



Cisco UCS GUI Firmware Management Guide for Cisco UCS Mini, Release 3.0

First Published: 2014-07-15

Last Modified: 2015-03-09

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2014-2015 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface

Preface ix

Audience ix

Conventions ix

Related Cisco UCS Documentation xi

Documentation Feedback xi

CHAPTER 1

Overview 1

Overview of Firmware 1

Firmware Auto Sync for FI Cluster 2

Firmware Management in Cisco UCS Central 2

Firmware Versions 3

CHAPTER 2

Cautions, Guidelines, and Limitations 5

Cautions, Guidelines, and Limitations for Managing Firmware in Cisco UCS Central 5

PART I

Managing Firmware through Cisco UCS Manager 7

CHAPTER 3

Completing the Prerequisites for Upgrading the Firmware 9

Prerequisites for Upgrading and Downgrading Firmware 9

Creating an All Configuration Backup File 10

Faults Generated Due to Reboot During the Upgrade of a Fabric Interconnect 12

 Modifying Baseline Expiration Interval for Faults 12

 Viewing Faults Generated During the Upgrade of a Fabric Interconnect 13

Verifying the Overall Status of the Fabric Interconnects 13

Verifying the High Availability Status and Roles of a Cluster Configuration 13

Verifying the Status of I/O Modules 14

Verifying the Status of Servers 14

Verifying the Status of Adapters on Servers in a Chassis	15
Obtaining Cisco UCS PowerTool and Running the Duplicate IQN Script	16

CHAPTER 4**Downloading and Managing Firmware in Cisco UCS Manager 19**

Firmware Image Management	19
Firmware Image Headers	20
Firmware Image Catalog	20
Firmware Image Management for Cisco UCS Mini	21
Obtaining Software Bundles from Cisco	21
Downloading Firmware Images to the Fabric Interconnect from a Remote Location	23
Downloading Firmware Images to the Fabric Interconnect from the Local File System	24
Canceling an Image Download	25
Determining the Contents of a Firmware Package	25
Checking the Available Space on a Fabric Interconnect	25

CHAPTER 5**Upgrading Firmware through Auto Install 27**

Firmware Upgrades through Auto Install	27
Direct Upgrade After Auto Install	28
Install Infrastructure Firmware	28
Install Server Firmware	28
Required Order of Steps for Auto Install	29
Upgrading the Infrastructure Firmware with Auto Install	29
Acknowledging the Reboot of the Primary Fabric Interconnect	31
Canceling an Infrastructure Firmware Upgrade	32
Clearing the Startup Version of the Default Infrastructure Pack	32
Upgrading the Server Firmware with Auto Install	33

CHAPTER 6**Using Firmware Automatic Synchronization Server Policy 37**

Firmware Automatic Synchronization	37
Setting the Firmware Auto-Sync Server Policy	38

CHAPTER 7**Directly Upgrading Firmware at Endpoints 39**

Direct Firmware Upgrade at Endpoints	39
Stages of a Direct Firmware Upgrade	40
Outage Impacts of Direct Firmware Upgrades	41

Updating the Firmware on Multiple Endpoints	42
Adapter Firmware	43
Updating the Firmware on an Adapter	43
Activating the Firmware on an Adapter	44
BIOS Firmware	45
Updating the BIOS Firmware on a Server	45
Activating the BIOS Firmware on a Server	46
CIMC Firmware	46
Updating the CIMC Firmware on a Server	46
Activating the CIMC Firmware on a Server	47
PSU Firmware Update	48
Updating the Firmware on a PSU	48
Activating the Firmware on a PSU	49
Board Controller Firmware	49
Activating the Board Controller Firmware on a Cisco UCS B-Series M2 Blade Server	51
Activating the Board Controller Firmware on Cisco UCS B-Series M3 and M4 Blade Servers	51
Activating the Board Controller Firmware on Cisco UCS C-Series M3 and M4 Rack Servers	53
Cisco UCS Manager Firmware	54
Activating the Cisco UCS Manager Software	55
Fabric Interconnect Firmware	55
Activating the Firmware on a Subordinate Fabric Interconnect	55
Activating the Firmware on a Primary Fabric Interconnect	56
Activating the Firmware on a Standalone Fabric Interconnect	57
Verifying Firmware Versions on Components	58

CHAPTER 8
Upgrading Firmware through Firmware Packages in Service Profiles 59

Firmware Upgrades through Firmware Packages in Service Profiles	59
Host Firmware Package	60
Management Firmware Package	61
Stages of a Firmware Upgrade through Firmware Packages in Service Profiles	62
Effect of Updates to Firmware Packages in Service Profiles	62
Creating a Host Firmware Package	65
Updating a Host Firmware Package	66

Updating a Management Firmware Package	67
Adding Firmware Packages to an Existing Service Profile	68

CHAPTER 9**Managing the Capability Catalog in Cisco UCS Manager 69**

Capability Catalog	69
Contents of the Capability Catalog	69
Updates to the Capability Catalog	70
Activating a Capability Catalog Update	71
Verifying that the Capability Catalog Is Current	71
Viewing a Capability Catalog Provider	72
Downloading Individual Capability Catalog Updates	72
Obtaining Capability Catalog Updates from Cisco	72
Updating the Capability Catalog from a Remote Location	73
Updating the Capability Catalog from the Local File System	73

CHAPTER 10**Updating Management Extensions 75**

Management Extensions	75
Activating a Management Extension	75

CHAPTER 11**Verifying that the Data Path is Ready 77**

Verifying that Dynamic vNICs Are Up and Running	77
Verifying the Ethernet Data Path	78
Verifying the Data Path for Fibre Channel Switch Mode	78

PART II**Managing Firmware through Cisco UCS Central 81****CHAPTER 12****Downloading and Managing Firmware in Cisco UCS Central 83**

Downloading Firmware from Cisco.com	83
Firmware Library of Images	84
Configuring Firmware Download from Cisco	84
Downloading a Firmware Image from Cisco	85
Downloading Firmware from a Remote Location	85
Downloading Firmware from a Local File System	86
Viewing Image Download Faults	86
Viewing Firmware Images in the Library	87

Deleting Image Metadata from the Library of Images 87

CHAPTER 13**Upgrading Firmware in Cisco UCS Domains through Cisco UCS Central 89**

Firmware Upgrades for Cisco UCS Domains 89

Configuring an Infrastructure Firmware Upgrade for a Cisco UCS Domain 89

Acknowledging a Pending Activity 90

Deleting an Infrastructure Firmware Package 91

Creating a Host Firmware Package 91

Deploying a Host Firmware Upgrade 92

Deleting a Host Firmware Package 93

Scheduling Firmware Upgrades 93

 Firmware Upgrade Schedules 93

 Creating a Maintenance Policy 93

 Creating a One Time Occurrence Schedule 94

 Creating a Recurring Occurrence Schedule 95

 Deleting a Firmware Upgrade Schedule 95

CHAPTER 14**Managing the Capability Catalog in Cisco UCS Central 97**

Capability Catalog 97

 Contents of the Capability Catalog 97

 Updates to the Capability Catalog 98

Configuring a Capability Catalog Update for a Cisco UCS Domain 98



Preface

- [Audience, page ix](#)
- [Conventions, page ix](#)
- [Related Cisco UCS Documentation, page xi](#)
- [Documentation Feedback, page xi](#)

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 <i>this font</i> .
TUI elements	In a Text-based User Interface, text the system displays appears in <code>this font</code> .
System output	Terminal sessions and information that the system displays appear in <code>this font</code> .

Text Type	Indication
CLI commands	CLI command keywords appear in this font . Variables in a CLI command appear in <i>this font</i> .
[]	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.

**Timesaver**

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

**Caution**

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

**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 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.



Overview

This chapter includes the following sections:

- [Overview of Firmware, page 1](#)
- [Firmware Auto Sync for FI Cluster, page 2](#)
- [Firmware Management in Cisco UCS Central , page 2](#)
- [Firmware Versions, page 3](#)

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. The upgrade order for the endpoints in a Cisco UCS domain depends upon the upgrade path, but includes the following:

- Cisco UCS Manager
- Fabric interconnects
- Endpoints physically located on adapters, including NIC and HBA firmware, and Option ROM (where applicable) that can be upgraded through firmware packages included in a service profile
- Endpoints physically located on servers, such as the BIOS, storage controller (RAID controller), and Cisco Integrated Management Controller (CIMC) that can be upgraded through firmware packages included in a service profile

See the required order of steps for your upgrade path to determine the appropriate order in which to upgrade the endpoints in your Cisco UCS domain.

Cisco maintains a set of best practices for managing firmware images and updates in this document and in the following technical note: [Unified Computing System Firmware Management Best Practices](#).

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.

Firmware Auto Sync for FI Cluster

Addition of a secondary Fabric Interconnect to form a cluster – either as a replacement or a conversion from standby to HA requires the infrastructure bundle firmware versions to match. Administrators today manually upgrade/downgrade the replacement FI to the correct version before they connect it to the cluster. Firmware Auto Sync allows the users to automatically upgrade/downgrade the infrastructure bundle to the same version as the survivor FI when the replacement is added as standby to HA. The software package is the UCS software/firmware that resides on the FI.

Software and Hardware Requirements

The software package on the survivor FI should be greater than or equal to Cisco UCS Release 1.4. The model numbers of the Fabric Interconnects should be same. For example, firmware Auto Sync will not trigger for a combination of 61XX and 62XX FI models that are being setup for HA.

Implementation

With the earlier implementation, the user would compulsorily configure the replacement FI as standalone mode if there was a mismatch in the version of software packages. The replacement FI is manually upgraded/downgraded to the same version of software package on survivor FI through the usual upgrade/downgrade process. Then the replacement FI is added to the cluster since the upgrade/downgrade of the replacement FI is a manual process.

The user is now given an additional option of synchronization of the software packages of the replacement FI with the survivor FI along with the current option. If the user decides to Auto Sync the firmware, the software packages of the survivor FI are copied to the replacement FI. The software packages on the replacement FI are then activated and the FI is added to the cluster. The sync-up of the Cisco UCSM database and the configuration happens via the usual mechanisms once the HA cluster is formed successfully.

Firmware Auto Sync Benefits

In a UCS cluster where one Fabric Interconnect has failed, the Auto Sync feature ensures that the software package of the replacement FI is brought up to the same revision of the survivor. The whole process requires minimal end user interaction while providing clear and concise feedback during the procedure.

Firmware Management in Cisco UCS Central

Cisco UCS Central enables you to manage all firmware components for all registered Cisco UCS domains.

**Note**

To manage Cisco UCS domains firmware from Cisco UCS Central, you must enable the global firmware management option in Cisco UCS Manager. You can enable the global firmware management option when you register Cisco UCS Manager with Cisco UCS Central. You can also turn global management option on or off based on your management requirements.

The Cisco UCS domains are categorized into domain groups in Cisco UCS Central for management purposes. You can manage firmware for each domain group separately at the domain group level or for all domain groups from the domain group root. Cisco UCS Central provides you the option to manage the following Cisco UCS domain firmware packages:

- **Capability Catalog**— One capability catalog per domain group . All Cisco UCS domains registered to a particular domain group will use the capability catalog defined in the domain group.
- **Infrastructure Firmware**— One infrastructure firmware policy per domain group . All Cisco UCS domains registered to a particular domain group will use the same Infrastructure firmware version defined in the domain group.
- **Host Firmware**— You can have more than one host firmware policy for the different host firmware components in a domain group. The Cisco UCS domains registered in the domain group will be able to choose any defined host firmware policy in the group. Cisco UCS Central provides you the option to upgrade the host firmware globally to all Cisco UCS domains in a domain group at the same time.

**Note**

For more information on managing firmware in Cisco UCS Central, see the Firmware Management chapters in the *Cisco UCS Central User Manual* and *Cisco UCS Central CLI Reference Manual*.

Firmware Versions

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

Firmware Versions in CIMC, and Adapters

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

The following firmware version terminology is used in 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.

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.



CHAPTER 2

Cautions, Guidelines, and Limitations

This chapter includes the following sections:

- [Cautions, Guidelines, and Limitations for Managing Firmware in Cisco UCS Central, page 5](#)

Cautions, Guidelines, and Limitations for Managing Firmware in Cisco UCS Central

Before you start managing Cisco UCS Manager firmware from Cisco UCS Central, consider the following cautions, guidelines and limitations:

- The firmware policies you define for a domain group will be applied to any new Cisco UCS Domain added to this domain group. If a firmware policy is not defined in the domain group, Cisco UCS Domain will inherit the policy from the parent domain group.
- The global policies will remain global in Cisco UCS Manager even when Cisco UCS Manager loses connection with Cisco UCS Central. If you want to apply any changes to any of the policies that are global in Cisco UCS Manager, you must change the ownership to local from global.
- When you create a host firmware package from Cisco UCS Central, it must be associated to a service profile to deploy updates in Cisco UCS domains.
- When you modify a host firmware package in Cisco UCS Central, the changes are applied to Cisco UCS domains during the next maintenance schedule associate with the host firmware update.
- The host firmware maintenance policies you define in Cisco UCS Central apply to the org-root in Cisco UCS domains. You cannot define separate host maintenance policies for sub organizations in a Cisco UCS Domain from Cisco UCS Central.
- Any server with no service profile association will get upgraded to the default version of the host firmware pack. Since these servers do not have a maintenance policy, they will reboot immediately.
- If you specify a maintenance policy in Cisco UCS Central and enable user acknowledgment and do not specify a schedule, you can acknowledge the pending task only from Cisco UCS Manager. To acknowledge pending activities from Cisco UCS Central, you must schedule maintenance using global schedulers and enable user acknowledgment.

- When you schedule a maintenance policy in Cisco UCS Central and enable user acknowledgment, that task will be displayed on the pending activities tab at the time specified in the schedule.
- You can view the pending activity for a maintenance policy only from the domain group section.
- Make sure to enable user acknowledgment for any firmware schedule to avoid any unexpected reboot in the Cisco UCS domains.



