Upgrading Cisco UCS from Release 1.4(1) or 1.4(2) to Release 1.4(3)

First Published: June 23, 2011

Last Modified: February 20, 2012

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

Text Part Number: OL-25310-04

CONTENTS

Preface v

Audience v

Organization v

Conventions vi

Related Documentation vii

Documentation Feedback vii

Obtaining Documentation and Submitting a Service Request vii

Overview of Upgrading to Release 1.4(3) 1

Overview of Firmware 1

Firmware Image Management 2

Firmware Versions 3

Firmware Upgrade to Cisco UCS, Release 1.4 4

Required Order of Steps When Upgrading from Release 1.4(1) or 1.4(2) 5

Required Order of Steps for Adding a Cisco UCS B230 Server 6

Required Order of Steps for Integrating a Cisco UCS Rack-Mount Server 6

Cautions, Guidelines, and Best Practices for Upgrading Cisco UCS 6

Configuration Changes and Settings that Can Impact Upgrades 6

Hardware-Related Guidelines and Best Practices for Firmware Upgrades 7

Firmware- and Software-Related Best Practices for Upgrades 8

Outage Impacts of Direct Firmware Upgrades 10

Completing the Prerequisites for Upgrading the Firmware 13

Prerequisites for Upgrading and Downgrading Firmware 13

Creating an All Configuration Backup File 14

Verifying the Overall Status of the Fabric Interconnects 15

Verifying the High Availability Status and Roles of a Cluster Configuration 16

Verifying the Status of I/O Modules 16

Verifying the Status of Servers 17

Verifying the Status of Adapters on Servers in a Chassis 18

Downloading the Release 1.4 Firmware 19
Obtaining Software Bundles from Cisco 19
Downloading Firmware Packages to the Fabric Interconnect 20
Determining the Contents of a Firmware Package 22
Canceling an Image Download 22
Verifying Local Storage Space on a Fabric Interconnect 23
Checking the Available Space on a Fabric Interconnect 23
Deleting Firmware Packages from a Fabric Interconnect 23
Deleting Firmware Images from a Fabric Interconnect 24
Upgrading the Firmware to Release 1.4(3) 25
Required Order of Steps When Upgrading from Release 1.4(1) or 1.4(2) 25
Disabling Call Home 26
Updating the Firmware on the Adapters, CIMCs, and IOMs 27
Activating the Firmware on the Adapters and CIMCs 28
Activating the Board Controller Firmware on a Server 30
Activating the Cisco UCS Manager Software to Release 1.4 30
Activating the Firmware on the IOMs to Release 1.4 31
Activating the Fabric Interconnect Firmware for a Cluster Configuration 32
Activating the Firmware on a Subordinate Fabric Interconnect to Release 1.4 32
Verifying that the Data Path is Ready 33
Verifying that Dynamic vNICs Are Up and Running 33
Verifying the Ethernet Data Path 34
Verifying the Data Path for Fibre Channel End-Host Mode 34
Verifying the Data Path for Fibre Channel Switch Mode 35
Activating the Firmware on a Primary Fabric Interconnect to Release 1.4 36
Activating the Firmware on a Standalone Fabric Interconnect to Release 1.4 37
Updating Host and Management Firmware Packages 37
Effect of Updates to Host Firmware Packages and Management Firmware Packages 37
Updating a Management Firmware Package 40
Updating a Host Firmware Package 41
Enabling Call Home 42

Preface

This preface includes the following sections:

- Audience, page v
- Organization, page v
- Conventions, page vi
- Related Documentation, page vii
- Documentation Feedback, page vii
- Obtaining Documentation and Submitting a Service Request, page vii

Audience

This guide is intended primarily for those who need to upgrade an existing Cisco Unified Computing System (Cisco UCS) instance.

Organization

This document includes the following chapters:

Chapter	Title	Description
Chapter 1	Overview	Provides an overview of the upgrade to Cisco UCS to the specified release with UCS Manager GUI, including the required order of upgrade steps and other information you need to know before you begin.
Chapter 2	Completing the Prerequisites	Describes the prerequisites to the upgrade.
Chapter 3	Downloading the Firmware	Describes where to find the firmware that you need for the upgrade and how to download it to Cisco UCS Manager.

Chapter	Title	Description
Chapter 4	Upgrading the Firmware	Contains the procedures that you need to follow to complete the upgrade, in the required order.

Conventions

This document uses the following conventions:

Convention	Indication
bold font	Commands, keywords, GUI elements, and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
`courier`font	Terminal sessions and information that the system displays appear in `courier` font.
[ ]	Elements in square brackets are optional.
{x | y | z}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means *reader take note*.

Tip Means *the following information will help you solve a problem*.

Caution	Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.
Timesaver	Means *the described action saves time*. You can save time by performing the action described in the paragraph.
Warning	Means *reader be warned*. In this situation, you might perform an action that could result in bodily injury.

Related Documentation

A roadmap that lists all documentation for Cisco Unified Computing System (Cisco UCS) B-Series hardware and software is available at the following URL:

http://www.cisco.com/go/unifiedcomputing/b-series-doc

Documentation Feedback

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

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation.

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

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

CHAPTER 1

Overview of Upgrading to Release 1.4(3)

This chapter includes the following sections:

- Overview of Firmware, page 1
- Firmware Image Management, page 2
- Firmware Versions, page 3
- Firmware Upgrade to Cisco UCS, Release 1.4, page 4

Overview of Firmware

Cisco UCS uses firmware obtained from and certified by Cisco to support the endpoints in a Cisco UCS instance. Each endpoint is a component in the instance that requires firmware to function. The upgrade order for the endpoints in a Cisco UCS instance depends upon the upgrade path, but includes the following:

- Cisco UCS Manager
- I/O modules
- 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 instance.

