Cisco UCS B-Series GUI Firmware Management Guide, Release 2.1

First Published: November 16, 2012

Last Modified: November 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-28300-02

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.

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

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.

CONTENTS

Preface

CHAPTER 1

CHAPTER 2

Preface

This preface includes the following sections:

Audience

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

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

Conventions

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.

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

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

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

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

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

Warning IMPORTANT SAFETY INSTRUCTIONS

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

SAVE THESE INSTRUCTIONS

Related Cisco UCS Documentation

Documentation Roadmaps

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

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

Other Documentation Resources

An ISO file containing all B and C-Series documents is available at the following URL: http://www.cisco.com/cisco/software/type.html?mdfid=283853163&flowid=25821. From this page, click **Unified Computing System (UCS) Documentation Roadmap Bundle**.

The ISO file is updated after every major documentation release.

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

Documentation Feedback

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

CHAPTER 1

Overview

This chapter includes the following sections:

Overview of Firmware

Cisco UCS uses firmware obtained from and certified by Cisco to support the endpoints in a Cisco UCS domain. Each endpoint is a component in the Cisco UCS domain that requires firmware to function. The upgrade order for the endpoints in a Cisco UCS domain 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 domain.

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 35.

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.

Cross-Version Firmware Support

Cisco UCS supports cross-version firmware support in the following way:

- Infrastructure firmware must be at the current release.
- Server firmware can be at one release prior to the infrastructure firmware.

For example, if you upgrade the infrastructure firmware to Cisco UCS, Release 2.1, you can have firmware on some or all of the servers in a Cisco UCS domain can remain at the most recent version of Cisco UCS, Release 2.0.

Important If you implement cross-version firmware, you must ensure that the configurations for the Cisco UCS domain are supported by the firmware version on the server endpoints. For example, the minimum power budget for the servers must be no lower than the minimum supported in Cisco UCS, Release 2.0. The lower budget supported in Cisco UCS, Release 2.1 is not supported for servers that are running Cisco UCS, Release 2.0 firmware.

Options for Firmware Upgrades

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

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

Upgrading a Cisco UCS domain through Cisco UCS Manager

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

- Upgrade infrastructure and servers with Auto Install—This option upgrades all infrastructure components in the first stage. Then you can upgrade all server endpoints through host firmware packages in the second stage.
- Upgrade servers through firmware packages in service profiles—This option enables you to upgrade all server endpoints in a single step, reducing the amount of disruption caused by a server reboot. You can combine this option with the deferred deployment of service profile updates to ensure that server reboots occur during scheduled maintenance windows.
- Direct upgrades of infrastructure and server endpoints—This option enables you to upgrade many infrastructure and server endpoints directly, including the fabric interconnects, I/O modules, adapters, and board controllers. However, 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.

Note The Cisco UCS Manager GUI does not allow you to choose options that a release does not support. If a Cisco UCS domain includes hardware that is not supported in the release to which you are upgrading, Cisco UCS Manager GUI does not display the firmware as an option for that hardware or allow you to upgrade to it.

Upgrading a Cisco UCS domain through Cisco UCS Central

If you have registered one or more Cisco UCS domains with Cisco UCS Central, you can manage and upgrade all firmware components in the domain through Cisco UCS Central. This option allows you to centralize the control of firmware upgrades and ensure that all Cisco UCS domains in your data center are the required levels.

You can use Cisco UCS Central to upgrade the capability catalog, infrastructure, and server endpoints in all registered Cisco UCS domains that are configured for global firmware management.

Firmware Upgrades through Auto Install

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

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

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

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

Note You cannot use Auto Install to upgrade either the infrastructure or the servers in a Cisco UCS domain if Cisco UCS Manager in that domain is at a release prior to Cisco UCS 2.1(1). However, if you upgrade Cisco UCS Manager to Release 2.1(1), you can use Auto Install to upgrade the remaining components in a Cisco UCS domain that is at Release 1.4 or higher.

Install Infrastructure Firmware

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

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

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

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

Install Server Firmware

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

- Cisco UCS B-Series Blade Server Software Bundle for all blade servers in the chassis.

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

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

Firmware Upgrades through Firmware Packages in Service Profiles

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

You cannot upgrade the firmware on an I/O module, fabric interconnect, or Cisco UCS Manager through service profiles. You must upgrade the firmware on those endpoints directly.

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

Host Firmware Package

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

- **Adapter**
- **CIMC**
- **BIOS**
- **Board Controller**
- **FC Adapters**
- **HBA Option ROM**
- **Storage Controller**

Tip You can include more than one type of firmware in the same host firmware package. For example, a host firmware package can include 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.

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

Management Firmware Package

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

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

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

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

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

Stages of a Firmware Upgrade through Firmware Packages in Service Profiles

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

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

New Service Profile

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

Firmware Package Policy Creation

During this stage, you create the host firmware packages.

Service Profile Association

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

Existing Service Profile

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

Effect of Updates to Firmware Packages in Service Profiles

To update firmware through a firmware package in a service profile, you need to update the firmware in the package. What happens after you save the changes to a firmware package depends upon how the Cisco UCS domain is configured.

The following table describes the most common options for upgrading servers with a firmware package in a service profile.

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

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

Firmware Management in Cisco UCS Central

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

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

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

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

Direct Firmware Upgrade at Endpoints

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

You can directly upgrade the firmware on the following endpoints:

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

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

Note Upgrades of a CIMC through a management firmware package or an adapter through a firmware package in the service profile associated with the server take precedence over direct firmware upgrades. You cannot directly upgrade an endpoint if the service profile associated with the server includes a firmware package. To perform a direct upgrade, you must remove the firmware package from the service profile.

Stages of a Direct Firmware Upgrade

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

Update

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

The update stage applies only to the following endpoints:

- Adapters
- CIMCs
- I/O modules

Caution Do not remove the hardware that contains the endpoint or perform any maintenance on it until the update process 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.