PART **I**

Managing Firmware through Cisco UCS Manager

- [Completing the Prerequisites for Upgrading the Firmware, page 9](#)
- [Downloading and Managing Firmware in Cisco UCS Manager, page 19](#)
- [Upgrading Firmware through Auto Install, page 27](#)
- [Using Firmware Automatic Synchronization Server Policy, page 37](#)
- [Directly Upgrading Firmware at Endpoints, page 39](#)
- [Upgrading Firmware through Firmware Packages in Service Profiles, page 59](#)
- [Managing the Capability Catalog in Cisco UCS Manager, page 69](#)
- [Updating Management Extensions, page 75](#)
- [Verifying that the Data Path is Ready, page 77](#)



Completing the Prerequisites for Upgrading the Firmware

This chapter includes the following sections:

- [Prerequisites for Upgrading and Downgrading Firmware, page 9](#)
- [Creating an All Configuration Backup File, page 10](#)
- [Faults Generated Due to Reboot During the Upgrade of a Fabric Interconnect, page 12](#)
- [Verifying the Overall Status of the Fabric Interconnects, page 13](#)
- [Verifying the High Availability Status and Roles of a Cluster Configuration, page 13](#)
- [Verifying the Status of I/O Modules, page 14](#)
- [Verifying the Status of Servers, page 14](#)
- [Verifying the Status of Adapters on Servers in a Chassis, page 15](#)
- [Obtaining Cisco UCS PowerTool and Running the Duplicate IQN Script, page 16](#)

Prerequisites for Upgrading and Downgrading Firmware

All endpoints in a Cisco UCS domain must be fully functional and all processes must be complete before you begin a firmware upgrade or downgrade on those endpoints. You cannot upgrade or downgrade an endpoint that is not in a functional state. For example, the firmware on a server that has not been discovered cannot be upgraded or downgraded. An incomplete process, such as an FSM that has failed after the maximum number of retries, can cause the upgrade or downgrade on an endpoint to fail. If an FSM is in progress, Cisco UCS Manager queues up the update and activation and runs them when the FSM has completed successfully.

Colored boxes around components on the **Equipment** tab may indicate that an endpoint on that component cannot be upgraded or downgraded. Verify the status of that component before you attempt to upgrade the endpoints.



Note

The **Installed Firmware** tab in Cisco UCS Manager GUI does not provide sufficient information to complete these prerequisites.

Before you upgrade or downgrade firmware in a Cisco UCS domain, complete the following prerequisites:

- Review the Release Notes.
- Review the relevant [Hardware and Software Interoperability Matrix](#) to ensure the operating systems on all servers have the right driver levels for the release of Cisco UCS to which you plan to upgrade.
- Back up the configuration into an All Configuration backup file.
- 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.
- Verify that the data path is up and running. For more information, see the Verifying that the Data Path is Ready section in the appropriate [Firmware Management Guide](#).
- Verify that all servers, I/O modules, and adapters are fully functional. An inoperable server cannot be upgraded.
- Verify that the Cisco UCS domain does not include any critical or major faults. If such faults exist, you must resolve them before you upgrade the system. A critical or major fault may cause the upgrade to fail.
- Verify that all servers have been discovered. They do not need to be powered on or associated with a service profile.
- If you want to integrate a rack-mount server into the Cisco UCS domain, follow the instructions in the appropriate [C-Series Rack-Mount Server Integration Guide](#) for installing and integrating a rack-mount server in a system managed by Cisco UCS Manager.

Creating an All Configuration Backup File

This procedure assumes that you do not have an existing backup operation for an All Configuration backup file.

Before You Begin

Obtain the backup server IPv4 or IPv6 address and authentication credentials.

Procedure

-
- Step 1** In the **Navigation** pane, click **Admin**.
 - Step 2** Click the **All** node.
 - Step 3** In the **Work** pane, click the **General** tab.
 - Step 4** In the **Actions** area, click **Backup Configuration**.
 - Step 5** In the **Backup Configuration** dialog box, click **Create Backup Operation**.
 - Step 6** In the **Create Backup Operation** dialog box, do the following:
 - a) Complete the following fields:
 - **Admin State** field—Click the **Enabled** radio button to run the backup operation as soon as you click OK.

- **Type** field—Click the **All Configuration** radio button to create an XML backup file that includes all system and logical configuration information.
- **Preserve Identities** check box—If the Cisco UCS domain includes any identities derived from pools that you need to preserve, check this check box.

If this checkbox is selected for **Logical Configuration** type of backup operation, the backup file preserves all identities derived from pools, including vHBAs, WWPNs, WWNN, vNICs, MACs and UUIDs.

Note If this check box is not selected the identities will be reassigned and user labels will be lost after a restore.

- **Protocol** field—Click the one of the following radio buttons to indicate the protocol you want to use to transfer the file to the backup server:
 - **FTP**
 - **TFTP**
 - **SCP**
 - **SFTP**
 - **USB A**—The USB drive inserted into fabric interconnect A.
This option is only available for certain system configurations.
 - **USB B**—The USB drive inserted into fabric interconnect B.
This option is only available for certain system configurations.
- **Hostname** field—Enter the IP address or hostname of the location where the backup file is to be stored. This can be a server, storage array, local drive, or any read/write media that the fabric interconnect can access through the network. If you use a hostname, you must configure Cisco UCS Manager to use a DNS server.
- **Filename** field—Enter the full path to the backup configuration file. This field can contain the filename as well as the path. If you omit the filename, the backup procedure assigns a name to the file.
- **User** field—Enter the username that Cisco UCS Manager should use to log in to the backup location. You do not need to complete this field if you selected TFTP for the protocol.
- **Password** field—Enter the password associated with the username. You do not need to complete this field if you selected TFTP for the protocol.

b) Click **OK**.

Step 7 If Cisco UCS Manager displays a confirmation dialog box, click **OK**.
If you set the **Admin State** field to enabled, Cisco UCS Manager takes a snapshot of the configuration type that you selected and exports the file to the network location. The backup operation displays in the **Backup Operations** table in the **Backup Configuration** dialog box.

Step 8 (Optional) To view the progress of the backup operation, do the following:

- If the operation does not display in the **Properties** area, click the operation in the **Backup Operations** table.
- In the **Properties** area, click the down arrows on the **FSM Details** bar.

The **FSM Details** area expands and displays the operation status.

- Step 9** Click **OK** to close the **Backup Configuration** dialog box.
The backup operation continues to run until it is completed. To view the progress, re-open the **Backup Configuration** dialog box.
-

Faults Generated Due to Reboot During the Upgrade of a Fabric Interconnect

During firmware upgrade, to ensure proper functioning of all services on the fabric interconnect, it is essential to ensure that port configurations and services that go down when the fabric interconnect reboots are re-established after the fabric interconnect comes back up.

Cisco UCS Manager displays any service that is not re-established after the last reboot of a fabric interconnect. Cisco UCS Manager creates a baseline of the outstanding faults before a fabric interconnect is to be rebooted. After the fabric interconnect reboots and comes up, you can view the new faults generated since the last baseline to identify the services that went down because of the fabric reboot.

When a specific interval of time has passed after Cisco UCS Manager created a baseline of the outstanding faults, baselining is cleared and all faults show up as new faults. This interval is called baseline expiration interval. [Modifying Baseline Expiration Interval for Faults](#), on page 12 provides detailed information about modifying a baseline expiration interval in Cisco UCS Manager.

Cisco recommends that you resolve service-impacting faults before you continue with the fabric interconnect reboot or evacuation.

Modifying Baseline Expiration Interval for Faults

You can modify a baseline expiration interval in Cisco UCS Manager.

Procedure

- Step 1** In the **Navigation** pane, click **Admin**.
- Step 2** Expand **All > Faults, Events, and Audit Log**.
- Step 3** In the **Work** pane, click the **Settings** tab, and then click the **Global Fault Policy** subtab.
- Step 4** In the **Baseline Expiration Interval** area, update the **dd:hh:mm:ss** field.
The **dd:hh:mm:ss** field specifies the number of days, hours, minutes, and seconds that should pass before Cisco UCS Manager clears the fault baseline.
The default baseline expiration interval is 24 hours.
- Step 5** Click **Save Changes**.
-

Viewing Faults Generated During the Upgrade of a Fabric Interconnect

Procedure

- Step 1** In the **Navigation** pane, click **Admin**.
 - Step 2** Expand **All > Faults, Events, and Audit Log**.
 - Step 3** In the **Work** pane, click the **New Faults** radio button.
All faults generated after creating the baseline are displayed.
-

Verifying the Overall Status of the Fabric Interconnects

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
 - Step 2** Expand **Equipment > Fabric Interconnects**.
 - Step 3** Click the node for the fabric interconnect that you want to verify.
 - Step 4** In the **Work** pane, click the **General** tab.
 - Step 5** In the **Status** area, verify that the **Overall Status** is **operable**.
If the status is not **operable**, create and download a Tech Support file, and contact Cisco Technical Support. Do not proceed with the firmware upgrade. For more information about Tech Support files, see the *Cisco UCS Manager B-Series Troubleshooting Guide*.
-

Verifying the High Availability Status and Roles of a Cluster Configuration

The high availability status is the same for both fabric interconnects in a cluster configuration.

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
- Step 2** Expand **Equipment > Fabric Interconnects**.
- Step 3** Click the node for one of the fabric interconnects in the cluster.
- Step 4** In the **Work** pane, click the **General** tab.
- Step 5** If the fields in the **High Availability Details** area are not displayed, click the **Expand** icon to the right of the heading.
- Step 6** Verify that the following fields display the following values:

Field Name	Required Value
Ready field	Yes
State field	Up

If the values are different, create and download a Tech Support file, and contact Cisco Technical Support. Do not proceed with the firmware upgrade. For more information about Tech Support files, see the *Cisco UCS Manager B-Series Troubleshooting Guide*.

- Step 7** Note the value in the **Leadership** field to determine whether the fabric interconnect is the primary or subordinate.
You need to know this information to upgrade the firmware on the fabric interconnects.

Verifying the Status of I/O Modules

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
Step 2 Expand **Equipment > Chassis**.
Step 3 Click on the chassis for which you want to verify the status of the I/O modules.
Step 4 In the **Work** pane, click the **IO Modules** tab.
Step 5 For each I/O module, verify that the following columns display the following values:

Field Name	Desired Value
Overall Status column	ok
Operability column	operable

If the values are different, create and download a Tech Support file, and contact Cisco Technical Support. Do not proceed with the firmware upgrade. For more information about Tech Support files, see the *Cisco UCS Manager B-Series Troubleshooting Guide*.

- Step 6** Repeat Steps 3 through 5 to verify the status of the I/O modules in each chassis.

Verifying the Status of Servers

If a server is inoperable, you can proceed with the upgrade for other servers in the Cisco UCS domain. However, you cannot upgrade the inoperable server.

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
- Step 2** On the **Equipment** tab, click **Equipment**.
- Step 3** In the **Work** pane, click the **Servers** tab to display a list of all servers in all chassis.
- Step 4** For each server, verify that the following columns display the following values:

Field Name	Desired Value
Overall Status column	<p>ok, unassociated, or any value that does not indicate a failure.</p> <p>If the value indicates a failure, such as discovery-failed, the endpoints on that server cannot be upgraded.</p>
Operability column	operable

- Step 5** If you need to verify that a server has been discovered, do the following:
- Right-click the server for which you want to verify the discovery status and choose **Show Navigator**.
 - In the **Status Details** area of the **General** tab, verify that the **Discovery State** field displays a value of **complete**.
If the fields in the **Status Details** area are not displayed, click the **Expand** icon to the right of the heading.

Verifying the Status of Adapters on Servers in a Chassis

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
- Step 2** Expand **Equipment** > **Chassis** > *Chassis Number* > **Servers**.
- Step 3** Click the server for which you want to verify the status of the adapters.
- Step 4** In the **Work** pane, click the **Inventory** tab.
- Step 5** In the **Inventory** tab, click the **Adapters** subtab.
- Step 6** For each adapter, verify that the following columns display the following values:

Field Name	Desired Value
Overall Status column	ok
Operability column	operable

If the fields show a different value and the adapter is inoperable, you can proceed with the upgrade for other adapters on the servers in the Cisco UCS domain. However, you cannot upgrade the inoperable adapter.

Obtaining Cisco UCS PowerTool and Running the Duplicate IQN Script

You can use a script that runs in the Cisco UCS PowerTool to determine whether a Cisco UCS configuration for iSCSI boot includes duplicate IQNs.