Note Beginning with Cisco UCS, Release 1.4(1), Cisco is releasing firmware upgrades in multiple bundles, rather than one large firmware package. For more information see Firmware Image Management, on page 2.

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.

Note For more information about firmware management and upgrades of individual components, see the Cisco UCS Manager Configuration Guides.

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 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
- I/O module firmware

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 instance. 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 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 Versions

The firmware versions on an endpoint depend upon the type of endpoint. The endpoints physically located on a fabric interconnect have different versions than those physically located on a server or I/O module.

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

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

The following firmware version terminology is used in 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.

Firmware Upgrade to Cisco UCS, Release 1.4

The firmware upgrade to Cisco UCS, Release 1.4(3) from Release 1.4(2) should be planned with scheduled maintenance windows if necessary to accommodate data disruption of up to one minute for the servers to reboot after endpoint activation and the updated host firmware package is applied.

This firmware upgrade requires a combination of the following methods:

- Direct upgrade at the endpoints. For a cluster configuration with two fabric interconnects, a direct upgrade can be minimally disruptive to data traffic. However, it requires that the Cisco UCS instance does not include firmware policies for those endpoints that you upgrade directly. You cannot avoid disruption to traffic in a Cisco UCS instance with only one fabric interconnection.
- Upgrades to server endpoints through service profiles that include a host firmware package, a management firmware package, or both. This method is disruptive to data traffic and should be performed during a maintenance window.

Note Direct upgrade is not available for all endpoints, including the server BIOS, storage controller, HBA firmware, and HBA option ROM. You must upgrade those endpoints through the host firmware package included in the service profile associated with the server.

Required Order of Steps When Upgrading from Release 1.4(1) or 1.4(2)

Note If you do not follow this order, the firmware upgrade may fail and the servers may experience communication issues with Cisco UCS Manager.

The order of steps in this document and the recommended options minimize the disruption to data traffic. Therefore, when you upgrade from any version of release 1.4 to a later version of release 1.4, upgrade the components in the following order.

1. Download the following firmware images:
   - Cisco UCS Infrastructure Software Bundle—Required for all Cisco UCS instances.
   - Cisco UCS B-Series Blade Server Software Bundle—Required for all Cisco UCS instances that include blade servers.
   - Cisco UCS C-Series Rack-Mount Server Software Bundle—Only required for Cisco UCS instances 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.
2. (Optional) Disable Call Home—If the Cisco UCS instance includes Call Home or Smart Call Home, disable Call Home to ensure you do not receive unnecessary alerts when Cisco UCS Manager restarts components.
3. Update adapters, CIMC, and IOMs—If you prefer, you can upgrade the adapters in a host firmware package as part of the last upgrade step.
4. Activate adapters—Choose **Ignore Compatibility Check** and **Set Startup Version Only** when performing this step.
5. Activate CIMC—Choose **Ignore Compatibility Check** when performing this step.
6. Activate Cisco UCS Manager—Choose **Ignore Compatibility Check** when performing this step.
7. Activate I/O modules—Choose **Ignore Compatibility Check** and **Set Startup Version Only** when performing this step.
8. Activate subordinate fabric interconnect—Choose **Ignore Compatibility Check** when performing this step.
9. Verify that the data path has been restored.
10. Activate primary fabric interconnect—Choose **Ignore Compatibility Check** when performing this step.
11. Update management firmware package(s) for servers—You do not need to perform this step if you updated and activated the CIMC on the servers directly.
12. Update host firmware package(s) for servers—Must be the last firmware upgraded. We recommend that you upgrade the board controller firmware during this step to avoid an additional reboot of servers with that firmware. You must upgrade the following firmware in a host firmware package:
    - BIOS
    - Storage controller
    - Certain adapters

13 (Optional) Enable Call Home—If you disabled Call Home before the upgrading the firmware, enable Call Home.

Required Order of Steps for Adding a Cisco UCS B230 Server

When you add the first B230 server, you must perform the steps in the following order to add support in Cisco UCS Manager for the server:

1 If you have not already done so, upgrade the Cisco UCS instance to Release 1.4(1) or later.

2 Insert the blade server into the chassis as described in the server installation guide.

3 Wait for Cisco UCS Manager to discover the new server. If server discovery does not begin within a few minutes, acknowledge the server.

Note You do not need to update the Management Extensions or Capability Catalog to add a B230 server. The required support is included in each Cisco UCS, Release 1.4 infrastructure bundle.

Required Order of Steps for Integrating a Cisco UCS Rack-Mount Server

After you complete the upgrade of the existing Cisco UCS components, you can integrate a Cisco UCS rack-mount server. When you integrate a rack-mount server, you must perform the steps in the following order:

1 If you have not already done so, configure the rack server discovery policy in Cisco UCS Manager.

2 Follow the instructions in the server installation guide for installing and integrating a rack-mount server in a system managed by Cisco UCS Manager.

3 Wait for Cisco UCS Manager to discover the new server. If server discovery does not begin within a few minutes, acknowledge the server.

Cautions, Guidelines, and Best Practices for Upgrading Cisco UCS

Before you update the firmware for any endpoint in a Cisco UCS instance, consider the following cautions, guidelines, and best practices.