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

- Cisco UCS Manager
- Fabric interconnects
- Board controllers on those servers that support them

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

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

Outage Impacts of Direct Firmware Upgrades

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

Outage Impact of a Fabric Interconnect Firmware Upgrade

When you upgrade the firmware for a fabric interconnect, you cause the following outage impacts and disruptions:

- The fabric interconnect reboots.
- The corresponding I/O modules reboot.

Outage Impact of a Cisco UCS Manager Firmware Upgrade

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

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

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

Outage Impact of an I/O Module Firmware Upgrade

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

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

Outage Impact of a CIMC Firmware Upgrade

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

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

Outage Impact of an Adapter Firmware Upgrade

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

- The server reboots.
- Server traffic is disrupted.

Firmware Versions

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

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 Downgrades

You downgrade firmware in a Cisco UCS domain 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.

Note The Cisco UCS Manager GUI does not allow you to choose options that a release does not support. If a Cisco UCS domain includes hardware that is not supported in the release to which you are downgrading, Cisco UCS Manager GUI does not display the firmware as an option for that hardware or allow you to downgrade to it.

Firmware Downgrades and Auto Install

You cannot use Auto Install to downgrade a Cisco UCS domain to a Cisco UCS release that is earlier than Release 2.1.

Unsupported Features Must Be Removed Before Downgrade

If you plan to downgrade a Cisco UCS domain to an earlier release, you must first remove or unconfigure all features from the current release that are not supported in the earlier release.

Note If you attempt to downgrade without removing or unconfiguring all features that are not supported in the earlier release, the downgrade will fail with the following message: "This operation is not supported for UCSM version below 2.1."

For example, if you plan to downgrade a Cisco UCS domain from Cisco UCS, Release 2.1 to Release 2.0, you must first remove or unconfigure unsupported features, such as the following:

- iSCSI configurations, including iSCSI vNICs, from objects such as service profiles, service profiles templates, boot order policies, and LAN connectivity policies.
- VLAN port count optimization

For example, if you plan to downgrade a Cisco UCS domain from Cisco UCS, Release 2.1 to Release 1.4, you must first remove or unconfigure unsupported features, such as the following:

- iSCSI configurations, including iSCSI vNICs, from objects such as service profiles, service profiles templates, boot order policies, and LAN connectivity policies.
- FCoE uplink ports
- FCoE storage ports
- Unified uplink ports
- Appliance storage ports

Recommended Order of Steps for Firmware Downgrades

If you need to downgrade the firmware to an earlier release, we recommend that you do it in the following order:

1. Retrieve the configuration backup from the release to which you want to downgrade that you created when you upgraded to the current release.
2. Remove or unconfigure the features that are not supported in the release to which you want to downgrade.
3. Downgrade the Cisco UCS domain.

4 Perform an erase-config.

5 Import the configuration backup from the release to which you downgraded.

CHAPTER 2

Cautions, Guidelines, and Limitations

This chapter includes the following sections:

Cautions, Guidelines, and Limitations for Firmware Upgrades

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

Note The Cisco UCS Manager GUI does not allow you to choose options that a release does not support. If a Cisco UCS domain includes hardware that is not supported in the release to which you are upgrading, Cisco UCS Manager GUI does not display the firmware as an option for that hardware or allow you to upgrade to it.

Configuration Changes and Settings that Can Impact Upgrades

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

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

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

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

For a new installation of Cisco UCS release 2.0, the default VLAN IDs are as follows:

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

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

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

Note If a Cisco UCS domain uses one of the default VLAN IDs, which results in overlapping VLANs, you can change one or more of the default VLAN IDs to any VLAN ID that is not used or reserved. In release 2.0, VLANs with IDs from 3968 to 4047 are reserved.

VSANs with IDs in the Reserved Range are not Operational

A VSAN with an ID in the reserved range is not operational after an upgrade. Make sure that none of the VSANs configured in Cisco UCS Manager are in the reserved range, as follows:

- If you plan to use FC switch mode in a Cisco UCS domain, do not configure VSANs with an ID in the range from 3040 to 4078.
- If you plan to use FC end-host mode in a Cisco UCS domain, do not configure VSANs with an ID in the range from 3840 to 4079.

If a VSAN has an ID in the reserved range, change that VSAN ID to any VSAN ID that is not used or reserved.

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 domain, 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.

IQN Names Must Be Unique for Each iSCSI vNIC

Cisco UCS, Release 2.0(2) introduces the concepts of IQN pools. If a Cisco UCS domain is configured for iSCI boot, before you upgrade from Cisco UCS, Release 2.0(1) to Release 2.0(2), you must ensure that all iSCI vNICs used within a single service profile or across multiple service profiles have unique initiator names. Changing initiator names also involves storage side configuration, which is beyond the scope of this document.

Cisco provides a script for Cisco UCS PowerTool that identifies duplicate IQN names within a Cisco UCS domain. For more information, see Obtaining Cisco UCS PowerTool and Running the Duplicate IQN Script.

If you do not ensure that all iSCSI vNICs in a Cisco UCS domain are unique before you upgrade, Cisco UCS Manager raises a fault on the iSCSI vNICs to warn you that duplicate IQNs are present. For information on how to clear this fault and reconfigure the duplicate IQNs, see the Cisco UCS B-Series Troubleshooting Guide.

Impact of Upgrade from a Release Prior to Release 1.3(1i)

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 domain, 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 Limitations for Firmware Upgrades

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

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 Guidelines and Limitations for Upgrades

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

Determine the 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 domain 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.

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

When you upgrade a Cisco UCS domain, 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.

Cautions, Guidelines, and Limitations for Upgrading with Auto Install

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

Note These guidelines are specific to Auto Install and are in addition to those listed in Cautions, Guidelines, and Limitations for Firmware Upgrades, on page 17.

