



Upgrading Cisco UCS from Release 1.0(1) to Release 1.1(1)

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-21890-01

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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0910R)

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

© 2010 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface v

Audience v

Organization v

Conventions vi

Related Documentation vii

Documentation Feedback vii

Obtaining Documentation and Submitting a Service Request viii

Overview of Upgrading from Cisco UCS, Release 1.0(1) 1

Overview of Firmware 1

Firmware Upgrade to Cisco UCS, Release 1.1(1) 2

Required Order of Steps When Upgrading from Release 1.0(1) to Release 1.1(1) 2

Guidelines and Cautions for Upgrading to Cisco UCS, Release 1.1(1) 3

Firmware Versions 4

Direct Firmware Upgrade at Endpoints 5

Stages of a Direct Firmware Upgrade 5

Outage Impacts of Direct Firmware Upgrades 6

Firmware Upgrades through Service Profiles 7

Host Firmware Package 8

Management Firmware Package 8

Stages of a Firmware Upgrade through Service Profiles 9

Firmware Downgrades 9

Completing the Prerequisites for Upgrading the Firmware 11

Prerequisites for Upgrading and Downgrading Firmware 11

Creating an All Configuration Backup File 12

Verifying the Overall Status of the Fabric Interconnects 13

Verifying the High Availability Status and Roles of a Cluster Configuration 14

Verifying the Status of I/O Modules 14

Verifying the Status of Servers 15

Verifying the Status of Adapters on Servers in a Chassis	16
Downloading the Firmware Image	17
Obtaining the Cisco UCS Release 1.1(1) Image Bundle from Cisco	17
Downloading Images to the Fabric Interconnect	18
Determining the Contents of a Firmware Package	19
Canceling an Image Download	20
Checking the Available Space on a Fabric Interconnect	20
Deleting Firmware from a Fabric Interconnect	20
Upgrading the Firmware from Release 1.0(1) to Release 1.1(1)	23
Required Order of Steps When Upgrading from Release 1.0(1) to Release 1.1(1)	23
Updating the Firmware on the Adapters, BMCs, and IOMs	24
Activating the Firmware on the Adapters, BMCs, and IOMs	25
Activating the Fabric Interconnect Firmware for a Cluster Configuration	26
Activating the Firmware on a Subordinate Fabric Interconnect to Release 1.1(1)	26
Activating the Firmware on a Primary Fabric Interconnect to Release 1.1(1)	27
Activating the Firmware on a Standalone Fabric Interconnect to Release 1.1(1)	28
Activating the Cisco UCS Manager Software to Release 1.1(1)	29
Updating a Host Firmware Package to Release 1.1(1)	30



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 viii](#)

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 Unified Computing System (Cisco UCS), Release 1.1(1) 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 .
<i>italic font</i>	Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic 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.
courier font	Terminal sessions and information the system displays appear in <code>courier font</code> .
<>	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

Documentation for Cisco Unified Computing System (Cisco UCS) is available at the following URL:

<http://www.cisco.com>

The following are related Cisco UCS documents:

- *Cisco UCS B-Series Servers Documentation Roadmap*
- *Upgrading Cisco UCS from Release 1.0(1) to Release 1.1(1)*
- *Upgrading Cisco UCS from Release 1.0(2) to Release 1.1(1)*
- *Cisco UCS Manager GUI Configuration Guide*
- *Cisco UCS Manager CLI Configuration Guide*
- *Cisco UCS Manager XML API Programmer's Guide*
- *Cisco UCS Manager Troubleshooting Guide*
- *Cisco UCS Site Preparation Guide*
- *Cisco UCS 6100 Series Fabric Interconnect Hardware Installation Guide*
- *Cisco UCS 5108 Server Chassis Hardware Installation Guide*
- *Regulatory Compliance and Safety Information for Cisco UCS*
- *Release Notes for Cisco UCS*

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.

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, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

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.