Procedure

- Step 1** To download Cisco UCS PowerTool, do the following:
- In your web browser, navigate to the following website: <http://developer.cisco.com/web/unifiedcomputing/microsoft>
 - Scroll down to the **Cisco UCS PowerTool (PowerShell Toolkit) Beta Download** area.
 - Download the `CiscoUcs-PowerTool-0.9.6.0.zip` file.
 - Unzip the file and follow the prompts to install Cisco UCS PowerTool.
You can install Cisco UCS PowerTool on any Windows computer. You do not need to install it on a computer used to access Cisco UCS Manager.
- Step 2** To launch Cisco UCS PowerTool, enter the following at a command line:
C:\Program Files (x86)\Cisco\Cisco UCS PowerTool>C:\Windows\System32\windowspowershell\v1.0\powershell.exe -NoExit -ExecutionPolicy RemoteSigned -File .\StartUcsPS.ps1

Example:

The following example shows what happens when you launch Cisco UCS PowerTool:

```
C:\Program Files (x86)\Cisco\Cisco UCS PowerTool>C:\Windows\System32\windowspowershell\v1.0\powershell.exe -NoExit -ExecutionPolicy RemoteSigned -File .\StartUcsPS.ps1
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.
```

- Step 3** In Cisco UCS PowerTool, do the following:
- Connect to Cisco UCS Manager, as follows:
PS C:\> **Connect-Ucs IP_address**
 - Enter your username and password when prompted for your credential as shown in the following example:
cmdlet Connect-Ucs at command pipeline position 1
Supply values for the following parameters:
Credential
Cisco UCS PowerTool outputs the following to your screen after you log in.

```
Cookie           : 1331303969/2af0afde-6627-415c-b85f-a7cae6233de3
Domains          :
LastUpdateTime   : 3/9/2012 6:20:42 AM
Name             : 209.165.201.15
NoSsl            : False
NumPendingConfigs : 0
```

```

NumWatchers      : 0
Port              : 443
Priv              : {admin, read-only}
RefreshPeriod    : 600
SessionId        : web_49846_A
TransactionInProgress : False
Ucs               : ucs-4
Uri              : https://209.165.201.15
UserName         : admin
VirtualIpv4Address : 209.165.201.15
Version          : 3.0(1a)
WatchThreadStatus : None

```

- Step 4** In the Cisco UCS PowerTool, run the following script to validate your iSCSI boot configuration and check for duplicate IQNs :

```

PS C:\> Get-UcsServiceProfile -type instance | Get-UcsVnicIscsi | ? { $_.InitiatorName -ne "" } | select
Dn,InitiatorName | group InitiatorName | ? { $_.Count -gt 1 } | % { $obj = New-Object PSObject ; $obj
| Add-Member Noteproperty Count $_.Count; $obj | Add-Member Noteproperty InitiatorName $_.Name;
$obj | Add-Member Noteproperty Dn ($_ | select -exp Group | % { $_.Dn } ); $obj }

```

Cisco UCS PowerTool outputs the results to your screen, as follows:

```

Count InitiatorName          Dn
-----
2 iqn.2012-01.cisco.com:s... {org-root/ls-SP_1_6/is...
2 iqn.2012-01.cisco.com:s... {org-root/ls-SP_2_1/is...
2 iqn.2012-01.cisco.com:s... {org-root/ls-SP_2_41/i...
4 iqn.2012-01.cisco.com:s... {org-root/ls-SP_2_7/is...
2 iqn.2012-01.cisco.com:s... {org-root/org-sub1/ls-...
2 iqn.2012-01.cisco.com:s... {org-root/org-sub2/ls-...

```

- Step 5** (Optional) If you have .NET Framework 3.5 Service Pack 1 installed, you can use the following script to view the output in the GUI:

```

PS C:\> Get-UcsServiceProfile -type instance | Get-UcsVnicIscsi | ? { $_.InitiatorName -ne "" } | select
Dn,InitiatorName | group InitiatorName | ? { $_.Count -gt 1 } | % { $obj = New-Object PSObject ; $obj
| Add-Member Noteproperty Count $_.Count; $obj | Add-Member Noteproperty InitiatorName $_.Name;
$obj | Add-Member Noteproperty Dn ($_ | select -exp Group | % { $_.Dn } ); $obj } | ogv

```

- Step 6** Disconnect from Cisco UCS Manager, as follows:

```

PS C:\> Disconnect-Ucs

```

What to Do Next

If you do not ensure that all iSCSI vNICs are unique across all service profiles in a Cisco UCS domain before you upgrade, Cisco UCS Manager raises a fault on the iSCSI vNICs to warn you that duplicate IQNs are present. Also, if you do not ensure that there are no duplicate IQN names within a service profile (for example, the same name used for both iSCSI vNICs), Cisco UCS reconfigures the service profile to have a single IQN. For information on how to clear this fault and reconfigure the duplicate IQNs, see the [Cisco UCS B-Series Troubleshooting Guide](#).



CHAPTER 4

Downloading and Managing Firmware in Cisco UCS Manager

This chapter includes the following sections:

- [Firmware Image Management, page 19](#)
- [Firmware Image Management for Cisco UCS Mini, page 21](#)
- [Obtaining Software Bundles from Cisco, page 21](#)
- [Downloading Firmware Images to the Fabric Interconnect from a Remote Location, page 23](#)
- [Downloading Firmware Images to the Fabric Interconnect from the Local File System, page 24](#)
- [Canceling an Image Download, page 25](#)
- [Determining the Contents of a Firmware Package, page 25](#)
- [Checking the Available Space on a Fabric Interconnect, page 25](#)

Firmware Image Management

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

Cisco UCS Infrastructure Software Bundle

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

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



Note Cisco UCS Infrastructure Bundle cannot be activated on Cisco UCS Mini and vice versa.

Cisco UCS B-Series Blade Server Software Bundle

This bundle includes the following firmware images that are required to update the firmware for the blade servers in a Cisco UCS domain. In addition to the bundles created for a release, these bundles can also be released between infrastructure bundles to enable Cisco UCS Manager to support a blade server that is not included in the most recent infrastructure bundle.

- CIMC firmware
- BIOS firmware
- Adapter firmware
- Board controller firmware
- Third-party firmware images required by the new server

Cisco UCS C-Series Rack-Mount UCS-Managed Server Software Bundle

This bundle includes the following firmware images that are required to update components on rack-mount servers that have been integrated with and are managed by Cisco UCS Manager:

- CIMC firmware
- BIOS firmware
- Adapter firmware
- Storage controller firmware



Note You cannot use this bundle for standalone C-series servers. The firmware management system in those servers cannot interpret the header required by Cisco UCS Manager. For information on how to upgrade standalone C-series servers, see the C-series configuration guides.

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

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 Image Management for Cisco UCS Mini

Cisco UCS Minisupports 3 image bundles. The infrastructure bundle for Cisco UCS Mini contains UCS 6324 images for kickstart, system, and UCS Manager. The UCS 6324 images work only on Cisco UCS Mini platform. The blades and rack bundles are identical to the classic UCS bundle. The Cisco UCS Mini catalog works on the classic Cisco UCS.



Note

The Cisco UCS infrastructure bundle can be downloaded on Cisco UCS Mini but it cannot be activated. The classic UCS kickstart, system, and UCS Manager cannot be activated on Cisco UCS Mini. No classic UCS infrastructure bundle is released for Release 3.0.

Obtaining Software Bundles from Cisco

Before You Begin

Determine which of the following software bundles you need to update the Cisco UCS domain:

- Cisco UCS Infrastructure Software Bundle—Required for all Cisco UCS domains.
- Cisco UCS B-Series Blade Server Software Bundle—Required for all Cisco UCS domains that include blade servers.

- Cisco UCS C-Series Rack-Mount UCS-Managed Server Software Bundle—Only required for Cisco UCS domains that include integrated rack-mount servers. This bundle contains firmware to enable Cisco UCS Manager to manage those servers and is not applicable to standalone C-Series rack-mount servers.

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 Infrastructure Software Bundle	Click Cisco UCS Infrastructure and UCS Manager Software > Unified Computing System (UCS) Infrastructure Software Bundle .
Cisco UCS B-Series Blade Server Software Bundle	Click Cisco UCS B-Series Blade Server Software > Unified Computing System (UCS) Server Software Bundle .
Cisco UCS C-Series Rack-Mount UCS-Managed Server Software Bundle	Click Cisco UCS C-Series Rack-Mount UCS-Managed 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:
- Click the link for the latest software bundle for the release you want to download. 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.
 - 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.
 - Follow the prompts to complete your download of the software bundle(s).
- Step 8** Read the Release Notes before upgrading your Cisco UCS domain.

What to Do Next

Download the software bundles to the fabric interconnect.

Downloading Firmware Images to the Fabric Interconnect from a Remote Location



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

Before You Begin

Obtain the required firmware bundles from Cisco.

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
- Step 2** Click the **Equipment** node.
- Step 3** In the **Work** pane, click the **Firmware Management** tab.
- Step 4** Click the **Installed Firmware** tab.
- Step 5** Click **Download Firmware**.
- Step 6** In the **Download Firmware** dialog box, click the **Remote File System** radio button in the **Location of the Image File** field and fill in the required fields.
- Step 7** Click **OK**.
Cisco UCS Manager GUI begins downloading the firmware bundle to the fabric interconnect.
- Step 8** (Optional) Monitor the status of the download on the **Download Tasks** tab.
 - Note** If Cisco UCS Manager reports that the bootflash is out of space, delete obsolete bundles on the **Packages** tab to free up space. To view the available space in bootflash, navigate to the fabric interconnect, click **Equipment**, and expand the **Local Storage Information** area on the **General** tab.
- Step 9** Repeat this task until all the required firmware bundles have been downloaded to the fabric interconnect.

What to Do Next

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

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



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

Before You Begin

Obtain the required firmware bundles from Cisco.

Procedure

-
- Step 1** In the **Navigation** pane, click **Equipment**.
 - Step 2** Click the **Equipment** node.
 - Step 3** In the **Work** pane, click the **Firmware Management** tab.
 - Step 4** Click the **Installed Firmware** tab.
 - Step 5** Click **Download Firmware**.
 - Step 6** In the **Download Firmware** dialog box, click the **Local File System** radio button in the **Location of the Image File** field.
 - Step 7** In the **Filename** field, type the full path and name of the image file.
If you do not know the exact path to the folder where the firmware image file is located, click **Browse** and navigate to the file.
Note For the HTML5 GUI, click **Choose File** to locate the firmware image file.
 - Step 8** Click **OK**.
Cisco UCS Manager GUI begins downloading the firmware bundle to the fabric interconnect.
 - Step 9** (Optional) Monitor the status of the firmware bundle download on the **Download Tasks** tab.
Note If Cisco UCS Manager reports that the bootflash is out of space, delete obsolete bundles on the **Packages** tab to free up space. To view the available space in bootflash, navigate to the fabric interconnect on the **Equipment** tab and expand the **Local Storage Information** area on the **General** tab.
 - Step 10** Repeat this task until all the required firmware bundles have been downloaded to the fabric interconnect.

What to Do Next

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

Canceling an Image Download

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

Procedure

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

Determining the Contents of a Firmware Package

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
 - Step 2** Click the **Equipment** node.
 - Step 3** In the **Work** pane, click the **Firmware Management** tab.
 - Step 4** On the **Packages** subtab, click the + icon next to a package to view its contents.
 - Step 5** To take a snapshot of the package contents, do the following:
 - a) Highlight the rows that include the image name and its contents.
 - b) Right-click and choose **Copy**.
 - c) Paste the contents of your clipboard into a text file or other document.
-

Checking the Available Space on a Fabric Interconnect

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

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
 - Step 2** Expand **Equipment > Fabric Interconnects**.
 - Step 3** Click the fabric interconnect on which you want to check the available space.
 - Step 4** In the **Work** pane, click the **General** tab.
 - Step 5** Expand the **Local Storage Information** area.
When you download a firmware image bundle, a fabric interconnect needs at least twice as much available space as the size of the firmware image bundle. If the bootflash does not have sufficient space, delete the obsolete firmware, core files, and other unneeded objects from the fabric interconnect.
-



CHAPTER 5

Upgrading Firmware through Auto Install

This chapter includes the following sections:

- [Firmware Upgrades through Auto Install, page 27](#)
- [Required Order of Steps for Auto Install, page 29](#)
- [Upgrading the Infrastructure Firmware with Auto Install, page 29](#)
- [Acknowledging the Reboot of the Primary Fabric Interconnect, page 31](#)
- [Canceling an Infrastructure Firmware Upgrade, page 32](#)
- [Clearing the Startup Version of the Default Infrastructure Pack, page 32](#)
- [Upgrading the Server Firmware with Auto Install, page 33](#)

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, the I/O modules, and Cisco UCS Manager.
- **Install Server Firmware**—Uses the Cisco UCS B-Series Blade Server Software Bundle to upgrade all blade servers in the Cisco UCS domain and/or the Cisco UCS C-Series Rack-Mount UCS-Managed Server Software Bundle to upgrade all rack servers.

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.

**Note**

You cannot use Auto Install to upgrade either the infrastructure or the servers in a Cisco UCS domain if Cisco UCS Manager in that domain is at a release prior to Cisco UCS 2.1(1). However, after you upgrade Cisco UCS Manager to Release 2.1(1) or greater, you can use Auto Install to upgrade the remaining components in a Cisco UCS domain that is at the minimum required firmware level. For more information, see *Cautions, Guidelines, and Limitations for Upgrading with Auto Install* and the appropriate [Cisco UCS upgrade guide](#).

Direct Upgrade After Auto Install

During Auto Install, the startup version of the default infrastructure pack is configured. To successfully complete a direct upgrade or activation of Cisco UCS Manager, Fabric Interconnects, and IOMs after Auto Install, ensure that the startup version is cleared before starting direct upgrade or activation. If the startup version of the default infrastructure pack is configured, you cannot directly upgrade or activate Cisco UCS Manager, Fabric Interconnects, and IOMs. [Clearing the Startup Version of the Default Infrastructure Pack, on page 32](#) provides detailed steps for clearing the startup version.

Install Infrastructure Firmware

Install Infrastructure Firmware upgrades all infrastructure components in a Cisco UCS domain, including Cisco UCS Manager, and all fabric interconnects and I/O modules. 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.

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 B-Series Blade Server Software Bundle for all blade servers in the chassis.
- Cisco UCS C-Series Rack-Mount UCS-Managed Server Software Bundle for all rack-mount servers that are integrated into the Cisco UCS domain.

**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, the timing of the actual reboot of servers occurs depends upon the maintenance policy in the service profile associated with the server.

Required Order of Steps for Auto Install

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

- 1 Install Infrastructure Firmware
- 2 Install Server Firmware

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

Upgrading the Infrastructure Firmware with Auto Install

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

**Note**

You cannot use Auto Install to upgrade either the infrastructure or the servers in a Cisco UCS domain if Cisco UCS Manager in that domain is at a release prior to Cisco UCS 2.1(1). However, after you upgrade Cisco UCS Manager to Release 2.1(1) or greater, you can use Auto Install to upgrade the remaining components in a Cisco UCS domain that is at the minimum required firmware level. For more information, see *Cautions, Guidelines, and Limitations for Upgrading with Auto Install* and the appropriate [Cisco UCS upgrade guide](#).

Before You Begin

Complete all prerequisites listed in [Prerequisites for Upgrading and Downgrading Firmware](#), on page 9.

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

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
- Step 2** On the **Equipment** tab, click the **Equipment** node.
- Step 3** In the **Work** pane, click the **Firmware Management** tab.
- Step 4** In the **Work** pane, click the **Firmware Auto Install** tab.
- Step 5** In the **Actions** area, click **Install Infrastructure Firmware**.
- Step 6** In the **Prerequisites** page of the **Install Infrastructure Firmware** dialog box, ensure that you address the warnings before proceeding.