State of the Endpoints

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

- For a cluster configuration, verify that the high availability status of the fabric interconnects shows that both are up and running.
- For a standalone configuration, verify that the Overall Status of the fabric interconnect is Operable.
- For all endpoints to be upgraded, verify that they are in an Operable state.
- For all servers to be upgraded, verify that all the servers have been discovered and that discovery did not fail. Install Server Firmware will fail if any server endpoints cannot be upgraded.

Minimum Firmware Levels Required to Run Auto Install

A Cisco UCS domain must meet the following minimum firmware levels if you want to upgrade some or all of the endpoints with Auto Install:

- All endpoints must be Cisco UCS, Release 1.4 or later.
- All endpoints must run the latest firmware maintenance release or patch for that release.

For example, a Cisco UCS domain that is running Cisco UCS, Release 1.4 must be running Cisco UCS, Release 1.4(4j), and a Cisco UCS domain that is running Cisco UCS, Release 2.0 must be running 2.0(4a).

Cannot Upgrade Infrastructure and Server Firmware Simultaneously

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

Required Privileges

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

Privileges	Upgrade Tasks User Can Perform
admin	• Run Install Infrastructure Firmware • Run Install Server Firmware • Add, delete, and modify host firmware packages

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

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

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

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

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

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

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

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

Upgrading Server Firmware on Newly Added Servers

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

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

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

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

PART I

Managing Firmware through Cisco UCS Manager

CHAPTER 3

Completing the Prerequisites for Upgrading the Firmware

This chapter includes the following sections:

Prerequisites for Upgrading and Downgrading Firmware

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

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

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

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

- Review the Release Notes.

- Review the relevant Hardware and Software Interoperability Matrix to ensure the operating systems on all servers have the right driver levels for the release of Cisco UCS to which you plan to upgrade.
- Back up the configuration into an All Configuration backup file.
- For a cluster configuration, verify that the high availability status of the fabric interconnects shows that both are up and running.
- For a standalone configuration, verify that the Overall Status of the fabric interconnect is Operable.
- Verify that the data path is up and running. For more information, see Verifying that the Data Path is Ready.
- Verify that all servers, I/O modules, and adapters are fully functional. An inoperable server cannot be upgraded.
- Verify that the Cisco UCS domain does not include any critical or major faults. If such faults exist, you must resolve them before you upgrade the system. A critical or major fault may cause the upgrade to fail.
- Verify that all servers have been discovered. They do not need to be powered on or associated with a service profile.
- If you want to integrate a rack-mount server into the Cisco UCS domain, follow the instructions in the appropriate C-Series Rack-Mount Server Integration Guide for installing and integrating a rack-mount server in a system managed by Cisco UCS Manager.
- For Cisco UCS domains that are configured for iSCI boot, do the following before you upgrade to Cisco UCS, Release 2.0(2) or higher:
    - Ensure that all iSCI vNICs used within a single service profile or across multiple service profiles have unique initiator names.
    - If any iSCSI vNICs have the same initiator name, reconfigure the IQNs with unique initiator names.
    - Make the corresponding IQN initiator name changes on any network storage devices to ensure that the boot LUNs are visible to the new IQN.

Creating an All Configuration Backup File

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

Before You Begin

Obtain the backup server 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 domain 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 domain. 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 domain. However, you cannot upgrade the inoperable adapter.

CHAPTER 4

Downloading and Managing Firmware in Cisco UCS Manager

This chapter includes the following sections:

Firmware Image Management

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

Cisco UCS Infrastructure Software Bundle

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

- Cisco UCS Manager software
- Kernel and system firmware for the fabric interconnects
- 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 domain. In addition to the bundles created for a release, these bundles can also be released between infrastructure bundles to enable Cisco UCS Manager to support a blade server that is not included in the most recent infrastructure bundle.

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

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

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

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

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

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

Firmware Image Headers

Every firmware image has a header, which includes the following:

- Checksum
- Version information
- Compatibility information that the system can use to verify the compatibility of component images and any dependencies

Firmware Image Catalog

Cisco UCS Manager provides you with two views of the catalog of firmware images and their contents that have been downloaded to the fabric interconnect:

Packages

This view provides you with a read-only representation of the firmware bundles that have been downloaded onto the fabric interconnect. This view is sorted by image, not by the contents of the image. For packages, you can use this view to see which component images are in each downloaded firmware bundle.

Images

The images view lists the component images available on the system. You cannot use this view to see complete firmware bundles or to group the images by bundle. The information available about each component image includes the name of the component, the image size, the image version, and the vendor and model of the component.

You can use this view to identify the firmware updates available for each component. You can also use this view to delete obsolete and unneeded images. Cisco UCS Manager deletes a package after all images in the package have been deleted.

Tip Cisco UCS Manager stores the images in bootflash on the fabric interconnect. In a cluster system, space usage in bootflash on both fabric interconnects is the same, because all images are synchronized between them. If Cisco UCS Manager reports that the bootflash is out of space, delete obsolete images to free up space.

Obtaining Software Bundles from Cisco

Before You Begin

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

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

Procedure

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

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

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

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

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

Bundle	Navigation Path
Cisco UCS Infrastructure Software Bundle	Click **Cisco UCS Infrastructure and UCS Manager Software** > **Unified Computing System (UCS) Infrastructure Software Bundle**.
Cisco UCS B-Series Blade Server Software Bundle	Click **Cisco UCS B-Series Blade Server Software** > **Unified Computing System (UCS) Server Software Bundle**.
Cisco UCS C-Series Rack-Mount UCS-Managed Server Software Bundle	Click **Cisco UCS C-Series Rack-Mount UCS-Managed Server Software** > **Unified Computing System (UCS) Server Software Bundle**.