CHAPTER 1

Overview of Upgrading from Cisco UCS, Release 1.0(1)

This chapter includes the following sections:

- [Overview of Firmware, page 1](#)
- [Firmware Upgrade to Cisco UCS, Release 1.1\(1\), page 2](#)
- [Firmware Downgrades, page 9](#)

Overview of Firmware

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

- Endpoints physically located on servers, such as the BIOS, storage controller (RAID controller), and baseboard management controller (BMC)
- Endpoints physically located on adapters, including NIC and HBA firmware, and Option ROM (where applicable)
- I/O modules
- Fabric interconnects
- Cisco UCS Manager

Cisco maintains a set of best practices for managing firmware images and updates in 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.

Firmware Upgrade to Cisco UCS, Release 1.1(1)

The firmware upgrade to Cisco UCS, Release 1.1(1) must be planned with scheduled maintenance windows. With this firmware upgrade, you should expect the following:

- With a cluster configuration, data traffic disruption of up to one minute. Failover between the fabric interconnects prevents the longer disruption required for the fabric interconnects and I/O modules to reboot.
- With a standalone fabric interconnect, data traffic disruption of up to one minute for the servers to reboot and approximately ten minutes for the fabric interconnect and I/O module to reboot.

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 1.0(1) to Release 1.1(1)

When you upgrade from Cisco UCS, Release 1.0(1) to Release 1.1(1), upgrade the components in the following order. If you do not follow this order, the firmware upgrade may fail and the servers may experience communication issues with Cisco UCS Manager. In addition, the order of steps in this document and the recommended options minimize the disruption to data traffic.

- 1 Adapter (interface card)—If you plan to upgrade the adapters directly, perform this step first. However, if you prefer, you can omit this step and upgrade the adapters as part of the last step, in a host firmware package.
- 2 BMC—If you upgrade the adapters in the host firmware package, perform this step first.
- 3 I/O module.
- 4 Fabric interconnect.
- 5 Cisco UCS Manager.
- 6 Host firmware package—Must be the last step in the upgrade process. You must upgrade the BIOS and storage controller firmware during this step.

Guidelines and Cautions for Upgrading to Cisco UCS, Release 1.1(1)

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

Determine Appropriate Type of Firmware Upgrade for Each Endpoint

Some endpoints, such as adapters and the server BMC, 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 BMC for those servers through the firmware package.

Upgrades of a BMC 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.

No Partial Upgrades

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

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.

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.

Do Not Activate All Endpoints Simultaneously

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

During a direct upgrade, you should configure **Set Startup Version Only** for an adapter or an I/O module. With this setting, the activated firmware moves into the pending-next-boot state, and the endpoint is not immediately rebooted. Cisco UCS Manager activates the firmware the next time the endpoint 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 moves into 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 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 it and the I/O module, Cisco UCS Manager automatically updates the I/O module with the firmware version that matches its own and then activates the firmware and reboots the I/O module again.

For more information about the impact of activation, see [Outage Impacts of Direct Firmware Upgrades](#), page 6.

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

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

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 BMC, I/O Modules, and Adapters

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

The following firmware version terminology is used in 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 recent activate. 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 BMC 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.

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 instance.

You can directly upgrade the firmware on the following endpoints:

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



Note

Upgrades of a BMC 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
- BMCs

- I/O modules

You can set the update as Startup Version Only to avoid rebooting the endpoint immediately. This allows you to perform the update at any time and then activate and reboot during a maintenance period.

**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.

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.

For Cisco UCS Manager and the fabric interconnects, only the activate stage occurs because the specified firmware image already exists on the fabric interconnect. During activation, 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 it and the I/O module, Cisco UCS Manager automatically updates the I/O module with the firmware version that matches its own 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 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 BMC Firmware Upgrade

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

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

Outage Impact of an Adapter Firmware 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.

Firmware Upgrades through Service Profiles

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

- Host Firmware Package policy
- Management Firmware Package policy

**Note**

You cannot 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.

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 includes the following firmware for server and adapter endpoints:

- Adapter firmware images
- Storage controller firmware images
- Fibre Channel adapter firmware images
- BIOS firmware images
- HBA Option ROM firmware images

**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.

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.