Warnings are given in the following categories:

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

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

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

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

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

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

- Step 9** Click **OK**.
The **Firmware Installer** field on the **Firmware Auto Install** tab displays the status of the infrastructure firmware upgrade.
- Note** If there is not enough space under bootflash, a warning will display and the upgrade process will stop.

What to Do Next

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

Acknowledging the Reboot of the Primary Fabric Interconnect

Before You Begin



Caution

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

- Ensure that all the IOMs that are attached to the Fabric Interconnect are up before you acknowledge the reboot of the Fabric Interconnect. If all IOMs are not up, all the servers connected to the Fabric Interconnect will immediately be re-discovered and cause a major disruption.
- Ensure that both of the Fabric Interconnects and the service profiles are configured for failover.
- Verify that the data path has been successfully restored from the secondary Fabric Interconnect before you acknowledge the reboot of the primary Fabric Interconnect. For more information, see [Verifying that the Data Path is Ready](#), on page 77.

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

Procedure

- Step 1** On the toolbar, click **Pending Activities**.
 - Step 2** In the **Pending Activities** dialog box, click the **User Acknowledged Activities** tab.
 - Step 3** In the table, locate the row for the pending reboot of the primary fabric interconnect.
 - Step 4** In the **Reboot Now** column for that row, check the **Acknowledge All** check box.
 - Step 5** Click **OK**.
Cisco UCS Manager immediately reboots the primary fabric interconnect. You cannot stop this reboot after you click **OK**.
-

Canceling an Infrastructure Firmware Upgrade



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

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
 - Step 2** On the **Equipment** tab, click the **Equipment** node.
 - Step 3** In the **Work** pane, click the **Firmware Management** tab.
 - Step 4** In the **Work** pane, click the **Firmware Auto Install** tab.
 - Step 5** In the **Actions** area, click **Install Infrastructure Firmware**.
 - Step 6** In the **Actions** area of the **Install Infrastructure Firmware** dialog box, click **Cancel Infrastructure Upgrade**.
 - Step 7** If a confirmation dialog box displays, click **Yes**.
 - Step 8** Click **OK**.
-

Clearing the Startup Version of the Default Infrastructure Pack

You must clear the startup version of the default infrastructure pack before directly upgrading or activating Cisco UCS Manager, Fabric Interconnects, and IOMs.

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
 - Step 2** Click the **Equipment** node.
 - Step 3** In the **Work** pane, click the **Firmware Management** tab.
 - Step 4** In the **Work** pane, click the **Firmware Auto Install** tab.
 - Step 5** In the **Actions** area, click **Clear Startup Version**.
 - Step 6** In the confirmation dialog box that appears, click **Yes**.
 - Step 7** Click **OK**.
-

Upgrading the Server Firmware with Auto Install

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



Note

You cannot use Auto Install to upgrade either the infrastructure or the servers in a Cisco UCS domain if Cisco UCS Manager in that domain is at a release prior to Cisco UCS 2.1(1). However, after you upgrade Cisco UCS Manager to Release 2.1(1) or greater, you can use Auto Install to upgrade the remaining components in a Cisco UCS domain that is at the minimum required firmware level. For more information, see *Cautions, Guidelines, and Limitations for Upgrading with Auto Install* and the appropriate [Cisco UCS upgrade guide](#).



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, the timing of the actual reboot of servers occurs depends upon the maintenance policy in the service profile associated with the server.

Before You Begin

Complete all prerequisites listed in [Prerequisites for Upgrading and Downgrading Firmware](#), on page 9.

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
- Step 2** On the **Equipment** tab, click the **Equipment** node.
- Step 3** In the **Work** pane, click the **Firmware Management** tab.
- Step 4** In the **Work** pane, click the **Firmware Auto Install** tab.
- Step 5** In the **Actions** area, click **Install Server Firmware**.
- Step 6** On the **Prerequisites** page of the **Install Server Firmware** wizard, carefully review the prerequisites and guidelines listed on this page and then do one of the following:

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

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

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

If the Cisco UCS domain includes both blade servers and rack servers, we recommend that you choose a new firmware version for the B-Series blade servers and C-Series rack-mount servers in the **Select Package Versions** page and upgrade all servers in the domain.

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

- Click **Next**.

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

- Expand the node for each organization that contains a host firmware package you want to update with the selected software.
- Check the check box next to the name of each host firmware package that you want to update.
This step updates the selected host firmware package with the new version of firmware. You must choose the host firmware packages included in the service profiles associated with all servers in the Cisco UCS domain to update all servers.
- Click **Next**.

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

- Expand the node for each host firmware package listed in the table.
- Review the list of service profiles that include the host firmware package.
- If desired, click a link in one of the following columns:
 - **Host Pack DN** column—Opens the navigator for the host firmware package.
 - **Service Profile DN** column—Opens the navigator for the service profile.
- Do one of the following:
 - If you want to change one or more of the selected host firmware packages, click **Prev**.
 - If you are satisfied that you have selected the appropriate host firmware packages and want to review the impact of the server firmware upgrade on the endpoints, click **Next**.
 - If you want to start the server upgrade immediately, click **Install**.

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

- Click the appropriate check boxes to filter the results in the **Impacted Endpoints** table.
You can filter the results by the type of endpoint and by whether the impact of the upgrade is disruptive or not.

- b) Review the list of impacted endpoints.
- c) If desired, click the link in the **Maintenance Policy** column to open the navigator for that policy.
- d) Do one of the following:
 - If you want to change one or more of the selected host firmware packages, click **Prev**.
 - If you are satisfied that you have selected the appropriate host firmware packages and want to start the server upgrade, click **Install**.

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



Using Firmware Automatic Synchronization Server Policy

This chapter includes the following sections:

- [Firmware Automatic Synchronization](#), page 37
- [Setting the Firmware Auto-Sync Server Policy](#), page 38

Firmware Automatic Synchronization

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



Important

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

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

- **User Acknowledge**—Firmware on the server is not synchronized until the administrator acknowledges the upgrade in the **Pending Activities** dialog box.
- **No Action**—No firmware upgrade is initiated on the server.

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

- The firmware version on a server or the endpoint on a server differs from the firmware version configured in the default host firmware pack.

- The value for the **Firmware Auto Sync Server** policy has been modified. For example, if you had initially set it as **No Action** and you change it to **User Acknowledge**.

**Important**

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

Setting the Firmware Auto-Sync Server Policy

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

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

Before You Begin

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

Procedure

-
- Step 1** In the Navigation pane, click the **Equipment** tab.
- Step 2** On the **Equipment** tab, click the **Equipment** node.
- Step 3** In the Work pane, click the **Policies** tab.
- Step 4** Click the **Global Policies** subtab.
- Step 5** In the **Firmware Auto Sync Server Policy** area, select one of the following values as the **Sync State**:
- **User Acknowledge**—Firmware on the server is not synchronized until the administrator acknowledges the upgrade in the **Pending Activities** dialog box.
 - **No Action**—No firmware upgrade is initiated on the server.
- Step 6** Click **Save Changes**.
-



Directly Upgrading Firmware at Endpoints

This chapter includes the following sections:

- [Direct Firmware Upgrade at Endpoints, page 39](#)
- [Updating the Firmware on Multiple Endpoints, page 42](#)
- [Adapter Firmware, page 43](#)
- [BIOS Firmware, page 45](#)
- [CIMC Firmware, page 46](#)
- [PSU Firmware Update, page 48](#)
- [Board Controller Firmware, page 49](#)
- [Cisco UCS Manager Firmware, page 54](#)
- [Fabric Interconnect Firmware, page 55](#)
- [Verifying Firmware Versions on Components, page 58](#)

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:

- Adapters
- CIMCs
- I/O modules
- Board controllers
- Cisco UCS Manager
- Fabric interconnects

The adapter and board controller 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 Upgrades of a CIMC through a management firmware package or an adapter through a firmware package in the service profile associated with the server take precedence over direct firmware upgrades. 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.

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:

- Adapters
- CIMCs
- I/O modules



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
- Board controllers on those servers that support them

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.


Caution

When you configure **Set Startup Version Only** for an I/O module, the I/O module is rebooted when the fabric interconnect in its data path is rebooted. If you do not configure **Set Startup Version Only** for an I/O module, the I/O module reboots and disrupts traffic. In addition, if Cisco UCS Manager detects a protocol and firmware version mismatch between the fabric interconnect and the I/O module, Cisco UCS Manager automatically updates the I/O module with the firmware version that matches the firmware in the fabric interconnect, and then activates the firmware and reboots the I/O module again.

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 following outage impacts and disruptions:

- The fabric interconnect reboots.
- The corresponding I/O modules 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 an I/O Module Firmware Upgrade

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

- For a standalone configuration with a single fabric interconnect, data traffic is disrupted when the I/O module reboots. For a cluster configuration with two fabric interconnects, data traffic fails over to the other I/O module and the fabric interconnect in its data path.
- If you activate the new firmware as the startup version only, the I/O module reboots when the corresponding fabric interconnect is rebooted.
- If you activate the new firmware as the running and startup version, the I/O module reboots immediately.
- An I/O module can take up to ten minutes to become available after a firmware upgrade.

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 an Adapter Firmware Upgrade

If you activate the firmware for an adapter and do not configure the **Set Startup Version Only** option, you cause the following outage impacts and disruptions:

- The server reboots.
- Server traffic is disrupted.

Updating the Firmware on Multiple Endpoints

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

- Adapters
- CIMCs
- I/O modules



Caution

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

Procedure

-
- Step 1** In the **Navigation** pane, click **Equipment**.
 - Step 2** On the **Equipment** tab, click the **Equipment** node.
 - Step 3** In the **Work** pane, click the **Firmware Management** tab.
 - Step 4** On the **Installed Firmware** tab, click **Update Firmware**.
Cisco UCS Manager GUI opens the **Update Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS domain. This step might take a few minutes, based on the number of chassis and servers.
 - Step 5** In the **Update Firmware** dialog box, do the following:
 - a) From the **Filter** drop-down list on the menu bar, select **ALL**.
If you want to update all endpoint firmware of a specific type, such as all adapters or server BIOS, select that type from the drop-down list.
 - b) In the **Select** field, do one of the following:

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

c) Click **OK**.

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

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

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

Step 6 (Optional) To monitor the progress of the update to a specific endpoint, right-click the endpoint and choose **Show Navigator**.

Cisco UCS Manager displays the progress in the **Update Status** area on the **General** tab. If the navigator has an **FSM** tab, you can also monitor the progress there. An entry in the **Retry #** field might not indicate that the update failed. The retry count also includes retries that occur when Cisco UCS Manager retrieves the update status.

What to Do Next

Activate the firmware.

Adapter Firmware

Updating the Firmware on an Adapter



Caution

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

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
- Step 2** Expand **Equipment > Chassis > Chassis Number > Servers**.
- Step 3** Expand the node for the server which includes the adapter you want to update.
- Step 4** Expand **Adapters** and select the adapter you want to upgrade.
- Step 5** In the **General** tab, click **Update Firmware**.
- Step 6** In the **Update Firmware** dialog box, do the following:
- From the **Version** drop-down list, select the firmware version to update the endpoint.
 - Click **OK**.
If one or more endpoints cannot be directly updated, Cisco UCS Manager displays a notification message. After you acknowledge the notification message, Cisco UCS Manager updates the firmware for all other endpoints on servers that can be directly updated.
- Cisco UCS Manager copies the selected firmware package to the backup memory slot, where it remains until you activate it.
- Step 7** (Optional) Monitor the status of the update in the **Update Status** area. The update process can take several minutes. Do not activate the firmware until the selected firmware package displays in the **Backup Version** field in the **Firmware** area of the **General** tab.
-

What to Do Next

Activate the firmware.

Activating the Firmware on an Adapter

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
- Step 2** Expand **Equipment > Chassis > Chassis Number > Servers**.
- Step 3** Expand the node for the server that includes the adapter for which you want to activate the updated firmware.
- Step 4** Expand **Adapters** and select the adapter for which you want to activate the firmware.
- Step 5** In the **General** tab, click **Activate Firmware**.
- Step 6** In the **Activate Firmware** dialog box, do the following:
- Select the appropriate version from the **Version To Be Activated** drop-down list.
If one or more of the selected endpoints are not configured with the required version as the backup version, that version does not display in the **Set Version** drop-down list. You must select the version from the **Startup Version** column for each individual endpoint.
 - If you want to set the startup version and not change the version running on the endpoint, check the **Set Startup Version Only** check box.
During a direct upgrade, you should configure **Set Startup Version Only** for an adapter. With this setting, the activated firmware moves into the pending-next-boot state, and the server is not immediately rebooted.

The activated firmware does not become the running version of firmware on the adapter until the server is rebooted. You cannot configure **Set Startup Version Only** for an adapter in the host firmware package.

If a server is not associated with a service profile, the activated firmware remains in the pending-next-boot state. Cisco UCS Manager does not reboot the endpoints or activate the firmware until the server is associated with a service profile. If necessary, you can manually reboot or reset an unassociated server to activate the firmware.

- c) Click **OK**.
-

BIOS Firmware

Updating the BIOS Firmware on a Server



Caution

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

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
- Step 2** Expand **Equipment** > **Chassis** > *Chassis Number* > **Servers**.
- Step 3** Expand the node for the server for which you want to update the BIOS firmware.
- Step 4** On the **General** tab, click the **Inventory** tab.
- Step 5** Click the **Motherboard** tab.
- Step 6** In the **Actions** area, click **Update Bios Firmware**.
- Step 7** In the **Update Firmware** dialog box, do the following:
 - a) From the **Version** drop-down list, select the firmware version to which you want to update the server BIOS.
 - b) (Optional) If you want to update the firmware regardless of any possible incompatibilities or currently executing tasks, check the **Force** check box.
 - c) Click **OK**.

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

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

What to Do Next

Activate the firmware.