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

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

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

a) Click the link for the release you want to downloadthe latest release 2.0 software bundle.
The release number is followed by a number and a letter in parentheses. The number identifies the maintenance release level, and the letter differentiates between patches of that maintenance release. For more information about what is in each maintenance release and patch, see the latest version of the Release Notes.

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

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

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

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

What to Do Next

Download the software bundles to the fabric interconnect.

Downloading Firmware Images to the Fabric Interconnect from a Remote Location

Note In a cluster setup, the image file for the firmware bundle is downloaded to both fabric interconnects, regardless of which fabric interconnect is used to initiate the download. Cisco UCS Manager maintains all firmware packages and images in both fabric interconnects in sync. If one fabric interconnect is down, the download 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 On the **Equipment** tab, click the **Equipment** node.

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

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

Step 5 Click **Download Firmware**.

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

Step 7 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. If the Cisco UCS domain is not registered with Cisco UCS Central or DNS management is set to **local**, configure a DNS server in Cisco UCS Manager. If the Cisco UCS domain is registered with Cisco UCS Central and DNS management is set to **global**, configure a DNS server in Cisco UCS Central.
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.

Name	Description
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.

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

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

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

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

What to Do Next

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

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

Note In a cluster setup, the image file for the firmware bundle is downloaded to both fabric interconnects, regardless of which fabric interconnect is used to initiate the download. Cisco UCS Manager maintains all firmware packages and images in both fabric interconnects in sync. If one fabric interconnect is down, the download 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 On the **Equipment** tab, click the **Equipment** node.

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

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

Step 5 Click **Download Firmware**.

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

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

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

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

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

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

What to Do Next

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

Canceling an Image Download

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

Procedure

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

Step 2 Expand the **Equipment** node.

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

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

Determining the Contents of a Firmware Package

Procedure

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

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

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

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

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

a) Highlight the rows that include the image name and its contents.
b) Right-click and choose **Copy**.
c) Paste the contents of your clipboard into a text file or other document.

Checking the Available Space on a Fabric Interconnect

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

Procedure

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

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

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

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

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

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.

For releases prior to Cisco UCS, Release 1.3(1), you cannot delete firmware packages from the **Packages** tab. After you delete all images from the package, Cisco UCS Manager removes the packages.

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 5

Upgrading Firmware through Auto Install

This chapter includes the following sections:

Firmware Upgrades through Auto Install

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

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

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

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

Note You cannot use Auto Install to upgrade either the infrastructure or the servers in a Cisco UCS domain if Cisco UCS Manager in that domain is at a release prior to Cisco UCS 2.1(1). However, if you upgrade Cisco UCS Manager to Release 2.1(1), you can use Auto Install to upgrade the remaining components in a Cisco UCS domain that is at Release 1.4 or higher.

Install Infrastructure Firmware

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

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

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

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

Install Server Firmware

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

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

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

Required Order of Steps for Auto Install

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

1. Install Infrastructure Firmware
2. Install Server Firmware

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

Upgrading the Infrastructure Firmware with Auto Install

Before You Begin

Complete all prerequisites listed in Prerequisites for Upgrading and Downgrading Firmware, on page 27.

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

Procedure

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

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

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

Step 4 In the **Work** pane, click the **Firmware Auto Install** tab.

Step 5 In the **Actions** area, click **Install Infrastructure Firmware**.

Step 6 In the **Properties** area of the **Install Infrastructure Firmware** dialog box, complete the following fields:

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

Step 7 In the **Infrastructure Schedule** area of the **Install Infrastructure Firmware** dialog box, do one of the following:

Option	Description
Start Time field	The date and time that the occurrence will run. Click the down arrow at the end of the field to select the date from a calendar.

Option	Description
Upgrade Now check box	If checked, Cisco UCS Manager ignores the **Start Time** field and upgrades the infrastructure firmware as soon as you click **OK**.

Step 8 Click **OK**.
The **Firmware Installer** field on the **Firmware Auto Install** tab displays the status of the infrastructure firmware upgrade.

What to Do Next

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

Acknowledging the Reboot of the Primary Fabric Interconnect

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

Procedure

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

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

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

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

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

Canceling an Infrastructure Firmware Upgrade

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

Procedure

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

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

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

Step 4 In the **Work** pane, click the **Firmware Auto Install** tab.

Step 5 In the **Actions** area, click **Install Infrastructure Firmware**.

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

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

Step 8 Click **OK**.

Upgrading the Server Firmware with Auto Install

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

Before You Begin

Complete all prerequisites listed in Prerequisites for Upgrading and Downgrading Firmware, on page 27.

Procedure

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

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

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

Step 4 In the **Work** pane, click the **Firmware Auto Install** tab.

Step 5 In the **Actions** area, click **Install Server Firmware**.

Step 6 On the **Prerequisites** page of the **Install Server Firmware** wizard, carefully review the prerequisites and guidelines listed on this page and then do one of the following:

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

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

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

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

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

c) Click **Next**.

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

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

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

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

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

a) Click the appropriate check boxes to filter the results in the **Impacted Endpoints** table.
   You can filter the results by the type of endpoint and by whether the impact of the upgrade is disruptive or not.
b) Review the list of impacted endpoints.
c) If desired, click the link in the **Maintenance Policy** column to open the navigator for that policy.
d) Do one of the following:
   - If you want to change one or more of the selected host firmware packages, click **Prev**.
   - If you are satisfied that you have selected the appropriate host firmware packages and want to start the server upgrade, click **Install**.

Step 11 (Optional) To check on the progress of the server firmware upgrade, check the **FSM** tab for each server that you are upgrading.

The **Firmware Installer** field on the **Firmware Auto Install** tab shows only the status of an infrastructure firmware upgrade.