Configuration Changes and Settings that Can Impact Upgrades

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

All Connectivity May Be Lost During Upgrades if vNIC Failover and NIC Teaming Are Both Enabled

All connectivity may be lost during firmware upgrades if you have configured both **Enable Failover** on one or more vNICs and you have also configured NIC teaming/bonding at the host operating system level. Please design for availability by using one or the other method, but never both.

To determine whether you have enabled failover for one or more vNICs in a Cisco UCS Cisco UCS instance, verify the configuration of the vNICs within each service profile associated with a server. For more information, see the Cisco UCS Manager configuration guide for the release that you are running.

VLAN 4048 is Reserved in Releases 1.4(1) and Higher

As of Release 1.4(1), VLAN 4048 is a reserved VLAN. If your Cisco UCS instance is configured to use VLAN 4048, you must reconfigure that VLAN to use a different ID before you upgrade.

Impact of Upgrade to Release 1.3(1i) or Higher

An upgrade from an earlier Cisco UCS firmware release to release 1.3(1i) or higher has the following impact on the Protect Configuration property of the local disk configuration policy the first time servers are associated with service profiles after the upgrade:

Unassociated Servers

After you upgrade the Cisco UCS instance, the initial server association proceeds without configuration errors whether or not the local disk configuration policy matches the server hardware. Even if you enable the Protect Configuration property, Cisco UCS does not protect the user data on the server if there are configuration mismatches between the local disk configuration policy on the previous service profile and the policy in the new service profile.

Note If you enable the Protect Configuration property and the local disk configuration policy encounters mismatches between the previous service profile and the new service profile, all subsequent service profile associations with the server are blocked.

Associated Servers

Any servers that are already associated with service profiles do not reboot after the upgrade. Cisco UCS Manager does not report any configuration errors if there is a mismatch between the local disk configuration policy and the server hardware.

When a service profile is disassociated from a server and a new service profile associated, the setting for the Protect Configuration property in the new service profile takes precedence and overwrites the setting in the previous service profile.

Hardware-Related Guidelines and Best Practices for Firmware Upgrades

The hardware in a Cisco UCS instance can impact how you upgrade. Before you upgrade any endpoint, consider the following guidelines and best practices:

No Server or Chassis Maintenance

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

Avoid Replacing RAID-Configured Hard Disks Prior to Upgrade

Under the following circumstances, Cisco UCS Manager may scrub all data on a hard disk as part of the RAID synchronization process during an upgrade of the server firmware:

- The hard disks in the server are configured for RAID.
- One or more of the RAID-configured hard disks in the server are removed.
- The hard disk or disks are replaced with hard disks that are configured with a pre-existing RAID and the local disk configuration policy included in the service profile on the server is not used to configure those hard disks.
- The server firmware is upgraded, causing the server to reboot and Cisco UCS Manager to begin the RAID synchronization process.

If the original hard disks contained vital data that needs to preserved, avoid inserting new hard disks that are already configured for RAID.

Always Upgrade Cisco UCS Gen-2 Adapters through a Host Firmware Package

You cannot upgrade Cisco UCS Gen-2 adapters directly at the endpoints. You must upgrade the firmware on those adapters through a host firmware package.

Cannot Upgrade Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter

The firmware on the Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter (N20-AI0002), Intel-based adapter card, is burned into the hardware at manufacture. You cannot upgrade the firmware on this adapter.

Number of Fabric Interconnects

For a cluster configuration with two fabric interconnects, you can take advantage of the failover between the fabric interconnects and perform a direct firmware upgrade of the endpoints without disrupting data traffic. However, you cannot avoid disrupting data traffic for those endpoints which must be upgraded through a host or management firmware package.

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.

Firmware- and Software-Related Best Practices for Upgrades

Before you upgrade any endpoint, consider the following guidelines and best practices:

No Partial Upgrades

We recommend that all endpoints in a Cisco UCS instance be upgraded to the same firmware release. New functionality and changes within a firmware release for one endpoint may have dependencies upon the same functionality and changes within another endpoint. Therefore, a mix of firmware releases may cause performance or other issues during ordinary usage or may cause the update to fail.

Determine Appropriate Type of Firmware Upgrade for Each Endpoint

Some endpoints, such as adapters and the server CIMC, can be upgraded through either a direct firmware upgrade or a firmware package included in a service profile. The configuration of a Cisco UCS instance determines how you upgrade these endpoints. If the service profiles associated with the servers include a host firmware package, upgrade the adapters for those servers through the firmware package. In the same way, if the service profiles associated with the servers include a management firmware package, upgrade the CIMC for those servers through the firmware package.

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.

Do Not Activate All Endpoints Simultaneously in Cisco UCS Manager GUI

If you use Cisco UCS Manager GUI to update the firmware, do not select **ALL** from the **Filter** drop-down list in the **Activate Firmware** dialog box to activate all endpoints simultaneously. Many firmware releases and patches have dependencies that require the endpoints to be activated in a specific order for the firmware update to succeed. This order can change depending upon the contents of the release or patch. Activating all endpoints does not guarantee that the updates occur in the required order and can disrupt communications between the endpoints and the fabric interconnects and Cisco UCS Manager. For information about the dependencies in a specific release or patch, see the release notes provided with that release or patch.

Impact of Activation for Adapters and I/O Modules

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.

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.

Select Ignore Compatibility Check When Upgrading

During a direct upgrade to a newer release, we recommend that you choose **Ignore Compatibility Check**. Newer releases may have incompatible code with older releases. This option ensures that the upgrade can proceed and avoids compatibility issues.