Activating the BIOS Firmware on a Server

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
 - Step 2** Expand **Equipment > Chassis > Chassis Number > Servers**.
 - Step 3** Expand the node for the server for which you want to activate the updated BIOS firmware.
 - Step 4** On the **General** tab, click the **Inventory** tab.
 - Step 5** Click the **Motherboard** tab.
 - Step 6** In the **Actions** area, click **Activate Bios Firmware**.
 - Step 7** In the **Activate Firmware** dialog box, do the following:
 - a) Select the appropriate server BIOS version from the **Version To Be Activated** drop-down list.
 - b) If you want to set the start up version and not change the version running on the server, check the **Set Startup Version Only** check box.
If you configure **Set Startup Version Only**, the activated firmware moves into the pending-next-reboot state and the server is not immediately rebooted. The activated firmware does not become the running version of firmware until the server is rebooted.
 - c) Click **OK**.
-

CIMC Firmware

Updating the CIMC Firmware on a Server



Caution

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

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
- Step 2** Expand **Equipment > Chassis > Chassis Number > Servers**.
- Step 3** Expand the node for the server for which you want to update the CIMC.
- Step 4** In the **General** tab, click the **Inventory** tab.
- Step 5** Click the **CIMC** tab.
- Step 6** In the **Actions** area, click **Update Firmware**.
- Step 7** In the **Update Firmware** dialog box, do the following:

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

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

- Step 8** (Optional) Monitor the status of the update in the **Update Status** area. The update process can take several minutes. Do not activate the firmware until the selected firmware package displays in the **Backup Version** field in the **Firmware** area of the **General** tab.

What to Do Next

Activate the firmware.

Activating the CIMC Firmware on a Server

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



Caution

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

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
- Step 2** Expand **Equipment** > **Chassis** > *Chassis Number* > **Servers**.
- Step 3** Expand the node for the server that includes the CIMC for which you want to activate the updated firmware.
- Step 4** On the **General** tab, click the **Inventory** tab.
- Step 5** Click the **CIMC** tab.
- Step 6** In the **Actions** area, click **Activate Firmware**.
- Step 7** In the **Activate Firmware** dialog box, do the following:
 - a) Select the appropriate version from the **Version To Be Activated** drop-down list. If one or more of the selected endpoints are not configured with the required version as the backup version, that version does not display in the **Set Version** drop-down list. You must select the version from the **Startup Version** column for each individual endpoint.
 - b) If you want to set the startup version and not change the version running on the endpoint, check the **Set Startup Version Only** check box. If you configure **Set Startup Version Only**, the activated firmware moves to the pending-next-reboot state and the endpoint is not immediately rebooted. The activated firmware does not become the running version of firmware until the endpoint reboots.
 - c) Click **OK**.

PSU Firmware Update

Beginning with Release 3.0(2), you can update PSU firmware directly from Cisco UCS Manager. The following PSU models are supported:

- Emerson Dual Voltage (DV) PSU with PID: UCSB-PSU-2500-ACDV
- Delta Dual Voltage (DV) PSU with PID: UCSB-PSU-2500-ACDV

Updating the Firmware on a PSU



Caution

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

Procedure

-
- Step 1** In the **Navigation** pane, click **Equipment**.
 - Step 2** On the **Equipment** tab, expand **Equipment > Chassis**.
 - Step 3** Select the chassis for which you want to manage the PSUs.
 - Step 4** In the **Work** pane, click **PSUs**.
 - Step 5** Click the **Firmware Management** tab.
 - Step 6** Right-click the PSU that you want to upgrade and choose **Update Firmware**.
 - Step 7** In the **Update Firmware** dialog box, do the following:
 - a) From the **Version** drop-down list, select the firmware version to which you want to update the endpoint.
 - b) Click **OK**.

Cisco UCS Manager copies the selected firmware package to the backup memory slot, where it remains until you explicitly activate it.
 - Step 8** (Optional) Monitor the status of the update in the **Update Status** area. The update process can take several minutes. Do not activate the firmware until the selected firmware package displays in the **Backup Version** field in the **Firmware** area of the **General** tab.
-

What to Do Next

Activate the firmware.

Activating the Firmware on a PSU

Procedure

-
- Step 1** In the **Navigation** pane, click **Equipment**.
- Step 2** On the **Equipment** tab, expand **Equipment > Chassis**.
- Step 3** Select the chassis for which you want to manage the PSUs.
- Step 4** In the **Work** pane, click **PSUs**.
- Step 5** Right-click the PSU that you want to upgrade and choose **Activate Firmware**.
- Step 6** In the **General** tab, click **Activate Firmware**.
- Step 7** In the **Activate Firmware** dialog box, do the following:
- Select the appropriate version from the **Version To Be Activated** drop-down list.
If one or more of the selected endpoints are not configured with the required version as the backup version, that version does not display in the **Set Version** drop-down list. You must select the version from the **Startup Version** column for each individual endpoint.
 - If you want to set the startup version and not change the version running on the endpoint, check the **Set Startup Version Only** check box.
If you configure **Set Startup Version Only**, the activated firmware moves to the pending-next-reboot state and the endpoint is not immediately rebooted. The activated firmware does not become the running version of firmware until the endpoint reboots.
 - Click **OK**.
-

Board Controller Firmware

Board controllers maintain various programmable logic and power controllers for all B-Series blade servers, and C-Series rack servers. The board controller update utility enables you to make critical hardware updates.

Board controllers, introduced in Cisco UCS Manager Release 2.1(2a), allow you to make optimizations for components, such as voltage regulators, through an update to a digital controller configuration file by using the board controller update utility. Earlier, updating a voltage regulator required changing physical components. These updates are at a hardware level, and are designed to be backward-compatible. Therefore, having the latest version of the board controller is always preferred.

Guidelines for Activating Cisco UCS B-Series M3 and M4 Blade Server Board Controller Firmware

The following guidelines apply to Cisco UCS B-Series M3 and M4 blade server board controller firmware:

- You never need to downgrade the board controller firmware.
- The board controller firmware version of the blade server should be the same as or later than the installed software bundle version. Leaving the board controller firmware at a later version than the version that is currently running in your existing Cisco UCS environment does not violate the software matrix or TAC supportability.
- Board controller firmware updates are backward compatible with the firmware of other components.

Some Cisco UCS B200 M4 blade servers running on releases prior to Release 2.2(4b) may generate a false Cisco UCS Manager alert, documented in CSCuu15465. This false board controller mismatch alert was resolved in Cisco UCS Manager Capability Catalogs 2.2(4c)T and 2.2(5b)T. You will not see this alert if you use either the 2.2(4c)T or the 2.2(5b)T capability catalog.



Note For more information, refer to <https://tools.cisco.com/bugsearch/bug/CSCuu15465>

You can apply the capability catalog update as follows:

- 1 Download 2.2(4c) Infra/Catalog or 2.2(5b) Infra/Catalog software bundle. [Downloading and Managing Firmware in Cisco UCS Manager, on page 19](#) provides detailed information about downloading software bundles.
- 2 Load catalog version 2.2(4c)T or 2.2(5b)T (or the catalog version included) and activate the catalog. [Activating a Capability Catalog Update](#) provides detailed information about activating a capability catalog through Cisco UCS Manager.
- 3 Decommission the newly inserted blade server.
- 4 Associate the service profile with the host firmware pack policy that has the earlier board controller version.
When the service profile is associated with the updated host firmware pack policy, any false mismatch alert (such as the one caused by the CSCuu15465 bug) will not be raised any more.
- 5 Click **Save**.
- 6 Re-discover the blade server.

Guidelines for Activating Cisco UCS C-Series M3 and M4 Rack Server Board Controller Firmware

The following guidelines apply to Cisco UCS C-Series M3 and M4 rack server board controller firmware:

- The board controller firmware and the CIMC firmware must be of the same package version.
- When you upgrade the C-Series server firmware for Cisco UCS C220 M4 or C240 M4 servers to Cisco UCS Manager 2.2(6c), you will see the following critical alarm:

`Board controller upgraded, manual a/c power cycle required on server x`
This alarm, documented in CSCuv45173, is incorrectly categorized as a critical alarm. It does not impact the functionality of the server, and can be ignored.

To avoid seeing this alarm, you can do one of the following:

- Create a custom host firmware package in Cisco UCS Manager to exclude the board controller firmware from the Cisco UCS Manager 2.2(6c) update and keep the older version.
- Upgrade Cisco UCS Manager infrastructure (A Bundle) to Release 2.2(6c) and continue to run the host firmware (C Bundle) on any Cisco UCS C220 M4 or C240 M4 server at a lower version, according to the mixed firmware support matrix in Table 2 of the *Release Notes for Cisco UCS Manager, Release 2.2*.



Note For more information, refer to <https://tools.cisco.com/bugsearch/bug/CSCuv45173>

- If the activation status of the board controller displays **Pending Power Cycle** after you upgrade the board controller, a manual power cycle is required. A fault is also generated. After the power cycle is complete, the fault is cleared and the board controller activation status displays **Ready**.

Activating the Board Controller Firmware on a Cisco UCS B-Series M2 Blade Server

The board controller firmware controls many of the server functions, including eUSBs, LEDs, and I/O connectors.



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

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
- Step 2** On the **Equipment** tab, click the **Equipment** node.
- Step 3** In the **Work** pane, click the **Firmware Management** tab.
- Step 4** On the **Installed Firmware** tab, click **Activate Firmware**.
Cisco UCS Manager GUI opens the **Activate Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS domain. This step might take a few minutes, based on the number of chassis and servers.
- Step 5** From the **Filter** drop-down list on the menu bar of the **Activate Firmware** dialog box, select **Board Controller**. Cisco UCS Manager GUI displays all servers that have board controllers in the **Activate Firmware** dialog box.
- Step 6** In the **Select** field, do one of the following:
 - To activate the board controller firmware on all servers to the same version, click the **Version** radio button and select the appropriate version from the **Set Version** drop-down list.
 - To activate the board controller firmware on all servers to the firmware version included in a specific bundle, click the **Bundle** radio button and select the appropriate bundle from the **Set Bundle** drop-down list .
- Step 7** Click **OK**.

Activating the Board Controller Firmware on Cisco UCS B-Series M3 and M4 Blade Servers

The board controller firmware controls many of the server functions, including eUSBs, LEDs, and I/O connectors.

**Note**

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

The following limitations apply to M3 and M4 board controller firmware:

- You cannot downgrade the firmware after the upgrade is complete.
- You must be using Cisco UCS Manager, Release 2.1(2a) or greater.
- The board controller firmware version of the blade server should be the same or newer than the installed software bundle version.

Before you activate the board controller firmware on M3 and M4 blade servers, consider the following guidelines:

- Leaving the board controller firmware at a later version than the version that is currently running in your existing Cisco UCS environment does not violate the software matrix or TAC supportability.
- Board controller firmware updates are always backward compatible with the firmware of other components. However, you cannot downgrade the board controller firmware in Cisco UCS Manager.
- If blade server components, such as CIMC, and adapter, are running a firmware version that is earlier than the firmware version of the board controller, you do not need to upgrade the blade components to match the firmware version running on the board controller.

Additionally, you may be impacted by a defect, documented in CSCuu15465, which creates a board controller "mismatch" alert. This is a false alert and was resolved in UCSM Capability Catalogs 2.2(4c)T and 2.2(5b)T.

**Note**

For more information, please refer to <https://tools.cisco.com/bugsearch/bug/CSCuu15465>

You can apply the capability catalog update as follows:

- 1 Download 2.2(4c) Infra/Catalog or 2.2(5b) Infra/Catalog software bundle. [Downloading and Managing Firmware in Cisco UCS Manager, on page 19](#) provides detailed information about downloading software bundles.
- 2 Load catalog version 2.2(4c)T or 2.2(5b)T (or the catalog version included) and activate the catalog. [Activating a Capability Catalog Update](#) provides detailed information about activating a capability catalog through Cisco UCS Manager.
- 3 Decommission the newly inserted blade server.
- 4 Associate the blade server with the host firmware pack policy that has the earlier board controller version. No false mismatch alerts are raised because the catalog has the fix for CSCuu15465.

**Note**

This is a catalog-only fix

Procedure

-
- Step 1** In the **Navigation** pane, click **Equipment**.
- Step 2** On the **Equipment** tab, click the **Equipment** node.
- Step 3** In the **Work** pane, click the **Firmware Management** tab.
- Step 4** On the **Installed Firmware** tab, click **Activate Firmware**.
Cisco UCS Manager GUI opens the **Activate Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS domain. This step might take a few minutes, based on the number of chassis and servers.
- Step 5** From the **Filter** drop-down list on the menu bar of the **Activate Firmware** dialog box, select **Board Controller**. Cisco UCS Manager GUI displays all servers that have board controllers in the **Activate Firmware** dialog box.
- Step 6** For the board controller you want to update, select a version from the **Startup Version** drop-down list.
- Step 7** Click **OK**.
- Step 8** (Optional) You can also use the **Force Board Controller Activation** option to update the firmware version when you upgrade CPUs with different architectures. For example, when you upgrade from Sandy Bridge to Ivy Bridge CPUs.
-

Activating the Board Controller Firmware on Cisco UCS C-Series M3 and M4 Rack Servers

The board controller firmware controls many of the server functions, including eUSBs, LEDs, and I/O connectors.



Note

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

The following limitations apply to M3 and M4 board controller firmware:

- You must be using Cisco UCS Manager, Release 2.2(1a) or greater.
- The board controller firmware and the CIMC firmware must be of the same package version.
- If the activation status of the board controller displays **Pending Power Cycle** after you upgrade the board controller, a manual power cycle is required. A fault is also generated. After the power cycle is complete, the fault is cleared and the board controller activation status displays **Ready**.