CHAPTER 6

Directly Upgrading Firmware at Endpoints

This chapter includes the following sections:

Direct Firmware Upgrade at Endpoints

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

You can directly upgrade the firmware on the following endpoints:

- Adapters

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

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

Note Upgrades of a CIMC through a management firmware package or an adapter through a firmware package in the service profile associated with the server take precedence over direct firmware upgrades. You cannot directly upgrade an endpoint if the service profile associated with the server includes a firmware package. To perform a direct upgrade, you must remove the firmware package from the service profile.

Stages of a Direct Firmware Upgrade

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

Update

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

The update stage applies only to the following endpoints:

- Adapters
- CIMCs
- I/O modules

Caution Do not remove the hardware that contains the endpoint or perform any maintenance on it until the update process 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.

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

- Cisco UCS Manager
- Fabric interconnects
- Board controllers on those servers that support them

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

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

Outage Impacts of Direct Firmware Upgrades

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

Outage Impact of a Fabric Interconnect Firmware Upgrade

When you upgrade the firmware for a fabric interconnect, you cause the following outage impacts and disruptions:

- The fabric interconnect reboots.
- The corresponding I/O modules reboot.

Outage Impact of a Cisco UCS Manager Firmware Upgrade

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

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

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

Outage Impact of an I/O Module Firmware Upgrade

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

- For a standalone configuration with a single fabric interconnect, data traffic is disrupted when the I/O module reboots. For a cluster configuration with two fabric interconnects, data traffic fails over to the other I/O module and the fabric interconnect in its data path.

- If you activate the new firmware as the startup version only, the I/O module reboots when the corresponding fabric interconnect is rebooted.
- If you activate the new firmware as the running and startup version, the I/O module reboots immediately.
- An I/O module can take up to ten minutes to become available after a firmware upgrade.

Outage Impact of a CIMC Firmware Upgrade

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

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

Outage Impact of an Adapter Firmware Upgrade

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

- The server reboots.
- Server traffic is disrupted.

Updating the Firmware on Multiple Endpoints

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

- Adapters
- CIMCs
- I/O modules

Caution Do not remove the hardware that contains the endpoint or perform any maintenance on it until the update process 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** tab, click **Update Firmware**.
Cisco UCS Manager GUI opens the **Update Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS domain. This step 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, select **ALL**.
If you want to update all endpoint firmware of a specific type, such as all adapters or server BIOS, select that type from the drop-down list.

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

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

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

Cisco UCS Manager copies the selected firmware image to the backup memory partition and verifies that the image is not corrupt. The image remains as the backup version until you 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 the endpoint and choose **Show Navigator**.
Cisco UCS Manager displays the progress in the **Update Status** area on the **General** tab. If the navigator has an **FSM** tab, you can also monitor the progress there. An entry in the **Retry #** field may not indicate that the update has failed. The retry count also includes retries that occur when Cisco UCS Manager retrieves the update status.

What to Do Next

Activate the firmware.

Updating the Firmware on an Adapter

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, expand **Equipment** > **Chassis** > ***Chassis Number*** > **Servers**.

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

Step 4 Expand **Adapters** and select the adapter you want to upgrade.

Step 5 In the **General** tab, click **Update Firmware**.

Step 6 In the **Update Firmware** dialog box, do the following:

a) From the **Version** drop-down list, select the firmware version to which you want to update the endpoint.

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

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

Step 7 (Optional) Monitor the status of the update in the **Update Status** area.
The update process can take several minutes. Do not activate the firmware until the selected firmware package displays in the **Backup Version** field in the **Firmware** area of the **General** tab.

What to Do Next

Activate the firmware.

Activating the Firmware on an Adapter

Procedure

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

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

Step 3 Expand the node for the server that includes the adapter for which you want to activate the updated firmware.

Step 4 Expand **Adapters** and select the adapter for which you want to activate the firmware.

Step 5 In the **General** tab, click **Activate Firmware**.

Step 6 In the **Activate Firmware** dialog box, do the following:

a) Select the appropriate version from the **Version To Be Activated** drop-down list.
If one or more of the selected endpoints are not configured with the desired version as the backup version, Cisco UCS Manager GUI does not display that version in the **Set Version** drop-down list. You must select the version from the **Startup Version** column for each individual endpoint.

b) If you want to set the start up version and not change the version running on the endpoint, check the **Set Startup Version Only** check box.
During a direct upgrade, you should configure **Set Startup Version Only** for an adapter. With this setting, the activated firmware moves into the pending-next-boot state, and the server is not immediately rebooted.

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

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

c) Click **OK**.

Updating the BIOS Firmware on a Server

Caution Do not remove the hardware that contains the endpoint or perform any maintenance on it until the update process 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, expand **Equipment** > **Chassis** > ***Chassis Number*** > **Servers**.

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

Step 4 On the **General** tab, click the **Inventory** tab.

Step 5 Click the **Motherboard** tab.

Step 6 In the **Actions** area, click **Update Bios Firmware**.

Step 7 In the **Update Firmware** dialog box, do the following:

a) From the **Version** drop-down list, select the firmware version to which you want to update the server BIOS.

b) (Optional) If you want to update the firmware regardless of any possible incompatibilities or currently executing tasks, check the **Force** check box.

c) Click **OK**.

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

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

What to Do Next

Activate the firmware.

Activating the BIOS Firmware on a Server

Procedure

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

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

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

Step 4 On the **General** tab, click the **Inventory** tab.

Step 5 Click the **Motherboard** tab.

Step 6 In the **Actions** area, click **Activate Bios Firmware**.

Step 7 In the **Activate Firmware** dialog box, do the following:

a) Select the appropriate server BIOS version from the **Version To Be Activated** drop-down list.

b) If you want to set the start up version and not change the version running on the server, check the **Set Startup Version Only** check box.
If you configure **Set Startup Version Only**, the activated firmware moves into the pending-next-reboot state and the server is not immediately rebooted. The activated firmware does not become the running version of firmware until the server is rebooted.

c) Click **OK**.