Disable Call Home before Upgrading to Avoid Unnecessary Alerts (Optional)

When you upgrade a Cisco UCS instance, Cisco UCS Manager restarts the components to complete the upgrade process. This restart causes events that are identical to service disruptions and component failures that trigger Call Home alerts to be sent. If you do not disable Call Home before you begin the upgrade, you can ignore the alerts generated by the upgrade-related component restarts.

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 instance.

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. Console sessions are not 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.

CHAPTER 2

Completing the Prerequisites for Upgrading the Firmware

This chapter includes the following sections:

- Prerequisites for Upgrading and Downgrading Firmware, page 13
- Creating an All Configuration Backup File, page 14
- Verifying the Overall Status of the Fabric Interconnects, page 15
- Verifying the High Availability Status and Roles of a Cluster Configuration, page 16
- Verifying the Status of I/O Modules, page 16
- Verifying the Status of Servers, page 17
- Verifying the Status of Adapters on Servers in a Chassis, page 18

Prerequisites for Upgrading and Downgrading Firmware

All endpoints in a Cisco UCS instance 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.

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

- Review the Release Notes.
- 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 all servers, I/O modules, and adapters are fully functional. An inoperable server cannot be upgraded.

- Verify that the Cisco UCS instance 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.

Creating an All Configuration Backup File

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

For more information on backing up a Cisco UCS instance, see the *Cisco UCS Manager GUI Configuration Guide* and the *Cisco UCS Manager CLI Configuration Guide*.

Before You Begin

Obtain the backup server IP address and authentication credentials.

Procedure

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

Step 2 Click the **All** node.

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

Step 4 In the **Actions** area, click **Backup**.

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 instance includes any identities derived from pools that you need to preserve, check this check box.

  Identities such as MAC addresses, WWNNs, WWPNs, or UUIDS are assigned at runtime. If you do not want these identities to change after you import the backup file, you must check this check box. If you do not, these identities may be changed after the import and operations such as a PXE boot or a SAN boot may no longer function.
- **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**

- **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.
- **Remote File** 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:

a) If the operation does not display in the **Properties** area, click the operation in the **Backup Operations** table.
b) 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.

Verifying the Overall Status of the Fabric Interconnects

Procedure

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

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

Step 3 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 the **Equipment** tab.

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

Step 2 On the **Equipment** tab, 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 instance. However, you cannot upgrade the inoperable server.

Procedure

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

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	**ok**, **unassociated**, or any value that does not indicate a failure. If the value indicates a failure, such as **discovery-failed**, the endpoints on that server cannot be upgraded.
Operability column	**operable**

Step 5 If you need to verify that a server has been discovered, do the following:

a) Right-click the server for which you want to verify the discovery status and choose **Show Navigator**.

b) 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 the **Equipment** tab.

Step 2 On the **Equipment** tab, 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 instance. However, you cannot upgrade the inoperable adapter.

CHAPTER 3

Downloading the Release 1.4 Firmware

This chapter includes the following sections:

- Obtaining Software Bundles from Cisco, page 19
- Downloading Firmware Packages to the Fabric Interconnect, page 20
- Determining the Contents of a Firmware Package, page 22
- Canceling an Image Download, page 22
- Verifying Local Storage Space on a Fabric Interconnect, page 23

Obtaining Software Bundles from Cisco

Before You Begin

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

- Cisco UCS Infrastructure Software Bundle—Required for all Cisco UCS instances.
- Cisco UCS B-Series Blade Server Software Bundle—Required for all Cisco UCS instances that include blade servers.
- Cisco UCS C-Series Rack-Mount Server Software Bundle—Only required for Cisco UCS instances 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 **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 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 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:

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

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

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

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

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

What to Do Next

Download the software bundles to the fabric interconnect.

Downloading Firmware Packages to the Fabric Interconnect

You can use the same procedure to download a single firmware image to the fabric interconnect.

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 still finishes successfully. The images are synced to the other fabric interconnect when it comes back online.

Before You Begin

Obtain the required firmware bundles from Cisco.

Procedure

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

Step 2 Click the **Equipment** node.

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

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

Step 5 Click **Download Firmware**.

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

Name	Description
Protocol field	The protocol to use when communicating with the remote server. This can be one of the following: • **FTP** • **TFTP** • **SCP** • **SFTP** **Note** TFTP has a file size limitation of 32 MB. Because firmware bundles can be much larger than that, we recommend that you do not choose TFTP for firmware downloads.
Server field	If the file came from a remote server, this is the IP address or hostname of the remote server on which the files resides. If the file came from a local source, this field displays "local". **Note** If you use a hostname rather than an IP address, you must configure a DNS server in Cisco UCS Manager.
Filename field	The name of the firmware file.
Path field	The absolute path to the file on the remote server. If you use SCP, the absolute path is always required. If you use any other protocol, you may not need to specify a remote path if the file resides in the default download folder. For details about how your file server is configured, contact your system administrator.
User field	The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP.
Password field	The password for the remote server username. This field does not apply if the protocol is TFTP.

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

Step 7 Click **OK**.

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

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

What to Do Next

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

Determining the Contents of a Firmware Package

Procedure

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

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

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

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

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

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

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

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

Canceling an Image Download

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

Procedure

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

Step 2 Expand the **Equipment** node.