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
- Step 2** On the **Equipment** tab, click the **Equipment** node.
- Step 3** In the **Work** pane, click the **Firmware Management** tab.
- Step 4** On the **Installed Firmware** tab, click **Activate Firmware**.
Cisco UCS Manager GUI opens the **Activate Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS domain. This step might take a few minutes, based on the number of chassis and servers.
- Step 5** From the **Filter** drop-down list on the menu bar of the **Activate Firmware** dialog box, select **Board Controller**. Cisco UCS Manager GUI displays all servers that have board controllers in the **Activate Firmware** dialog box.
- Step 6** For the board controller you want to update, select a version from the **Startup Version** drop-down list.
- Step 7** Click **OK**.
- Step 8** (Optional) You can also use the **Force Board Controller Activation** option to update the firmware version when you upgrade CPUs with different architectures. For example, you upgrade from Sandy Bridge to Ivy Bridge CPUs.
-

Cisco UCS Manager Firmware

Consider the following guidelines and best practices while activating firmware on the Cisco UCS Manager software:

- In a cluster configuration, Cisco UCS Manager on both fabric interconnects must run the same version.
- Cisco UCS Manager activation brings down management for a brief period. All virtual shell (VSH) connections are disconnected.
- In a cluster configuration, Cisco UCS Manager on both fabric interconnects is activated.
- A Cisco UCS Manager update does not affect server application I/O because fabric interconnects do not need to be reset.
- If Cisco UCS Manager is updated while the subordinate fabric interconnect is down, the subordinate fabric interconnect is automatically updated when it comes back up.

Upgrade Validation

Cisco UCS Manager validates the upgrade or downgrade process and displays all firmware upgrade validation failures, such as deprecated hardware, in the **Upgrade Validation** tab. If there are upgrade validation failures, the upgrade fails, and Cisco UCS Manager rolls back to the earlier version. You must resolve these faults before continuing with the upgrade.

When upgrading or downgrading the infrastructure firmware through the Auto Install method, if you do not want Cisco UCS Manager to report issues with the upgrade or downgrade process, check the **Skip Validation** check box. Conversely, to report issues with the upgrade or downgrade process, clear the **Skip Validation** check box. The **Skip Validation** check box is cleared by default.

Activating the Cisco UCS Manager Software

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
- Step 2** On the **Equipment** tab, click the **Equipment** node.
- Step 3** In the **Work** pane, click the **Firmware Management** tab.
- Step 4** On the **Installed Firmware** tab, click **Activate Firmware**.
Cisco UCS Manager GUI opens the **Activate Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS domain. This step might take a few minutes, based on the number of chassis and servers.
- Step 5** On the **UCS Manager** row of the **Activate Firmware** dialog box, do the following:
- a) From the drop-down list in the **Startup Version** column, select the version to which you want to update the software.
 - b) Click **OK**.
- Cisco UCS Manager disconnects all active sessions, logs out all users, and activates the software. When the upgrade is complete, you are prompted to log back in. If you are prompted to re-login immediately after being disconnected, the login will fail. You must wait until the activation of Cisco UCS Manager is completed, which takes a few minutes.
- Cisco UCS Manager makes the selected version the startup version and schedules the activation to occur when the fabric interconnects are upgraded.
-

Fabric Interconnect Firmware

Activating the Firmware on a Subordinate Fabric Interconnect

Before You Begin

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

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
- Step 2** On the **Equipment** tab, click the **Equipment** node.
- Step 3** In the **Work** pane, click the **Firmware Management** tab.
- Step 4** On the **Installed Firmware** tab, click **Activate Firmware**.
Cisco UCS Manager GUI opens the **Activate Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS domain. This step might take a few minutes, based on the number of chassis and servers.

- Step 5** From the **Filter** drop-down list on the menu bar, choose **Fabric Interconnects**.
- Step 6** On the row of the **Activate Firmware** dialog box for the subordinate fabric interconnect, do the following:
- In the **Kernel** row, choose the firmware version to which you want to upgrade from the drop-down list in the **Startup Version** column.
 - In the **System** row, choose the firmware version to which you want to upgrade from the drop-down list in the **Startup Version** column.
- Step 7** Click **Apply**.
Cisco UCS Manager updates and activates the firmware and reboots the fabric interconnect and any I/O module in the data path to that fabric interconnect, disrupting data traffic to and from that fabric interconnect. However, assuming the Cisco UCS domain is configured to permit traffic and port failover, data traffic fails over to the primary fabric interconnect and is not disrupted.
- Step 8** Verify the high availability status of the subordinate fabric interconnect.
If the **High Availability Details** area for the fabric interconnect does not show the following values, contact Cisco Technical Support immediately. Do not continue to update the primary fabric interconnect.

Field Name	Required Value
Ready field	Yes
State field	Up

What to Do Next

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

Activating the Firmware on a Primary Fabric Interconnect

This procedure continues directly from [Activating the Firmware on a Subordinate Fabric Interconnect](#), on page 55 and assumes you are on the **Firmware Management** tab.

Before You Begin

Activate the subordinate fabric interconnect.

Procedure

- Step 1** On the **Installed Firmware** tab, click **Activate Firmware**.
Cisco UCS Manager GUI opens the **Activate Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS domain. This step might take a few minutes, based on the number of chassis and servers.
- Step 2** From the **Filter** drop-down list on the menu bar, choose **Fabric Interconnects**.
- Step 3** On the row of the **Activate Firmware** dialog box for the subordinate fabric interconnect, do the following:

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

Step 4 Click **Apply**.

Cisco UCS Manager updates and activates the firmware and reboots the fabric interconnect and any I/O module in the data path to that fabric interconnect, disrupting data traffic to and from that fabric interconnect. However, assuming the Cisco UCS domain is configured to permit traffic and port failover, data traffic fails over to the other fabric interconnect, which becomes the primary. When it comes back up, this fabric interconnect is the subordinate fabric interconnect.

Step 5 Verify the high availability status of the fabric interconnect.

If the **High Availability Details** area for the fabric interconnect does not show the following values, contact Cisco Technical Support immediately.

Field Name	Required Value
Ready field	Yes
State field	Up

Activating the Firmware on a Standalone Fabric Interconnect

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

**Tip**

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

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
- Step 2** On the **Equipment** tab, click the **Equipment** node.
- Step 3** Expand the **Fabric Interconnects** node and click the standalone fabric interconnect.
- Step 4** On the **General** tab, click **Activate Firmware**.
- Step 5** In the **Activate Firmware** dialog box, complete the following fields:

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

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

Step 6 Click **OK**.

Cisco UCS Manager activates the firmware and reboots the fabric interconnect and any I/O module in the data path to that fabric interconnect. For a standalone fabric interconnect, this disrupts all data traffic in the Cisco UCS domain.

Verifying Firmware Versions on Components

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
 - Step 2** On the **Equipment** tab, click the **Equipment** node.
 - Step 3** In the **Work** pane, click the **Firmware Management** tab.
 - Step 4** On the **Installed Firmware** tab, review the firmware versions listed for each component.
-



Upgrading Firmware through Firmware Packages in Service Profiles

This chapter includes the following sections:

- [Firmware Upgrades through Firmware Packages in Service Profiles](#) , page 59
- [Creating a Host Firmware Package](#) , page 65
- [Updating a Host Firmware Package](#) , page 66
- [Updating a Management Firmware Package](#) , page 67
- [Adding Firmware Packages to an Existing Service Profile](#) , page 68

Firmware Upgrades through Firmware Packages in Service Profiles

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

If the default host firmware pack is updated, and the server is not associated with a service profile, the server reboots and new firmware is applied. This behavior is not managed by the Firmware Auto Sync Server policy because it is only for recently discovered servers.

You cannot upgrade the firmware on an I/O module, 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 and adapter endpoints:

- **Adapter**
- **Server BIOS**
- **CIMC**
- **Board Controller**
- **Flex Flash Controller**
- **Graphics Card**
- **Host HBA**
- **Host HBA Option ROM**
- **Host NIC**
- **Host NIC Option ROM**
- **Local Disk**



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

To update local disk firmware, always include the **Blade Package** in the host firmware package. The blade package contains the local disk firmware for blade and rack servers.

- **PSU**
- **SAS Expander**
- **RAID Controller**
- **Storage Controller Onboard Device**
- **Storage Controller Onboard Device Cpld**
- **Storage Device Bridge**



Remember

To update local disk firmware for blade or rack servers, always include the blade package in the host firmware package. The blade package contains the local disk firmware for both blade and rack servers.

**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.

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

**Note**

Each host firmware package is associated with one list of excluded components, which is common across all firmware packages—Blade and Rack. To configure a separate exclusion list for each type of firmware package, use separate host firmware packages.

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
<p>Firmware package is not included in a service profile or an updating service profile template.</p> <p>OR</p> <p>You want to upgrade the firmware without making any changes to the existing service profile or updating service profile template.</p>	<p>No maintenance policy</p>	<p>After you update the firmware package, do one of the following:</p> <ul style="list-style-type: none"> • 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: <ol style="list-style-type: none"> 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. <p>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.</p>
<p>The firmware package is included in one or more service profiles, and the service profiles are associated with one or more servers.</p> <p>OR</p> <p>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.</p>	<p>No maintenance policy</p> <p>OR</p> <p>A maintenance policy configured for immediate updates.</p>	<p>The following occurs when you update the firmware package:</p> <ol style="list-style-type: none"> 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. <p>All servers associated with service profiles that include the firmware package are rebooted at the same time.</p>

Service Profile	Maintenance Policy	Upgrade Actions
<p>The firmware package is included in one or more service profiles, and the service profiles are associated with one or more servers.</p> <p>OR</p> <p>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.</p>	<p>Configured for user acknowledgment</p>	<p>The following occurs when you update the firmware package:</p> <ol style="list-style-type: none"> 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. <p>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.</p>
<p>The firmware package is included in one or more service profiles, and the service profiles are associated with one or more servers.</p> <p>OR</p> <p>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.</p>	<p>Configured for changes to take effect during a specific maintenance window.</p>	<p>The following occurs when you update the firmware package:</p> <ol style="list-style-type: none"> 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. <p>A manual reboot of the servers does not cause Cisco UCS to apply the firmware package, nor does it cancel the scheduled maintenance activities.</p>

Creating a Host Firmware Package



Tip

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

You can also exclude firmware of specific components from a host firmware package when creating a new host firmware package.



Important

Each host firmware package is associated with one list of excluded components, which is common across all firmware packages—Blade and Rack. To configure a separate exclusion list for each type of firmware package, use separate host firmware packages.

Before You Begin

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

Procedure

- Step 1** In the **Navigation** pane, click **Servers**.
- Step 2** Expand **Servers > Policies**.
- Step 3** Expand the node for the organization where you want to create the policy.
If the system does not include multitenancy, expand the **root** node.
- Step 4** Right-click **Host Firmware Packages** and choose **Create Package**.
- Step 5** In the **Create Host Firmware Package** dialog box, enter a unique name and description for the package. This name can be between 1 and 32 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.
- Step 6** To configure the host firmware package by selecting servers and components, select the **Simple** radio button in the **How would you like to configure the Host Firmware Package** field.
- Step 7** From the **Blade**, and **Rack** drop-down lists, select the firmware package.
- Step 8** In the **Excluded Components** area, check the checkboxes corresponding to the components that you want to exclude from this host firmware package.
If you do not check any component checkboxes, all the listed components are included in the host firmware package.

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

To update local disk firmware, always include the **Blade Package** in the host firmware package. The blade package contains the local disk firmware for blade and rack servers.

- Step 9** To configure the host firmware package with advanced options, select the **Advanced** radio button in the **How would you like to configure the Host Firmware Package** field.
- Step 10** On each subtab, do the following for each type of firmware that you want to include in the package:
- In the **Select** column, ensure that the check boxes for the appropriate lines are checked.
 - In the **Vendor**, **Model**, and **PID** columns, verify that the information matches the servers you want to update with this package.
The model and model number (PID) must match the servers that are associated with this firmware package. If you select the wrong model or model number, Cisco UCS Manager cannot install the firmware update.
 - In the **Version** column, choose the firmware version to which you want to update the firmware.
- Step 11** When you have added all the desired firmware to the package, click **OK**.

What to Do Next

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

Updating a Host Firmware Package

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

You can also exclude firmware of specific components from a host firmware package when modifying an existing host firmware package.



Important

Each host firmware package is associated with one list of excluded components, which is common across all firmware packages—Blade and Rack. To configure a separate exclusion list for each type of firmware package, use separate host firmware packages.

Before You Begin

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

Procedure

-
- Step 1** In the **Navigation** pane, click **Servers**.
- Step 2** Expand **Servers > Policies**.
- Step 3** Expand the node for the organization that includes the policy you want to update.
If the system does not include multitenancy, expand the **root** node.
- Step 4** Expand **Host Firmware Packages** and choose the policy you want to update.
- Step 5** In the **Work** pane, click the **General** tab.
- Step 6** On each subtab, do the following for each type of firmware that you want to include in the package:
- In the **Select** column, ensure that the check boxes for the appropriate lines are checked.

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

Step 7 To modify the components in the host firmware package, click **Modify Package Versions**. The **Modify Package Versions** window appears.

Step 8 On each server subtab, Blade and Rack, select the firmware package.

Step 9 In the **Excluded Components** area, check the checkboxes corresponding to the components that you want to exclude from this host firmware package.
If you do not check any component checkboxes, all the listed components are included in the host firmware package.

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

To update local disk firmware, always include the **Blade Package** in the host firmware package. The blade package contains the local disk firmware for blade and rack servers.

Step 10 Click **Save Changes**.
Cisco UCS Manager verifies the model numbers and vendor against all servers associated with service profiles that include this policy. If the model numbers and vendor match a firmware version in the policy, Cisco UCS Manager updates the firmware according to the settings in the maintenance policies included in the service profiles.

Updating a Management Firmware Package



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

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

Before You Begin

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

Procedure

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

Step 2 Expand **Servers** > **Policies**.

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

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

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

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

Step 6 In the firmware table, do the following:

- a) In the **Select** column, ensure that the check boxes for the appropriate lines are checked.
- b) In the **Vendor**, **Model**, and **PID** columns, verify that the information matches the servers you want to update with this package.
The model and model number (PID) must match the servers that are associated with this firmware package.
If you select the wrong model or model number, Cisco UCS Manager cannot install the firmware update.
- c) In the **Version** column, choose the firmware version to which you want to update the firmware.

