remote server username. If no password is configured, you are prompted for a password when you start the update.
Step 7	UCS-A /system/capability/cat-updater # **set protocol** {**ftp** | **scp** | **sftp** | **tftp** | **usbA** | **usbB**}	(Optional) Specifies the file transfer protocol for the remote server. **Note** TFTP has a file size limitation of 32 MB. Because catalog images can be much larger than that, we recommend that you do not use TFTP for catalog image downloads.
Step 8	UCS-A /system/capability/cat-updater # **set server** {*hostname* | *ip-address*}	(Optional) Specifies the hostname or IP address of the remote server.
Step 9	UCS-A /system/capability/cat-updater # **set path** *pathname/filename*	(Optional) Specifies the path and file name of the Capability Catalog file on the remote server.
Step 10	UCS-A /system/capability/cat-updater # **restart**	Restarts the Capability Catalog file update operation.

The following example changes the server IP address and restarts the Capability Catalog file update operation:

```
UCS-A# scope system
UCS-A /system # scope capability
UCS-A /system/capability # show cat-updater ucs-catalog.1.0.0.4.binshow cat-updater
ucs-catalog.2.5.0.233.T.bin

Catalog Updater:
    File Name                Protocol Server          Userid          Status
    ---------                -------- --------------- --------------- ------
    ucs-catalog.1.0.0.4.binucs-catalog.2.5.0.233.T.bin   Scp      192.0.2.111     user1
        Applied
```

```
UCS-A /system/capability # scope cat-updater ucs-catalog.1.0.0.4.binscope cat-updater
ucs-catalog.2.5.0.233.T.bin
UCS-A /system/capability/cat-updater # set server 192.0.2.112
UCS-A /system/capability/cat-updater # restart
UCS-A /system/capability/cat-updater #
```

Viewing a Capability Catalog Provider

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope system**	Enters system command mode.
Step 2	UCS-A /system # **scope capability**	Enters capability command mode.
Step 3	UCS-A /system/capability # **show** {**chassis** | **cpu** | **disk** | **fan** | **fru** | **iom** | **memory** | **psu** | **server**} [*vendor model revision*] [**detail** | **expand**]	Displays vendor, model, and revision information for all components in the specified component category. To view manufacturing and form factor details for a specific component, specify the *vendor* , *model* , and *revision* with the **expand** keyword. If any of these fields contains spaces, you must enclose the field with quotation marks.

Note If the server contains one or more SATA devices, such as a hard disk drive or solid state drive, the **show disk** command displays ATA in the Vendor field. Use the **expand** keyword to display additional vendor information.

The following example lists the installed fans and displays detailed information from the Capability Catalog about a specific fan:

```
UCS-A# scope system
UCS-A /system # scope capability
UCS-A /system/capability # show fan

Fan Module:
    Vendor                  Model                   HW Revision
    ----------------------- ----------------------- ------------
    Cisco Systems, Inc.     N20-FAN5                0
    Cisco Systems, Inc.     N10-FAN1                0
    Cisco Systems, Inc.     N10-FAN2                0
    Cisco Systems, Inc.     N5K-C5548P-FAN          0
    Cisco Systems, Inc.     N5K-C5596P-FAN          0
    Cisco Systems, Inc.     UCS-FAN-6248UP          0
    Cisco Systems, Inc.     UCS-FAN-6296UP          0

UCS-A /system/capability # show fan "Cisco Systems, Inc." N10-FAN1 0 expand

Fan Module:
    Vendor: Cisco Systems, Inc.
    Model: N10-FAN1
    Revision: 0

    Equipment Manufacturing:
```

```
        Name: Fan Module for UCS 6140 Fabric Interconnect
        PID: N10-FAN1
        VID: NA
        Caption: Fan Module for UCS 6140 Fabric Interconnect
        Part Number: N10-FAN1
        SKU: N10-FAN1
        CLEI:
        Equipment Type:

    Form Factor:
        Depth (C): 6.700000
        Height (C): 1.600000
        Width (C): 4.900000
        Weight (C): 1.500000

UCS-A /system/capability #
```