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

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

Verifying Local Storage Space on a Fabric Interconnect

Checking the Available Space on a Fabric Interconnect

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

Procedure

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

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

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

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

Step 5 Expand the **Local Storage Information** area.
When you download a firmware image bundle, a fabric interconnect needs at least twice as much available space as the size of the firmware image bundle. If the bootflash does not have sufficient space, delete the obsolete firmware, core files, and other unneeded objects from the fabric interconnect.

Deleting Firmware Packages from a Fabric Interconnect

Use this procedure if you want to delete an entire firmware package or bundle. If you prefer you can also delete one or more of the individual images in a package.

Procedure

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

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

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

Step 4 On the **Firmware Management** tab, click the **Packages** tab.

Step 5 In the table, click the package that you want to delete.
You can use the Shift key or Ctrl key to select multiple entries.

Step 6 Right-click the highlighted package or packages and choose **Delete**.

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

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

Deleting Firmware Images from a Fabric Interconnect

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

Procedure

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

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

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

Step 4 On the **Firmware Management** tab, click the **Images** tab.

Step 5 In the table, click the image that you want to delete.
You can use the Shift key or Ctrl key to select multiple entries.

Step 6 Right-click the highlighted image or images and choose **Delete**.

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

CHAPTER 4

Upgrading the Firmware to Release 1.4(3)

This chapter includes the following sections:

- Required Order of Steps When Upgrading from Release 1.4(1) or 1.4(2), page 25
- Disabling Call Home, page 26
- Updating the Firmware on the Adapters, CIMCs, and IOMs, page 27
- Activating the Firmware on the Adapters and CIMCs, page 28
- Activating the Board Controller Firmware on a Server, page 30
- Activating the Cisco UCS Manager Software to Release 1.4, page 30
- Activating the Firmware on the IOMs to Release 1.4, page 31
- Activating the Fabric Interconnect Firmware for a Cluster Configuration, page 32
- Activating the Firmware on a Standalone Fabric Interconnect to Release 1.4, page 37
- Updating Host and Management Firmware Packages, page 37
- Enabling Call Home, page 42

Required Order of Steps When Upgrading from Release 1.4(1) or 1.4(2)

Note If you do not follow this order, the firmware upgrade may fail and the servers may experience communication issues with Cisco UCS Manager.

The order of steps in this document and the recommended options minimize the disruption to data traffic. Therefore, when you upgrade from any version of release 1.4 to a later version of release 1.4, upgrade the components in the following order.

1 Download the following firmware images:

- Cisco UCS Infrastructure Software Bundle—Required for all Cisco UCS instances.

- Cisco UCS B-Series Blade Server Software Bundle—Required for all Cisco UCS instances that include blade servers.
- Cisco UCS C-Series Rack-Mount Server Software Bundle—Only required for Cisco UCS instances 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.

2. (Optional) Disable Call Home—If the Cisco UCS instance includes Call Home or Smart Call Home, disable Call Home to ensure you do not receive unnecessary alerts when Cisco UCS Manager restarts components.
3. Update adapters, CIMC, and IOMs—If you prefer, you can upgrade the adapters in a host firmware package as part of the last upgrade step.
4. Activate adapters—Choose **Ignore Compatibility Check** and **Set Startup Version Only** when performing this step.
5. Activate CIMC—Choose **Ignore Compatibility Check** when performing this step.
6. Activate Cisco UCS Manager—Choose **Ignore Compatibility Check** when performing this step.
7. Activate I/O modules—Choose **Ignore Compatibility Check** and **Set Startup Version Only** when performing this step.
8. Activate subordinate fabric interconnect—Choose **Ignore Compatibility Check** when performing this step.
9. Verify that the data path has been restored.
10. Activate primary fabric interconnect—Choose **Ignore Compatibility Check** when performing this step.
11. Update management firmware package(s) for servers—You do not need to perform this step if you updated and activated the CIMC on the servers directly.
12. Update host firmware package(s) for servers—Must be the last firmware upgraded. We recommend that you upgrade the board controller firmware during this step to avoid an additional reboot of servers with that firmware. You must upgrade the following firmware in a host firmware package:
    - BIOS
    - Storage controller
    - Certain adapters
13. (Optional) Enable Call Home—If you disabled Call Home before the upgrading the firmware, enable Call Home.

Disabling Call Home

This step is optional.

When you upgrade a Cisco UCS instance, Cisco UCS Manager restarts the components to complete the upgrade process. This restart causes events that are identical to service disruptions and component failures that trigger Call Home alerts to be sent. If you do not disable Call Home before you begin the upgrade, you can ignore the alerts generated by the upgrade-related component restarts.

Procedure

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

Step 2 On the **Admin** tab, expand **All** > **Communication Management** > **Call Home**.

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

Step 4 In the **Admin** area, click **off** in the **State** field.

Note If this field is set to **off**, Cisco UCS Manager hides the rest of the fields on this tab.

Step 5 Click **Save Changes**.

Updating the Firmware on the Adapters, CIMCs, and IOMs

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

Before You Begin

This procedure describes how to update the firmware on all of these endpoints in a Cisco UCS system simultaneously. Before you begin this procedure, answer the following questions to determine the appropriate type of upgrade for each of these endpoints:

- Are all endpoints configured with the same backup version? If yes, continue with the next question. If no, update all backup versions to the same firmware version before continuing.
- Does the service profile associated with one or more of the servers include a host or management firmware package? If yes, update the firmware for that server through the firmware packages. You can update all other firmware and servers through this procedure. If no, continue with the next question.