Step 7 Click **Save Changes**.

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

Adding Firmware Packages to an Existing Service Profile

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

Procedure

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

Step 2 Expand **Servers > Service Profiles**.

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

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

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

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

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

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

Step 9 Click **Save Changes**.



Managing the Capability Catalog in Cisco UCS Manager

This chapter includes the following sections:

- [Capability Catalog, page 69](#)
- [Activating a Capability Catalog Update, page 71](#)
- [Verifying that the Capability Catalog Is Current, page 71](#)
- [Viewing a Capability Catalog Provider, page 72](#)
- [Downloading Individual Capability Catalog Updates, page 72](#)

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, and local disk. 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.

For information about which hardware components are dependent upon a particular catalog release, see the component support tables in the [Service Notes for the B- Series servers](#). For information about which components are introduced in a specific release, see the Cisco UCS [Release Notes](#).

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 Technical Assistance Center, 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* accessible through the *Cisco UCS B-Series Servers Documentation Roadmap* available at the following URL: <http://www.cisco.com/go/unifiedcomputing/b-series-doc>.

Activating a Capability Catalog Update

Procedure

- Step 1** In the **Navigation** pane, click **Admin**.
 - Step 2** On the **Admin** tab, expand **All**.
 - Step 3** Click the **Capability Catalog** node.
 - Step 4** In the **Work** pane, click the **Catalog Update Tasks** tab.
 - Step 5** Click **Activate Catalog**.
 - Step 6** In the **Activate Catalog** dialog box, choose the capability catalog update that you want to activate from the **Version to be Activated** drop-down list.
 - Step 7** Click **OK**.
-

Verifying that the Capability Catalog Is Current

Before You Begin

Procedure

- Step 1** In the **Navigation** pane, click **Admin**.
 - Step 2** On the **Admin** tab, expand **All**.
 - Step 3** Click the **Capability Catalog** node.
 - Step 4** In the **Work** pane, click the **Catalog Update Tasks** tab.
The current version of the capability catalog is located on the upper right of that tab.
 - Step 5** On Cisco.com, determine the most recent release of the capability catalog available.
For more information about the location of capability catalog updates, see [Obtaining Capability Catalog Updates from Cisco](#), on page 72.
 - Step 6** If a more recent version of the capability catalog is available on Cisco.com, update the capability catalog with that version.
-

Viewing a Capability Catalog Provider

Procedure

- Step 1** In the **Navigation** pane, click **Admin**.
- Step 2** On the **Admin** tab, expand **All > Capability Catalog**.
- Step 3** In the **Work** pane, click the tab for the provider you want to view.
- Step 4** To view the details of a provider, do the following:
- In the table, click the row with the vendor, model, and revision of the provider you want to view.
 - Click the **Expand** icon to the right of the heading to display the properties for the following areas:
 - **Equipment Manufacturing** area
 - **Form Factor** area
-

Downloading Individual Capability Catalog Updates

Obtaining Capability Catalog Updates from Cisco

Procedure

- Step 1** In a web browser, navigate to Cisco.com.
- Step 2** Under **Support**, click **All Downloads**.
- Step 3** In the center pane, click **Unified Computing and Servers**.
- Step 4** If prompted, enter your Cisco.com username and password to log in.
- Step 5** In the right pane, click **Cisco UCS Infrastructure and UCS Manager Software > Unified Computing System (UCS) Manager Capability Catalog**.
- Step 6** Click the link for the latest release of the Capability Catalog.
- Step 7** Click one of the following buttons and follow the instructions provided:
- **Download Now**—Allows you to download the catalog update immediately
 - **Add to Cart**—Adds the catalog update to your cart to be downloaded at a later time
- Step 8** Follow the prompts to complete your download of the catalog update.
-

What to Do Next

Update the Capability Catalog.

Updating the Capability Catalog from a Remote Location

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

A B-series server bundle includes the Capability Catalog update for that server. You do not need to download a separate Capability Catalog update. You only need to activate the Capability Catalog update.

Procedure

-
- Step 1** In the **Navigation** pane, click **Admin**.
 - Step 2** On the **Admin** tab, expand **All**.
 - Step 3** Click the **Capability Catalog** node.
 - Step 4** In the **Work** pane, click the **Catalog Update Tasks** tab.
 - Step 5** Click **Update Catalog**.
 - Step 6** In the **Update Catalog** dialog box, click the **Remote File System** radio button in the **Location of the Image File** field and fill in the required fields.
 - Step 7** Click **OK**.
-

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

Updating the Capability Catalog from the Local File System

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

A B-series server bundle includes the Capability Catalog update for that server. You do not need to download a separate Capability Catalog update. You only need to activate the Capability Catalog update.

Procedure

-
- Step 1** In the **Navigation** pane, click **Admin**.
 - Step 2** On the **Admin** tab, expand **All**.
 - Step 3** Click the **Capability Catalog** node.
 - Step 4** In the **Work** pane, click the **Catalog Update Tasks** tab.
 - Step 5** Click **Update Catalog**.
 - Step 6** In the **Download Firmware** dialog box, click the **Local File System** radio button in the **Location of the Image File** field.
 - Step 7** In the **Filename** field, type the full path and name of the image file.
If you do not know the exact path to the folder where the firmware image file is located, click **Browse** and navigate to the file.
 - Step 8** Click **OK**.
-

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



CHAPTER 10

Updating Management Extensions

This chapter includes the following sections:

- [Management Extensions, page 75](#)
- [Activating a Management Extension, page 75](#)

Management Extensions

Management Extension updates are included in each Cisco UCS Manager update. Unless otherwise instructed by Cisco Technical Support, you only need to activate the Management Extension update after you've downloaded, updated, and activated an Cisco UCS Infrastructure Software Bundle.

Management Extensions enable you to add support for previously unsupported servers and other hardware to Cisco UCS Manager. For example, you may need to activate a Management Extension if you want to add a new, previously unsupported server to an existing Cisco UCS domain.

The Management Extension image contains the images, information, and firmware required by Cisco UCS Manager to be able to manage the new hardware.

Cisco UCS Manager may need to access a Management Extension when you activate. Therefore, the Management Extension is locked during the activation and update process.

Activating a Management Extension

The Management Extension is included in the server bundle that you have already downloaded. You do not need to download the Management Extension separately.

Procedure

- Step 1** In the **Navigation** pane, click **Admin**.
 - Step 2** On the **Admin** tab, expand **All**.
 - Step 3** Click the **Management Extension** node.
 - Step 4** In the **Work** pane, click the **General** tab.
 - Step 5** In the **Actions** area, click **Activate Management Extension**.
 - Step 6** In the **Activate Management Extension** dialog box, choose the management extension that you want to activate from the **Version to be Activated** drop-down list.
 - Step 7** Click **OK**.
-



Verifying that the Data Path is Ready

This chapter includes the following sections:

- [Verifying that Dynamic vNICs Are Up and Running, page 77](#)
- [Verifying the Ethernet Data Path, page 78](#)
- [Verifying the Data Path for Fibre Channel Switch Mode, page 78](#)

Verifying that Dynamic vNICs Are Up and Running

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

Perform this step in the Cisco UCS Manager GUI.

Procedure

- Step 1** In the **Navigation** pane, click **VM**.
 - Step 2** On the **VM** tab, expand **All > VMware > Virtual Machines**.
 - Step 3** Expand the virtual machine for which you want to verify the dynamic vNICs and choose a dynamic vNIC.
 - Step 4** In the **Work** pane, click the **VIF** tab.
 - Step 5** On the **VIF** tab, verify that the **Status** column for each VIF is **Online**.
 - Step 6** Repeat Steps 3 through 5 until you have verified that the VIFs for all dynamic vNICs on all virtual machines have a status of **Online**.
-