Prerequisites

This policy is not dependent upon any other policies. However, you must ensure that the appropriate firmware has been downloaded to the fabric interconnect. If the firmware image is not available when Cisco UCS Manager is associating a server with a service profile, Cisco UCS Manager ignores the firmware upgrade and completes the association.

Management Firmware Package

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 only includes the baseboard management controller (BMC) on the server. You do not need to use this package if you upgrade the BMC directly.

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

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

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

Prerequisites

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

Stages of a Firmware Upgrade through Service Profiles

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



Caution

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 and/or management firmware packages and include them in the appropriate firmware policies.
- 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. For a host firmware package, the server is rebooted to ensure that the endpoints are running the versions specified in the firmware package.

Existing Service Profile

If the service profile is already associated with a server, Cisco UCS Manager upgrades the firmware as soon as you save the changes to the host firmware packages. For a host firmware package, Cisco UCS Manager reboots the server as soon as the change is saved.

Firmware Downgrades

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



CHAPTER 2

Completing the Prerequisites for Upgrading the Firmware

This chapter includes the following sections:

- [Prerequisites for Upgrading and Downgrading Firmware, page 11](#)
- [Creating an All Configuration Backup File, page 12](#)
- [Verifying the Overall Status of the Fabric Interconnects, page 13](#)
- [Verifying the High Availability Status and Roles of a Cluster Configuration, page 14](#)
- [Verifying the Status of I/O Modules, page 14](#)
- [Verifying the Status of Servers, page 15](#)
- [Verifying the Status of Adapters on Servers in a Chassis, page 16](#)

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.

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 instance, complete the following prerequisites:

- 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 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 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:
- 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**, run a **show tech-support** command and contact Cisco Technical Support. Do not proceed with the firmware upgrade.

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, run a **show tech-support** command and contact Cisco Technical Support. Do not proceed with the firmware upgrade.

- 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, run a **show tech-support** command and contact Cisco Technical Support. Do not proceed with the firmware upgrade.

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 **Interface Cards** 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 Firmware Image

This chapter includes the following sections:

- [Obtaining the Cisco UCS Release 1.1\(1\) Image Bundle from Cisco](#), page 17
- [Downloading Images to the Fabric Interconnect](#), page 18
- [Determining the Contents of a Firmware Package](#), page 19
- [Canceling an Image Download](#), page 20
- [Checking the Available Space on a Fabric Interconnect](#), page 20
- [Deleting Firmware from a Fabric Interconnect](#), page 20

Obtaining the Cisco UCS Release 1.1(1) Image Bundle from Cisco

Procedure

- Step 1** In a web browser, navigate to <http://www.cisco.com>.
- Step 2** Under **Support**, click **Download Software**.
- Step 3** Click **Unified Computing**.
- Step 4** Enter your Cisco.com username and password to log in.
- Step 5** Click **Cisco Unified Computing System**.
- Step 6** Click **Unified Computing System (UCS) Complete Software Bundle**.
- Step 7** Under the **Latest Releases** folder, click the link for the latest 1.1(1) release.
The Release 1.1(1) image number is subject to change as a result of further maintenance releases and may include a different letter.
- Step 8** Click the Release Notes link to download the latest version of the Release Notes.
- Step 9** Click one of the following buttons and follow the instructions provided:
 - **Download Now**—Allows you to download the firmware image immediately

- **Add to Cart**—Adds the firmware image to your cart to be downloaded at a later time

Step 10 Follow the prompts to complete your download of the image.

Step 11 Read the Release Notes before upgrading Cisco UCS.

What to Do Next

Download the firmware image to the fabric interconnect.

Downloading Images to the Fabric Interconnect



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

Before You Begin

Obtain the firmware images from Cisco.

Procedure

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

Step 2 Click the **Equipment** node.

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

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

Step 5 Click **Download Firmware**.

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

Name	Description
Protocol field	The protocol to use when communicating with the remote server. This can be: <ul style="list-style-type: none"> • FTP • TFTP • SCP • SFTP <p>Note TFTP has a file size limitation of 32 MB. Because firmware bundles can be much larger than that, we recommend that you do not select TFTP for firmware downloads.</p>

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

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

Step 7 Click **OK**.