Updating the CIMC Firmware on a Server

Caution Do not remove the hardware that contains the endpoint or perform any maintenance on it until the update process 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, expand **Equipment** > **Chassis** > ***Chassis Number*** > **Servers**.

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

Step 4 In the **General** tab, click the **Inventory** tab.

Step 5 Click the **CIMC** tab.

Step 6 In the **Actions** area, click **Update Firmware**.

Step 7 In the **Update Firmware** dialog box, do the following:

a) From the **Version** drop-down list, select the firmware version to which you want to update the endpoint.

b) Click **OK**.

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

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

What to Do Next

Activate the firmware.

Activating the CIMC Firmware on a Server

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

⚠ **Caution** Do not remove the hardware that contains the endpoint or perform any maintenance on it until the update process 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, expand **Equipment** > **Chassis** > ***Chassis Number*** > **Servers**.

Step 3 Expand the node for the server that includes the CIMC for which you want to activate the updated firmware.

Step 4 On the **General** tab, click the **Inventory** tab.

Step 5 Click the **CIMC** tab.

Step 6 In the **Actions** area, click **Activate Firmware**.

Step 7 In the **Activate Firmware** dialog box, do the following:

a) Select the appropriate version from the **Version To Be Activated** drop-down list.
If one or more of the selected endpoints are not configured with the desired version as the backup version, Cisco UCS Manager GUI does not display that version in the **Set Version** drop-down list. You must select the version from the **Startup Version** column for each individual endpoint.

b) If you want to set the start up version and not change the version running on the endpoint, check the **Set Startup Version Only** check box.
If you configure **Set Startup Version Only**, the activated firmware moves into the pending-next-reboot state and the endpoint is not immediately rebooted. The activated firmware does not become the running version of firmware until the endpoint is rebooted.

c) Click **OK**.

Updating the Firmware on an IOM

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, expand **Equipment** > **Chassis** > *Chassis Number* > **IO Modules**.

Step 3 Click the I/O module that you want to update.

Step 4 In the **General** tab, click **Update Firmware**.

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

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

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

Step 6 (Optional) Monitor the status of the update in the **Update Status** area.
The update process can take several minutes. Do not activate the firmware until the selected firmware package displays in the **Backup Version** field in the **Firmware** area of the **General** tab.

What to Do Next

Activate the firmware.

Activating the Firmware on an IOM

Procedure

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

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

Step 3 Select the **IO Module** node that includes the I/O module for which you want to activate the updated firmware.

Step 4 In the **General** tab, click **Activate Firmware**.

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

a) Select the appropriate version from the **Version To Be Activated** drop-down list.
If one or more of the selected endpoints are not configured with the desired version as the backup version, Cisco UCS Manager GUI does not display that version in the **Set Version** drop-down list. You must select the version from the **Startup Version** column for each individual endpoint.

b) If you want to set the start up version and not change the version running on the endpoint, check the **Set Startup Version Only** check box.
If you configure **Set Startup Version Only**, the activated firmware moves into the pending-next-reboot state and the endpoint is not immediately rebooted. The activated firmware does not become the running version of firmware until the endpoint is rebooted.

c) 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.

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 as the last step of upgrading a Cisco UCS domain, along with the server BIOS.

Procedure

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

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

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

Step 4 On the **Installed Firmware** tab, click **Activate Firmware**.
Cisco UCS Manager GUI opens the **Activate Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS domain. This step 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 of the **Activate Firmware** dialog box, select **Board Controller**.
Cisco UCS Manager GUI displays all servers that have board controllers in the **Activate Firmware** dialog box.

Step 6 In the **Select** field, do one of the following:

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

Step 7 Click **OK**.

Activating the Cisco UCS Manager Software

Procedure

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

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

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

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

Step 5 On the **UCS Manager** row of the **Activate Firmware** dialog box, do the following:

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

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

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

Activating the Firmware on a Subordinate Fabric Interconnect

Before You Begin

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

Procedure

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

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

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

Step 4 On the **Installed Firmware** tab, click **Activate Firmware**.
Cisco UCS Manager GUI opens the **Activate Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS domain. This step 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 row of the **Activate Firmware** dialog box for the subordinate fabric interconnect, do the following:

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

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

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

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

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

What to Do Next

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

Activating the Firmware on a Primary Fabric Interconnect

This procedure continues directly from Activating the Firmware on a Subordinate Fabric Interconnect, on page 64 and assumes you are on the **Firmware Management** tab.

Before You Begin

Activate the subordinate fabric interconnect.

Procedure

Step 1 On the **Installed Firmware** tab, click **Activate Firmware**.
Cisco UCS Manager GUI opens the **Activate Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS domain. This step 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 row of the **Activate Firmware** dialog box for the subordinate fabric interconnect, do the following:

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

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

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

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

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

Activating the Firmware on a Standalone Fabric Interconnect

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

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

Procedure

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

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

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

Step 4 On the **General** tab, click **Activate Firmware**.

Step 5 In the **Activate Firmware** dialog box, complete the following fields:

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

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

Step 6 Click **OK**.

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

Verifying Firmware Versions on Components

Procedure

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

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

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

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

CHAPTER 7

UpgradingFirmwarethroughFirmwarePackages in Service Profiles

This chapter includes the following sections:

Firmware Upgrades through Firmware Packages in Service Profiles

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

You cannot upgrade the firmware on an I/O module, fabric interconnect, or Cisco UCS Manager through service profiles. You must upgrade the firmware on those endpoints directly.

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

Host Firmware Package

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

- **Adapter**
- **CIMC**
- **BIOS**
- **Board Controller**
- **FC Adapters**
- **HBA Option ROM**
- **Storage Controller**

Tip You can include more than one type of firmware in the same host firmware package. For example, a host firmware package can include 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.

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

Management Firmware Package

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

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

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

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

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

Stages of a Firmware Upgrade through Firmware Packages in Service Profiles

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

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

New Service Profile

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

Firmware Package Policy Creation

During this stage, you create the host firmware packages.