Verifying the Ethernet Data Path

Procedure

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

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

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

Verifying the Data Path for Fibre Channel Switch Mode

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

Procedure

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

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

```
UCS-A /fabric-interconnect # connect nxos a
UCS-A(nxos) # show flogi database
-----
INTERFACE          VSAN    FCID          PORT NAME          NODE NAME
-----
vfc726             800    0xef0003    20:00:00:25:b5:26:07:02  20:00:00:25:b5:26:07:00
vfc728             800    0xef0007    20:00:00:25:b5:26:07:04  20:00:00:25:b5:26:07:00
vfc744             800    0xef0004    20:00:00:25:b5:26:03:02  20:00:00:25:b5:26:03:00
vfc748             800    0xef0005    20:00:00:25:b5:26:04:02  20:00:00:25:b5:26:04:00
vfc764             800    0xef0006    20:00:00:25:b5:26:05:02  20:00:00:25:b5:26:05:00
vfc768             800    0xef0002    20:00:00:25:b5:26:02:02  20:00:00:25:b5:26:02:00
vfc772             800    0xef0000    20:00:00:25:b5:26:06:02  20:00:00:25:b5:26:06:00
vfc778             800    0xef0001    20:00:00:25:b5:26:01:02  20:00:00:25:b5:26:01:00

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




PART **II**

Managing Firmware through Cisco UCS Central

- [Downloading and Managing Firmware in Cisco UCS Central, page 83](#)
- [Upgrading Firmware in Cisco UCS Domains through Cisco UCS Central, page 89](#)
- [Managing the Capability Catalog in Cisco UCS Central, page 97](#)



CHAPTER 12

Downloading and Managing Firmware in Cisco UCS Central

This chapter includes the following sections:

- [Downloading Firmware from Cisco.com](#) , page 83
- [Firmware Library of Images](#), page 84
- [Configuring Firmware Download from Cisco](#), page 84
- [Downloading a Firmware Image from Cisco](#), page 85
- [Downloading Firmware from a Remote Location](#), page 85
- [Downloading Firmware from a Local File System](#), page 86
- [Viewing Image Download Faults](#), page 86
- [Viewing Firmware Images in the Library](#), page 87
- [Deleting Image Metadata from the Library of Images](#), page 87

Downloading Firmware from Cisco.com

You can configure Cisco UCS Central to communicate with the Cisco website at specified intervals to fetch the firmware image list. After configuring Cisco credentials for image download, when you refresh, Cisco UCS Central fetches the available image data from Cisco.com and displays the firmware image in the firmware image library. You can download the actual firmware images when creating a policy using the firmware image version or when downloading the image using the **Store Locally** option.



Important

Make sure that you create a Cisco.com account to download firmware from Cisco.com to Cisco UCS Central.

**Note**

If you change users in the Cisco.com account, this causes a full synchronization of the Image Library. Download operations are unavailable while it is synchronizing. This can take up to 15 minutes, depending on the size of the library.

Firmware Library of Images

Image Library in Cisco UCS Central displays a list of all firmware images downloaded into Cisco UCS Central from Cisco.com, local file system and remote file system.

The source for images downloaded from Cisco.com is Cisco and for images downloaded from local or remote file system is local. These firmware images are available for creating firmware policies.

The following are the options to delete firmware images from the library:

- **Deleting the firmware image** — You can delete any downloaded image in the firmware library using the delete option.
- **Purging the firmware image metadata** — You can delete the image metadata using the purge option. Even after you delete the firmware image from the library, the metadata will still exist. You can use the metadata information to download the actual firmware image anytime from Cisco.com even after deleting the image. If you want to completely remove the firmware image and associated metadata from the firmware image library, make sure to delete the actual firmware image and purge the metadata from the library.

**Important**

If you have already downloaded the image corresponding to the metadata into the firmware image library, you cannot purge the metadata without deleting the image.

Configuring Firmware Download from Cisco

When you configure firmware download from Cisco, Cisco UCS Central downloads the firmware metadata from Cisco.com and keeps the information available for you to download and save anytime from Cisco UCS Central.

Procedure

- Step 1** On the menu bar, click **Operations Management**.
- Step 2** In the **Navigation** pane, expand **Images**.
- Step 3** Click **Configure Downloads From Cisco**.
- Step 4** In the **Work** pane, **General** tab, fill in the fields with the required information. Make sure to have the username and password for the Cisco.com account that Cisco UCS Central uses to log in.
- Step 5** In the **Proxy** tab, fill in the required information for the proxy account.

Step 6 Click **Save**.

Downloading a Firmware Image from Cisco

When you configure firmware image download from Cisco.com and refresh the library of images, Cisco UCS Central is able to access to all available firmware image metadata. You can download the firmware image in the following ways:

- **Creating a firmware policy** — When you create a firmware policy and select the specific image, Cisco UCS Central automatically downloads the image specified in the firmware policy.
- **Storing the image locally** — When you select the store locally option, the selected firmware image is downloaded from Cisco.com and stored in the image library.

This procedure describes the process to download the image using store locally option.

Procedure

- Step 1** On the menu bar, click **Operations Management**.
 - Step 2** In the **Navigation** pane, expand **Images**.
 - Step 3** Click **Library**.
 - Step 4** In the **Work** pane, click **Packages** tab.
The image metadata downloaded from Cisco will have the **Source** as **Cisco** and **State** as **not-downloaded**.
 - Step 5** Right click on the bundle and from the options, choose **Store Locally**.
-

Downloading Firmware from a Remote Location

Before You Begin

You must have the remote server configured to support the file transfer protocol that you choose and they must be accessible to Cisco UCS Central.

Procedure

- Step 1** On the menu bar, click **Operations Management**.
 - Step 2** In the **Navigation** pane, expand **Images**.
 - Step 3** Click **Library**.
 - Step 4** In the **Work** pane, click **Downloads** tab.
 - Step 5** In the **Downloads** tab, click **Download Firmware**.
 - Step 6** In the **Download Firmware** dialog box, **Location of the Image File**, choose **Remote File System** and fill in the required fields.
 - Step 7** Click **OK**.
-

Downloading Firmware from a Local File System

Before You Begin

You must have obtained and saved the firmware image from Cisco in your local file system to configure downloading the firmware from local system into Cisco UCS Central.

Procedure

- Step 1** On the menu bar, click **Operations Management**.
 - Step 2** In the **Navigation** pane, expand **Images**.
 - Step 3** Click **Library**.
 - Step 4** In the **Work** pane, click **Downloads** tab.
 - Step 5** In the **Downloads** tab, click **Download Firmware**.
 - Step 6** In the **Download Firmware** dialog box, **Location of the Image File**, choose **Local File System**.
 - Step 7** Click **Download Image into Image Library**.
A dialog box opens with an option to select the file.
 - Step 8** Click **Browse** to browse to the firmware file location in your local system and select the file.
 - Step 9** Click **Submit**.
If the image download is successful, **Firmware Image Download** dialog box opens with a confirmation message.
 - Step 10** In the **Firmware Image Download** dialog box, click **OK**.
-

Viewing Image Download Faults

You can view the faults in firmware image download process from the same **Library of Images** panel.

Procedure

- Step 1** On the menu bar, click **Operations Management**.
 - Step 2** In the **Navigation** pane, expand **Images**.
 - Step 3** Click **Library**.
 - Step 4** In the **Work** pane, click **Faults** tab.
The faults table displays all download faults with details.
-

Viewing Firmware Images in the Library

You can view the downloaded firmware images and image metadata in the **Library of Images** panel.

Procedure

- Step 1** On the menu bar, click **Operations Management**.
 - Step 2** In the **Navigation** pane, expand **Images**.
 - Step 3** Click **Library**.
 - Step 4** The **Work** pane click the **Packages** tab.
The available packages are displayed. You can select a package and click **Properties** to view details on specific packages.
-

Deleting Image Metadata from the Library of Images

You can delete the firmware image metadata from the **Library of Images** using the purge option. The purge option clears only the metadata of already downloaded images.



- Note** If you want to delete any of the firmware packages such as the capability catalog, infrastructure and host firmware packages, you can do so from the firmware management section under each domain groups or from the domain group root.
-

Procedure

- Step 1** On the menu bar, click **Operations Management**.
 - Step 2** In the **Navigation** pane, expand **Images**.
 - Step 3** Click **Library**.
 - Step 4** In the **Work** pane, choose the firmware image metadata you want to delete from **Library of Images** and click **Purge**.
 - Step 5** If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.
-



CHAPTER 13

Upgrading Firmware in Cisco UCS Domains through Cisco UCS Central

This chapter includes the following sections:

- [Firmware Upgrades for Cisco UCS Domains, page 89](#)
- [Configuring an Infrastructure Firmware Upgrade for a Cisco UCS Domain, page 89](#)
- [Acknowledging a Pending Activity, page 90](#)
- [Deleting an Infrastructure Firmware Package, page 91](#)
- [Creating a Host Firmware Package, page 91](#)
- [Deploying a Host Firmware Upgrade, page 92](#)
- [Deleting a Host Firmware Package, page 93](#)
- [Scheduling Firmware Upgrades, page 93](#)

Firmware Upgrades for Cisco UCS Domains

You can deploy infrastructure and server firmware upgrades for registered Cisco UCS domains from Cisco UCS Central.

If desired, you can upgrade the Cisco UCS domains in each domain group with different versions of firmware. Cisco UCS Central also provides you the option to acknowledge the fabric interconnect reboot globally from Cisco UCS Central or individually from each Cisco UCS domain.

Configuring an Infrastructure Firmware Upgrade for a Cisco UCS Domain

You can create only one infrastructure firmware package for one Cisco UCS Domain group in Cisco UCS Central . The member Cisco UCS domains in a domain group will run the same infrastructure firmware version.



Note You can configure infrastructure firmware update from domain group root or at the domain group level. When you update the firmware at the domain group root level, all the domain groups under the root will get the same infrastructure firmware version.

Procedure

- Step 1** On the menu bar, click **Operations Management**.
 - Step 2** In the **Navigation** pane, expand **Domain Groups > Domain Groups Root > Firmware Management**.
 - Step 3** Click **Infrastructure Firmware**.
 - Step 4** In the **Work** pane, **Policies** tab, click **Create**.
 - Step 5** In the **Scheduler** area, specify a schedule to apply the infrastructure firmware on the Cisco UCS domains in the domain group.
 - Step 6** In the **Version** area, select the infrastructure firmware version.
Impacted Endpoints area displays the endpoints that will get impacted by the infrastructure firmware policy. During a firmware upgrade, these endpoints will be rebooted and will therefore be unavailable during part of the upgrade process.
 - Step 7** Click **Save**.
-

What to Do Next

Cisco UCS Central automatically creates two schedules for infrastructure firmware update and fabric interconnect reboot. These schedules are also updated in Cisco UCS Manager. Based on the schedule, the infrastructure firmware upgrade process begins in the registered Cisco UCS domains and generates the first acknowledge pending activities message in Cisco UCS Central. When you acknowledge the first pending activity, the components are updated with the specified infrastructure firmware package.

After the infrastructure firmware is updated, you will receive another pending activity notification. This acknowledgment prevents any accidental reboot of fabric interconnects. You have to acknowledge this pending activity to reboot the fabric interconnect and complete the infrastructure firmware upgrade.



Note If you have multiple domains in a domain group, you will have to acknowledge each pending activity for each Cisco UCS domain to complete the infrastructure firmware upgrade process.

Acknowledging a Pending Activity

if the service profiles in Cisco UCS domains use a global maintenance policy and global host firmware package, Cisco UCS Central provides you an option to enable user acknowledgment before deploying the firmware upgrade.

If you have created a maintenance policy with **User Ack** reboot policy, you must acknowledge the actual firmware upgrade in Cisco UCS Manager. If you have created a maintenance policy with a global schedule and enabled **User Ack**, you must acknowledge the actual upgrade for all Cisco UCS domains in Cisco UCS Central.



Note You can view and acknowledge pending activities from **Infrastructure Firmware** and **Host Firmware** sections. This procedure describes the process to acknowledge a pending activity from the host firmware section.

Procedure

- Step 1** On the menu bar, click **Operations Management**.
 - Step 2** In the **Navigation** pane, expand **Domain Groups > Domain Groups Root > Firmware Management**.
 - Step 3** In the **Work** pane, click **Pending Activities** tab.
 - Step 4** Choose the pending activity from the displayed list, right click and click **Acknowledge**.
-

Deleting an Infrastructure Firmware Package

Procedure

- Step 1** On the menu bar, click **Operations Management**.
 - Step 2** In the **Navigation** pane, expand **Domain Groups > Domain Groups Root > Firmware Management**.
 - Step 3** The **Work** pane displays a list of all created infrastructure firmware packages.
 - Step 4** Click **Delete**.
 - Step 5** If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.
-

Creating a Host Firmware Package

Procedure

- Step 1** On the menu bar, click **Servers**.
- Step 2** In the **Navigation** pane, expand **Servers > Policies > root**.
- Step 3** Click **Host Firmware Packages**.
- Step 4** In the **Work** pane, click **Create a Host FW Pack**.
- Step 5** In **Create a Host FW Pack** dialog box, fill in the following fields:
 - a) Fill in **Name** and **Description**.
 - b) In the **Blade Version** area, choose the blade server version.
 - c) In the **Rack Version** area, choose the rack server version.

d) In the **Modular Version** area, choose the modular server version.

- Step 6** The **Impacted Endpoints** dialog box displays the list of end points that will be affected by this host firmware policy.
During a firmware upgrade, these endpoints will be rebooted and will therefore be unavailable during part of the upgrade process
- Step 7** Click **OK**.
-

What to Do Next

The host firmware policy you create in Cisco UCS Central will be available for association to a service profile in a Cisco UCS Domain registered to a domain group.

Deploying a Host Firmware Upgrade

You can update all host firmware policies defined in Cisco UCS Central to specific B, C, and M bundles using the **Install Servers**.

Before You Begin

You must have created a host firmware package.

Procedure

- Step 1** On the menu bar, click **Operations Management**.
- Step 2** In the **Navigation** pane, expand **Domain Groups > Domain Groups Root > Firmware Management**.
- Step 3** Click **Host Firmware**.
- Step 4** In the **Work** pane, from the displayed list of host firmware packages, choose the firmware version you want to deploy.
- Step 5** Click **Install Servers** on the table header.
- Step 6** In the **Install Servers** dialog box, select **Blade Version**, **Rack Version**, **Modular Version** and **Impacted Endpoints**.
- Step 7** In **Upgrade host Firmware Warning** message dialog box, click **Yes**.
If the servers in the selected endpoints use the global host firmware upgrade policy, they will be upgraded with the host firmware package.
-

Deleting a Host Firmware Package

Procedure

-
- Step 1** On the menu bar, click **Servers**.
 - Step 2** In the **Navigation** pane, expand **Servers > Policies > root**.
 - Step 3** Click **Host Firmware Packages**.
 - Step 4** The **Work** pane displays a list of all created host firmware packages.
 - Step 5** Click and choose the host firmware package name you want to delete. The table header area shows action icons.
 - Step 6** Click **Delete**.
 - Step 7** If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.
-

Scheduling Firmware Upgrades

Firmware Upgrade Schedules

To upgrade firmware by domain groups in registered Cisco UCS domains, you can schedule upgrades from Cisco UCS Central in the following ways:

- As a one time occurrence
- As a recurring occurrence that recurs at designated intervals

If you configure the schedules for user acknowledgment, the fabric interconnect will not reboot without explicit acknowledgment.

Creating a Maintenance Policy

You can create the following types of maintenance policies for host firmware update in Cisco UCS Central:

- **Immediate** — The immediate option reboots the servers immediately without any user acknowledgment.
- **Timer-automatic** — In timer-automatic option, the server reboot will happen based on the schedule you select for this maintenance policy.



Important

If you use the timer automatic option, you must create a schedule in Cisco UCS Central to specify in the maintenance policy. When you create a schedule in Cisco UCS Central, you can acknowledge this scheduled maintenance policy only in Cisco UCS Central. Servers using this maintenance policy will reboot only during the maintenance window defined in the schedule. If user-ack is enabled in the schedule, then you must acknowledge the server reboot.

- **User-acknowledgment** — The user-ack option sends a pending activity notification in each Cisco UCS Domain before rebooting servers.



Important

The user-ack option provides Cisco UCS domains administrators the option to decide on rebooting servers in individual Cisco UCS domains at different times.

Procedure

- Step 1** On the menu bar, click **Operations Management**.
 - Step 2** In the **Navigation** Pane, expand **Domain Groups > Domain Group Root > Maintenance**.
 - Step 3** In the **Work** pane, click **Create Maintenance Policy**.
 - Step 4** In the **Create Maintenance Policy** dialog box, do fill in the required fields.
 - Step 5** Click **OK**.
-

What to Do Next

Associate the maintenance policy to a service profile in Cisco UCS Manager.

Creating a One Time Occurrence Schedule

Procedure

- Step 1** On the menu bar, click **Operations Management**.
 - Step 2** In the **Navigation** pane, expand **Domain Groups > Domain Groups Root > Schedules**.
 - Step 3** In the **Work** pane, click **Create Schedule**.
 - Step 4** In the **Create Schedule** dialog box, enter the details in the **Properties** area.
 - Step 5** Choose **One Time Occurrences** tab and click **Create One Time Occurrence**.
 - Step 6** In the **Create One Time Occurrence** dialog box, fill in the details.
 - Step 7** Click **OK**.
 - Step 8** Click **OK** in the **Create Schedule** dialog box.
The one time schedule you created is added to the **Schedules** table.
-

Creating a Recurring Occurrence Schedule

Procedure

- Step 1** On the menu bar, click **Operations Management**.
 - Step 2** In the **Navigation** pane, expand **Domain Groups > Domain Groups Root > Schedules**.
 - Step 3** In the **Work** pane, click **Create Schedule**.
 - Step 4** In the **Create Schedule** dialog box, enter the details in the **Properties** area.
 - Step 5** Choose **Recurring Occurrences** tab and click **Create Recurring Occurrence**.
 - Step 6** In the **Create Recurring Occurrence** dialog box, fill in the details.
 - Step 7** Click **OK**.
 - Step 8** Click **OK** in the **Create Schedule** dialog box.
The recurring schedule you created is added to the table.
-

Deleting a Firmware Upgrade Schedule

Procedure

- Step 1** On the menu bar, click **Operations Management**.
 - Step 2** In the **Navigation** pane, expand **Domain Groups > Domain Groups Root > Schedules**.
 - Step 3** The **Work** pane displays a list of all scheduled firmware events.
 - Step 4** Click and choose the schedule name you want to delete.
The table header area shows action icons.
 - Step 5** Click **Delete**.
 - Step 6** If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.
-



Managing the Capability Catalog in Cisco UCS Central

This chapter includes the following sections:

- [Capability Catalog, page 97](#)
- [Configuring a Capability Catalog Update for a Cisco UCS Domain, page 98](#)

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, and local disk. 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.

For information about which hardware components are dependent upon a particular catalog release, see the component support tables in the [Service Notes for the B- Series servers](#). For information about which components are introduced in a specific release, see the Cisco UCS [Release Notes](#).

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 Technical Assistance Center, 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* accessible through the *Cisco UCS B-Series Servers Documentation Roadmap* available at the following URL: <http://www.cisco.com/go/unifiedcomputing/b-series-doc>.

Configuring a Capability Catalog Update for a Cisco UCS Domain

You can create only one capability catalog per each Cisco UCS Domain group in Cisco UCS Central. All the member Cisco UCS domains of a group will run the same firmware version.



Note

You can configure capability catalog update from domain group root or at the domain group level. When you update the capability catalog at the domain group root level, if the domain groups under the root do not have a capability catalog defined, will get the same capability catalog version.

Procedure

- Step 1** On the menu bar, click **Operations Management**.
 - Step 2** In the **Navigation** pane, expand **Domain Groups > Domain Groups Root > Firmware Management**.
 - Step 3** Click **Capability Catalog**.
 - Step 4** In the **Work** pane, click **Create**.
 - Step 5** In the **Version** table, select the version of the capability catalog you want to associate with the Cisco UCS domains included in the selected Cisco UCS Central domain group.
The capability catalog version selected here overrides the version inherited from any parent groups, if an inherited version exists.
 - Step 6** Click **Save**.
-

Cisco UCS Central triggers the capability catalog update in the specified Cisco UCS domains.