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

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

What to Do Next

Update the firmware on the endpoints.

Determining the Contents of a Firmware Package

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

Procedure

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

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 from a Fabric Interconnect

You cannot delete firmware packages from the **Packages** tab. Cisco UCS Manager removes the packages after you have deleted all images in the package.

Before You Begin

We recommend that you determine the contents of a firmware package before you delete the package and its contents.

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 Cisco UCS Manager displays a confirmation dialog box, click **Yes**.
-



CHAPTER 4

Upgrading the Firmware from Release 1.0(1) to Release 1.1(1)

This chapter includes the following sections:

- [Required Order of Steps When Upgrading from Release 1.0\(1\) to Release 1.1\(1\)](#), page 23
- [Updating the Firmware on the Adapters, BMCs, and IOMs](#), page 24
- [Activating the Firmware on the Adapters, BMCs, and IOMs](#), page 25
- [Activating the Fabric Interconnect Firmware for a Cluster Configuration](#), page 26
- [Activating the Firmware on a Standalone Fabric Interconnect to Release 1.1\(1\)](#), page 28
- [Activating the Cisco UCS Manager Software to Release 1.1\(1\)](#), page 29
- [Updating a Host Firmware Package to Release 1.1\(1\)](#), page 30

Required Order of Steps When Upgrading from Release 1.0(1) to Release 1.1(1)

When you upgrade from Cisco UCS, Release 1.0(1) to Release 1.1(1), upgrade the components in the following order. If you do not follow this order, the firmware upgrade may fail and the servers may experience communication issues with Cisco UCS Manager. In addition, the order of steps in this document and the recommended options minimize the disruption to data traffic.

- 1 Adapter (interface card)—If you plan to upgrade the adapters directly, perform this step first. However, if you prefer, you can omit this step and upgrade the adapters as part of the last step, in a host firmware package.
- 2 BMC—If you upgrade the adapters in the host firmware package, perform this step first.
- 3 I/O module.
- 4 Fabric interconnect.
- 5 Cisco UCS Manager.

- 6 Host firmware package—Must be the last step in the upgrade process. You must upgrade the BIOS and storage controller firmware during this step.

Updating the Firmware on the Adapters, BMCs, 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.

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 1.1(1) firmware bundle from the drop-down list.
 - c) Click **OK**.
If one or more endpoints are included in a host firmware package, Cisco UCS Manager GUI notifies you that it cannot update those endpoints. If you acknowledge that message, Cisco UCS Manager GUI updates the firmware for the remaining endpoints that are not included in host firmware packages.

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** (Optional) To monitor the progress of the update to a specific endpoint, right-click on the endpoint and choose **Show Navigator**.
Cisco UCS Manager GUI 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 may not indicate that the update has failed. The retry count also includes retries that occur when Cisco UCS Manager GUI retrieves the update status.

What to Do Next

Activate the firmware.

Activating the Firmware on the Adapters, BMCs, and IOMs

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.

The firmware for Cisco UCS, Release 1.1(1) is not compatible with previous releases. Therefore, you must check the **Ignore Compatibility Check** check box to ensure that the activation succeeds.



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 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.

This procedure continues directly from [Updating the Firmware on the Adapters, BMCs, and IOMs, page 24](#) 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:
- From the **Filter** drop-down list, choose **Interface Cards**.
 - From the **Set Version** drop-down list, choose the firmware version included in the Release 1.1(1) firmware bundle.
 - Check the **Ignore Compatibility Check** check box.
 - Check the **Set Startup Version Only** check box.
Note During a direct upgrade, you should configure **Set Startup Version Only** for an adapter or an I/O module. With this setting, the activated firmware moves into the pending-next-boot state, and the endpoint is not immediately rebooted. Cisco UCS Manager activates the firmware the next time the endpoint is rebooted. You cannot configure **Set Startup Version Only** for an adapter in the host firmware package.
 - Click **Apply**.
When the **Activate Status** column for all adapters displays **pending-next-boot** or **ready** continue with Step 3.
- Step 3** If the BMC 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 BMC firmware:

- a) From the **Filter** drop-down list, choose **BMC**.
- b) From the **Set Version** drop-down list, choose the firmware version included in the Release 1.1(1) 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 BMC 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 BMC components displays **ready** continue with Step 4.