Service Profile Association

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

Existing Service Profile

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

Effect of Updates to Firmware Packages in Service Profiles

To update firmware through a firmware package in a service profile, you need to update the firmware in the package. What happens after you save the changes to a firmware package depends upon how the Cisco UCS domain is configured.

The following table describes the most common options for upgrading servers with a firmware package in a service profile.

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

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

Creating a Host Firmware Package

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

Before You Begin

Ensure that the appropriate firmware 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 where you want to create the policy.
If the system does not include multitenancy, expand the **root** node.

Step 4 Right-click **Host Firmware Packages** and choose **Create Package**.

Step 5 In the **Create Host Firmware Package** dialog box, enter a unique name and description for the package.
This name can be between 1 and 32 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object has been saved.

Step 6 On each sub-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 to which you want to update the firmware.

Step 7 When you have added all the desired firmware to the package, click **OK**.

What to Do Next

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

Updating a Host Firmware Package

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

Before You Begin

Ensure that the appropriate firmware 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 **Host Firmware Packages** and choose the policy you want to update.

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

Step 6 On each sub-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 to which you want to update the firmware.

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

Updating a Management Firmware Package

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

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

Before You Begin

Ensure that the appropriate firmware 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 firmware table, do the following:

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

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

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

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

Adding Firmware Packages to an Existing Service Profile

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

Procedure

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

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

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

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

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

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

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

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

Step 9 Click **Save Changes**.

CHAPTER 8

Managing the Capability Catalog in Cisco UCS Manager

This chapter includes the following sections:

Capability Catalog

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

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

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

Contents of the Capability Catalog

The contents of the Capability Catalog include the following:

Implementation-Specific Tunable Parameters

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

Hardware-Specific Rules

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

User Display Strings

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

Updates to the Capability Catalog

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

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

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

Note The Capability Catalog version is determined by the version of Cisco UCS that you are using. For example, Cisco UCS 2.0 releases work with any 2.0 release of the Capability Catalog, but not with 1.0 releases of the Capability Catalog. For information about Capability Catalog releases supported by specific Cisco UCS releases, see the *Release Notes for Cisco UCS Manager* accessible through the *Cisco UCS B-Series Servers Documentation Roadmap* available at the following URL: http://www.cisco.com/go/unifiedcomputing/b-series-doc.

Activating a Capability Catalog Update

Procedure

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

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

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

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

Step 5 Click **Activate Catalog**.

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

Step 7 Click **OK**.

Verifying that the Capability Catalog Is Current

Before You Begin

Procedure

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

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

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

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

Step 5 On Cisco.com, determine the most recent release of the capability catalog available.
For more information about the location of capability catalog updates, see Obtaining Capability Catalog Updates from Cisco, on page 82.

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

Viewing a Capability Catalog Provider

Procedure

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

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

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

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

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

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

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

Downloading Individual Capability Catalog Updates

Obtaining Capability Catalog Updates from Cisco

Procedure

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

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

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

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

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

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

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

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

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

What to Do Next

Update the Capability Catalog.

Updating the Capability Catalog from a Remote Location

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

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

Procedure

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

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

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

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

Step 5 Click **Update Catalog**.

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

Step 7 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**
Server field	The IP address or hostname of the remote server on which the catalog image resides.
Filename field	The name of the catalog executable you want to download.
Path field	The absolute path to the catalog image 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.

Step 8 Click **OK**.

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

What to Do Next

Activate the Capability Catalog update.

Updating the Capability Catalog from the Local File System

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

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

Procedure

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

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

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

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

Step 5 Click **Update Catalog**.

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

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

Step 8 Click **OK**.

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

What to Do Next

Activate the Capability Catalog update.

CHAPTER 9

Updating Management Extensions

This chapter includes the following sections:

Management Extensions

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

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

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

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

Activating a Management Extension

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

Procedure

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

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

Step 3 Click the **Management Extension** node.

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

Step 5 In the **Actions** area, click **Activate Management Extension**.

Step 6 In the **Activate Management Extension** dialog box, choose the management extension that you want to activate from the **Version to be Activated** drop-down list.

Step 7 Click **OK**.

PART II

Managing Firmware through Cisco UCS Central

CHAPTER 10

Downloading and Managing Firmware in Cisco UCS Central

This chapter includes the following sections:

Firmware Download from Cisco

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

Important Make sure you do the following to download firmware from Cisco into Cisco UCS Central.

- You must enable Cisco UCS Central to access Cisco.com either directly or using a proxy server.
- You must configure valid Cisco user credentials and enable download state in Cisco UCS Central.

Firmware Library of Images

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

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

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

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

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

Configuring Firmware Download from Cisco

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

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Images**.

Step 3 Click **Configure Downloads From Cisco**.

Step 4 In the **Work** pane, **General** tab, fill in the fields with the following information:

Name	Description
Username field	The username for the Cisco.com account that Cisco UCS Central uses to log in.
Password field	The password for this Cisco.com account.
Confirm Password field	The password again for confirmation purposes.

Name	Description
Download Interval drop-down list	How often Cisco UCS Central checks for a new versions of the infrastructure, server, and capability catalog firmware bundles on Cisco.com. This can be one of the following: • **1day**—Cisco UCS Central checks for new firmware once every 24 hours. • **1week**—Cisco UCS Central checks for new firmware once a week. • **2week**—Cisco UCS Central checks for new firmware once every two weeks. • **on-demand**—Cisco UCS Central does not automatically check for new firmware bundles. Instead, it waits until a user clicks **Refresh** on the Library of Images **General** tab.
Download State drop-down list	Whether Cisco UCS Central can download firmware image bundles or firmware metadata from Cisco.com. This can be one of the following: • **enable**—Cisco UCS Central downloads the firmware metadata for new firmware versions from Cisco.com using the schedule defined in the **Download Interval** field or when the user refreshes the image library. In addition, Cisco UCS Central downloads the firmware image bundles when users click the **Store Locally** button or when a firmware version is used in a firmware host package. • **disable**—Cisco UCS Central cannot download the firmware bundle or metadata from Cisco.com. If you select this option, the only way you can add new firmware bundles to Cisco UCS Central is to download them manually from Cisco.com and then download them into the image library using the **Downloads** subtab on the Library of Images **General** tab. Even if the firmware metadata already exists in the image library, or if the firmware has been added to a host firmware package, Cisco UCS Central cannot download the firmware bundle, nor can a user select the firmware metadata file and download it using the **Store Locally** option.