  If you want to update the firmware for a server directly, you must remove all host and management firmware packages from the associated service profiles. Removing the firmware from the host or management firmware package does not enable you to update them directly.
- Does the server include a Cisco UCS gen-2 adapter? If yes, you must update the adapter firmware for that server through the host firmware package. If no, you can use this procedure for that server.

Even if you answered yes to either of the last two questions above, you can use this procedure to update the I/O modules and any servers for which you answered no.

Procedure

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

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

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

Step 4 On the **Installed Firmware** subtab, 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 instance. This step may take a few minutes, depending upon 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, choose **ALL**.
If you would prefer to update one type of endpoint at a time, choose that endpoint from the **Filter** drop-down list.

b) From the **Set Version** drop-down list on the menu bar, choose the firmware version included in the Release 1.4(3) firmware bundle from the drop-down list.

c) Click **Apply** to begin the updates and leave the dialog box open so you can monitor the progress of the updates to each endpoint.
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 explicitly activate it. Cisco UCS Manager begins all updates at the same time. However, some updates may 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 When all updates are completed, click **OK**.

What to Do Next

Activate the firmware.

Activating the Firmware on the Adapters and CIMCs

This procedure ensures that the firmware activation for these endpoints causes minimal disruption to data traffic. If you do not activate the endpoints in the following order with the correct options configured, the endpoints may reboot and cause a temporary disruption in data traffic.

Caution Do not select **ALL** from the **Filter** drop-down list in the **Activate Firmware** dialog box to activate all endpoints simultaneously. Many firmware releases and patches have dependencies that require the endpoints to be activated in a specific order for the firmware update to succeed. This order can change depending upon the contents of the release or patch. Activating all endpoints does not guarantee that the updates occur in the required order and can disrupt communications between the endpoints, the fabric interconnects, and Cisco UCS Manager. For information about the dependencies in a specific release or patch, see the release notes provided with that release or patch.

This procedure continues directly from the previous one and assumes you are on the **Firmware Management** tab.

Procedure

Step 1 In the **Installed Firmware** tab, choose **Activate Firmware**.
If one or more of the selected endpoints are not configured with the desired version as the backup version, Cisco UCS Manager GUI does not display that version in the **Set Version** drop-down list. You must select the version from the **Startup Version** column for each individual endpoint.

Step 2 If the adapter firmware is not updated through a host firmware package in a service profile, do the following in the **Activate Firmware** dialog box to activate the adapter firmware:

a) From the **Filter** drop-down list, choose **Adapters**.
b) From the **Set Version** drop-down list, choose the firmware version included in the Release 1.4(3) firmware bundle.
c) Check the **Ignore Compatibility Check** check box.
The firmware for this release is not compatible with previous releases. Therefore, you must check the **Ignore Compatibility Check** check box to ensure that the activation succeeds.
d) Check the **Set Startup Version Only** check box.

Note 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.

e) Click **Apply**.
When the **Activate Status** column for all adapters displays **pending-next-boot** or **ready**, continue with Step 3.

Step 3 If the CIMC firmware is not updated through a management firmware package in a service profile, do the following in the **Activate Firmware** dialog box to activate the CIMC firmware:

a) From the **Filter** drop-down list, choose **CIMC**.
b) From the **Set Version** drop-down list, choose the firmware version included in the Release 1.4(3) firmware bundle.
If one or more of the selected endpoints are not configured with the desired version as the backup version, Cisco UCS Manager GUI does not display that version in the **Set Version** drop-down list. You must select the version from the **Startup Version** column for each individual endpoint.
c) Check the **Ignore Compatibility Check** check box.
d) Click **Apply**.

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.

When the **Activate Status** column for all CIMC components displays **ready** continue with Step 4.

Step 4 Click **OK**.

Activating the Board Controller Firmware on a Server

Only certain servers, such as the Cisco UCS B440 High Performance blade server and the Cisco UCS B230 blade server, have board controller firmware. The board controller firmware controls many of the server functions, including eUSBs, LEDs, and I/O connectors.

This procedure continues from the previous one and assumes that you are on the **Installed Firmware** tab.

Note This activation procedure causes the server to reboot. Depending upon whether or not the service profile associated with the server includes a maintenance policy, the reboot can occur immediately. To reduce the number of times a server needs to be rebooted during the upgrade process, we recommend that you upgrade the board controller firmware through the host firmware package in the service profile.

Procedure

Step 1 On the **Installed Firmware** subtab, click **Activate Firmware**.
Cisco UCS Manager GUI opens the **Update Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS instance. This step may take a few minutes, depending upon the number of chassis and servers.

Step 2 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 3 From the **Set Version** drop-down list on the menu bar of the **Activate Firmware** dialog box, choose the board controller firmware version included in the Release 1.4(3) firmware bundle.

Step 4 Check the **Ignore Compatibility Check** check box.

Step 5 Click **OK**.

Activating the Cisco UCS Manager Software to Release 1.4

This procedure continues directly from the previous one and assumes you are on the **Firmware Management** tab.

Procedure

Step 1 On the **Installed Firmware** subtab, click **Activate Firmware**.
Cisco UCS Manager GUI opens the **Update Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS instance. This step may take a few minutes, depending upon the number of chassis and servers.

Step 2 From the **Filter** drop-down list, choose **UCS Manager**.

Step 3 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 firmware version included in the Release 1.4 firmware bundle from the drop-down list.
b) Check the **Ignore Compatibility Check** check box.

Step 4 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.