Step 4 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 1.1(1) 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 it and the I/O module, Cisco UCS Manager automatically updates the I/O module with the firmware version that matches its own and then activates the firmware and reboots the I/O module again.
- e) Click **Apply**.
When the **Activate Status** column for all IOMs displays **pending-next-boot** or **ready** continue with Step 5.

Step 5 Click **OK**.

Activating the Fabric Interconnect Firmware for a Cluster Configuration

Activating the Firmware on a Subordinate Fabric Interconnect to Release 1.1(1)

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](#), page 14.

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:
- In the **Kernel** row, choose the firmware version included in the Release 1.1(1) firmware bundle from the drop-down list in the **Startup Version** column.
 - In the **System** row, choose the firmware version included in the Release 1.1(1) 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 then 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.
If the **High Availability Status** 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 to Release 1.1(1)

This procedure continues directly from [Activating the Firmware on a Subordinate Fabric Interconnect to Release 1.1\(1\)](#), page 26 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 subordinate fabric interconnect, do the following:
- In the **Kernel** row, choose the firmware version included in the Release 1.1(1) firmware bundle from the drop-down list in the **Startup Version** column.
 - In the **System** row, choose the firmware version included in the Release 1.1(1) 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 then 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.
If the **High Availability Status** 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 1.1(1)

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:
- In the **Kernel** row, choose the firmware version included in the Release 1.1(1) firmware bundle from the drop-down list in the **Startup Version** column.
 - In the **System** row, choose the firmware version included in the Release 1.1(1) firmware bundle from the drop-down list in the **Startup Version** column.
- Step 8** Click **OK**.
-

Cisco UCS Manager activates the firmware, and then 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.

Activating the Cisco UCS Manager Software to Release 1.1(1)

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:
- From the drop-down list in the **Startup Version** column, select the firmware version included in the Release 1.1(1) firmware bundle from the drop-down list.
 - Check the **Ignore Compatibility Check** check box.
 - Click **OK**.

Cisco UCS Manager disconnects all active sessions, logs out all users, and then activates the software. When the upgrade is complete, you are prompted to log back in.

Updating a Host Firmware Package to Release 1.1(1)

You must upgrade the BIOS and storage controller firmware through the host firmware package when you upgrade to Release 1.1(1). If you do not upgrade those packages, the servers may experience communication issues with Cisco UCS Manager and the BMC.



Caution

If the policy is included in one or more service profiles that is associated with a server, as soon as you save the host firmware package policy, Cisco UCS Manager updates and activates the firmware in the server and adapter with the new versions and reboots the server.

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 1.1(1) 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 multi-tenancy, expand the **root** node.
- Step 4** Expand **Host Firmware Packages** and select the policy you want to update.
- Step 5** In the table on the right, 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 6** On the **General** tab, click the down arrows to expand one or more of the following sections on the left:
 - **Adapter Firmware Packages**
 - **Storage Controller Firmware Packages**
 - **Fibre Channel Adapters Firmware Packages**
 - **BIOS Firmware Packages**
 - **HBA Option ROM Packages**
- Step 7** In each section for the endpoint to which you want to include firmware in the package:
 - a) Select the line in the table for the firmware version that you want to add to the pack.

By default, the entries are sorted by vendor name. To sort the entries, click on a column heading.

- b) Drag the line to the table on the right.

The firmware version must match the model numbers (PID) on the servers that are associated with this firmware pack. If you select a firmware version with the wrong model number, Cisco UCS Manager cannot install the firmware update.

For information on the specific firmware version to select for the release, see the [Release Notes](#) for that version.

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

Step 8 If you need to include firmware updates 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.

What to Do Next

Verify that the firmware on the endpoints included in the host firmware package has been updated to release 1.1(1). 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.