Activating the Firmware on the IOMs to Release 1.4

This procedure ensures that the firmware activation for these endpoints causes minimal disruption to data traffic. If you do not activate the endpoints in the following order with the correct options configured, the endpoints may reboot and cause a temporary disruption in data traffic.

Caution Do not select **ALL** from the **Filter** drop-down list in the **Activate Firmware** dialog box to activate all endpoints simultaneously. Many firmware releases and patches have dependencies that require the endpoints to be activated in a specific order for the firmware update to succeed. This order can change depending upon the contents of the release or patch. Activating all endpoints does not guarantee that the updates occur in the required order and can disrupt communications between the endpoints, the fabric interconnects, and Cisco UCS Manager. For information about the dependencies in a specific release or patch, see the release notes provided with that release or patch.

This procedure continues directly from the previous one and assumes you are on the **Firmware Management** tab.

Procedure

Step 1 In the **Installed Firmware** tab, choose **Activate Firmware**.
If one or more of the selected endpoints are not configured with the desired version as the backup version, Cisco UCS Manager GUI does not display that version in the **Set Version** drop-down list. You must select the version from the **Startup Version** column for each individual endpoint.

Step 2 To activate the IOM firmware, do the following in the **Activate Firmware** dialog box:

a) From the **Filter** drop-down list, choose **IO Modules**.

b) From the **Set Version** drop-down list, select the firmware version included in the Release 1.4 firmware bundle.
c) Check the **Ignore Compatibility Check** check box.
d) Check the **Set Startup Version Only** check box.

Important 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.

e) Click **Apply**.

Step 3 When the **Activate Status** column for all IOMs displays **pending-next-boot**, click **OK**.

Activating the Fabric Interconnect Firmware for a Cluster Configuration

Activating the Firmware on a Subordinate Fabric Interconnect to Release 1.4

Before You Begin

Determine which fabric interconnect in the cluster is the subordinate fabric interconnect. For more information, see Verifying the High Availability Status and Roles of a Cluster Configuration, on page 16.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.
Step 2 On the **Equipment** tab, click the **Equipment** node.
Step 3 In the **Work** pane, click the **Firmware Management** tab.
Step 4 On the **Installed Firmware** subtab, click **Activate Firmware**.
Cisco UCS Manager GUI opens the **Update Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS instance. This step may take a few minutes, depending upon 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 menu bar, check the **Ignore Compatibility Check** check box.
Step 7 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 included in the Release 1.4 firmware bundle from the drop-down list in the **Startup Version** column.
b) In the **System** row, choose the firmware version included in the Release 1.4 firmware bundle from the drop-down list in the **Startup Version** column.
Step 8 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 instance is configured to permit traffic and port failover, data traffic fails over to the primary fabric interconnect and is not disrupted.

Step 9 Verify the high availability status of the subordinate fabric interconnect.

Note 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.

Verifying that the Data Path is Ready

Before you continue to the next step in the upgrade, you must verify that the data path for the new the primary fabric interconnect has been restored and is ready to handle data traffic.

Verifying that Dynamic vNICs Are Up and Running

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

Perform this step in the Cisco UCS Manager GUI.

Procedure

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

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

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

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

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

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

Verifying the Ethernet Data Path

Procedure

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

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

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

Verifying the Data Path for Fibre Channel End-Host Mode

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

Procedure

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

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

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

Total number of flogi = 3.

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

Verifying the Data Path for Fibre Channel Switch Mode

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

Procedure

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

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

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

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

Activating the Firmware on a Primary Fabric Interconnect to Release 1.4

This procedure continues directly from the previous one and assumes you are on the **Firmware Management** tab.

Before You Begin

Activate the subordinate fabric interconnect.

Procedure

Step 1 On the **Installed Firmware** subtab, click **Activate Firmware**.
Cisco UCS Manager GUI opens the **Update Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS instance. This step may take a few minutes, depending upon 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 menu bar, check the **Ignore Compatibility Check** check box.

Step 4 On the row of the **Activate Firmware** dialog box for the primary fabric interconnect, do the following:

a) In the **Kernel** row, choose the firmware version included in the Release 1.4 firmware bundle from the drop-down list in the **Startup Version** column.

b) In the **System** row, choose the firmware version included in the Release 1.4 firmware bundle from the drop-down list in the **Startup Version** column.

Step 5 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 instance 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 6 Verify the high availability status of the fabric interconnect.

Note 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 to Release 1.4

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.

Procedure

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

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

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

Step 4 On the **Installed Firmware** subtab, click **Activate Firmware**.
Cisco UCS Manager GUI opens the **Update Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS instance. This step may take a few minutes, depending upon the number of chassis and servers.

Step 5 From the **Filter** drop-down list, choose **Fabric Interconnects**.

Step 6 On the menu bar, check the **Ignore Compatibility Check** check box.

Step 7 On the row of the **Activate Firmware** dialog box for the fabric interconnect, do the following:

a) In the **Kernel** row, choose the firmware version included in the Release 1.4 firmware bundle from the drop-down list in the **Startup Version** column.

b) In the **System** row, choose the firmware version included in the Release 1.4 firmware bundle from the drop-down list in the **Startup Version** column.

Step 8 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 instance.

Updating Host and Management Firmware Packages

Effect of Updates to Host Firmware Packages and Management Firmware Packages

To update firmware through a host firmware package or a management firmware package, you need to update the firmware in the package. What happens after you save the changes to a host or management firmware package depends upon how the Cisco UCS instance is configured.

The following table describes the most common options for upgrading servers with a host or management firmware package.

Note Maintenance policies are available in Cisco UCS, Release 1.4 and later.

Service Profile	Maintenance Policy	Upgrade Actions
Host or management firmware package is not included in a service profile or an updating service profile template. OR You want to upgrade the firmware without making any changes to the existing service profile or updating service profile template.	No maintenance policy	After you update the firmware package, do one of the following: • To reboot and upgrade some or all servers simultaneously, follow the procedure in the Cisco UCS Manager configuration guides for the appropriate release to add the firmware package to one or more service profiles that are associated with servers or to an updating service profile template. • To reboot and upgrade one server at a time, do the following for each server: **1** Create a new service profile and include the firmware package in that service profile. **2** Dissociate the server from its service profile. **3** Associate the server with the new service profile. **4** After the server has been rebooted and the firmware upgraded, disassociate the server from the new service profile and associate it with its original service profile. **Caution** If the original service profile includes a scrub policy, this procedure may result in data loss when the disk or the BIOS is scrubbed upon association with the new service profile.

Service Profile	Maintenance Policy	Upgrade Actions
Host or management firmware package is included in one or more service profiles, and the service profiles are associated with one or more servers. OR Host or management firmware package is included in an updating service profile template, and the service profiles created from that template are associated with one or more servers.	No maintenance policy OR A maintenance policy configured for immediate updates.	The following occurs when you update the firmware package: **1** The changes to the firmware package take effect as soon as you save them. **2** Cisco UCS 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 reboots the servers and updates the firmware. All servers associated with service profiles that include the firmware package are rebooted at the same time.
Host or management firmware package is included in one or more service profiles, and the service profiles are associated with one or more servers. OR Host or management firmware package is included in an updating service profile template, and the service profiles created from that template are associated with one or more servers.	Configured for user acknowledgment	The following occurs when you update the firmware package: **1** Cisco UCS Manager 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 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 reboots the server and updates the firmware. A manual reboot of the servers does not cause Cisco UCS Manager 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.

Service Profile	Maintenance Policy	Upgrade Actions
Host or management firmware package is included in one or more service profiles, and the service profiles are associated with one or more servers. OR Host or management firmware package is included in an updating service profile template, and the service profiles created from that template are associated with one or more servers.	Configured for changes to take effect during a specific maintenance window.	The following occurs when you update the firmware package: **1** Cisco UCS Manager 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 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 reboots the server and updates the firmware. A manual reboot of the servers does not cause Cisco UCS Manager to apply the firmware package, nor does it cancel the scheduled maintenance activities.

Updating a Management Firmware Package

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

Before You Begin

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

Procedure

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

Step 2 On the **Servers** tab, expand **Servers** > **Policies**.

Step 3 Expand the node for the organization that includes the policy you want to update.
If the system does not include 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 table on the right, do the following to delete the existing entry for the firmware you want to update:

a) Select the line in the table for the firmware version that you want to change.

b) Right-click and select **Delete**.

c) Click **Yes** to confirm that you want to delete that entry.

Step 7 In the **CIMC Firmware Packages** section on the left:

a) Click the down arrows to expand the section.
By default, the entries in a section are sorted by vendor name. To sort the entries, click on a column heading.

b) Select the line in the table which lists the firmware version for the release that you want to add to the firmware package.
The firmware version must match the model numbers (PID) on the servers that are associated with the firmware package . If you select a firmware version with the wrong model number, Cisco UCS Manager cannot install the firmware update.

c) Drag the line to the table on the right.

d) Click **Yes** to confirm that you selected the correct version.

Step 8 If you need to include CIMC firmware for servers with different model numbers (PIDs) in this management firmware package, repeat Step 6.

Step 9 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 Host Firmware Package

You must upgrade the BIOS and storage controller firmware through the host firmware package when you upgrade to Release 1.4(3). If you do not upgrade those packages, the servers may experience communication issues with Cisco UCS Manager and the CIMC.

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

This procedure assumes that the host firmware package already exists and that you have upgraded Cisco UCS Manager to Release 1.4(2). For information on how to create a host firmware package or on how to update an existing one in a previous release , see the appropriate *Cisco UCS Manager GUI Configuration Guide* for the release that Cisco UCS Manager is running.

Before You Begin

Before you update a host firmware package, do the following:

- Upgrade Cisco UCS Manager and the fabric interconnects.
- Determine an appropriate maintenance window to reduce the impact of the disruption of data traffic when the server reboots.
- Ensure you know the firmware version and model number (PID) for the servers or servers.

Procedure

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

Step 2 On the **Servers** tab, expand **Servers** > **Policies**.

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

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

Step 5 On each subtab of the **General** tab, do the following for each type of firmware you want to include in the package:

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

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

c) In the **Version** column, choose the firmware version from the Release 1.4(3) firmware image.

Step 6 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.

What to Do Next

Verify that the firmware on the endpoints included in the host firmware package has been updated to Release 1.4(3). If the firmware has not been updated, check the model numbers and vendors in the host firmware package against those on the endpoints that were not updated.

Enabling Call Home

This step is optional. You only need to enable Call Home if you disabled it before you began the firmware upgrades.

Procedure

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

Step 2 On the **Admin** tab, expand **All** > **Communication Management** > **Call Home**.

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

Step 4 In the **Admin** area, click **on** in the **State** field.

Note If this field is set to **On**, Cisco UCS Manager GUI displays the rest of the fields on this tab.

Step 5 Click **Save Changes**.