Step 5 In the **Proxy** tab, fill in the fields with the following information:

Name	Description
HTTP Proxy field	The HTTP proxy required for internet access, if any.
Port field	The port for the HTTP proxy server.
Proxy User drop-down list	The proxy server username.

Name	Description
Proxy Password field	The password for this proxy server account.
Confirm Proxy Password field	The password again for confirmation purposes.

Step 6 Click **Save**.

Downloading a Firmware Image from Cisco

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

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

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

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Images**.

Step 3 Click **Library**.

Step 4 In the **Work** pane, click **Packages** tab.
The image metadata downloaded from Cisco will have the **Source** as **Cisco** and **State** as **not-downloaded**.

Step 5 Right click on the bundle and from the options, choose **Store Locally**.

Downloading Firmware from a Remote Location

Before You Begin

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

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Images**.

Step 3 Click **Library**.

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

Step 5 In the **Downloads** tab, click **Download Firmware**.

Step 6 In the **Download Firmware** dialog box, **Location of the Image File**, choose **Remote File System**.
Fill in the following fields:

Name	Description
Protocol field	The remote server communication protocol. This can be one of the following: • **FTP** • **TFTP** • **SCP** • **SFTP**
Server field	Host name or IP address of the server that support the selected protocol.
Filename field	The name of the firmware file.
Remote Path field	The absolute path to the file on the remote server.
User field	The username Cisco UCS Central 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.

Step 7 Click **OK**.

Downloading Firmware from a Local File System

Before You Begin

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

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Images**.

Step 3 Click **Library**.

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

Step 5 In the **Downloads** tab, click **Download Firmware**.

Step 6 In the **Download Firmware** dialog box, **Location of the Image File**, choose **Local File System**.

Step 7 Click **Download Image into Image Library**.
A dialog box opens with an option to select the file.

Step 8 Click **Browse** to browse to the firmware file location in your local system and select the file.

Step 9 Click **Submit**.
If the image download is successful, **Firmware Image Download** dialog box opens with a confirmation message.

Step 10 In the **Firmware Image Download** dialog box, click **OK**.

Viewing Image Download Faults

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

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Images**.

Step 3 Click **Library**.

Step 4 In the **Work** pane, click **Faults** tab.
The faults table displays all download faults with details.

Viewing Firmware Images in the Library

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

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Images**.

Step 3 Click **Library**.

Step 4 The **Work** pane click the **Packages** tab.
The available packages are displayed as listed in the following table:

Name	Description
Filter button	Allows you to filter the data in the table. When you apply a filter, this button name changes to **Filter (on)**.
Hide button	Hides any firmware bundles that have the **Hide** check box checked in the table. To restore the hidden bundles, click **Show Hidden**.
Show Hidden button	Displays all firmware bundles, including those that have the **Hide** check box checked in the table.
Purge button	Deletes the selected image metadata from the library of images. Once you delete the metadata, you can no longer download the associated firmware bundle from Cisco.com through Cisco UCS Central. To access this bundle, you must download the firmware bundle through Cisco.com and import it into the image library manually.
Store Locally button	Downloads the firmware bundle associated with the selected image metadata entry from Cisco.com. **Note** This button is only available when you select image metadata in the table.
Delete button	Click this button to delete the currently selected firmware file from the Cisco UCS Central image library. **Note** This button is only available when you select a firmware bundle in the table.
Properties button	Displays detailed properties for the object selected in the table.
Name column	The name of the firmware bundle, sorted by firmware type. Expand a type to view the available firmware bundles of that type.
Version column	The firmware version associated with the bundle.

Name	Description
Source column	The source from which the image was downloaded. This can be one of the following: • **Cisco**—The image was downloaded through Cisco UCS Central using the image metadata from Cisco.com. • **Local**—The image was imported from a local system or remote server.
State column	The download state of the firmware bundle.
Type column	The type of firmware in the bundle.
Hide column	If checked, the firmware bundle is hidden when you click **Hide** in the toolbar.

Deleting Image Metadata from the Library of Images

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

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

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Images**.

Step 3 Click **Library**.

Step 4 In the **Work** pane, choose the firmware image metadata you want to delete from **Library of Images**and click **Purge**.

Step 5 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

CHAPTER 11

Upgrading Firmware in Cisco UCS Domains through Cisco UCS Central

This chapter includes the following sections:

Firmware Upgrades for Cisco UCS Domains

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

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

Configuring an Infrastructure Firmware Upgrade for a Cisco UCS Domain

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

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

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Groups Root** > **Firmware Management**.

Step 3 Click **Infrastructure Firmware**.

Step 4 In the **Work** pane, **Policies** tab, click **Create**.

Step 5 In the **Scheduler** area, specify a schedule to apply the infrastructure firmware on the Cisco UCS domains in the domain group.

Name	Description
Create button	Creates a infrastructure firmware policy for the selected domain group that overrides the settings inherited from its parent group, if an inherited policy exists. The upgrade schedule defined here overrides the version inherited from any parent groups, if an inherited schedule exists.
Delete button	Deletes the infrastructure firmware policy.
User Ack field	If checked, a user must acknowledge the action on the **Pending Activities** tab before the firmware infrastructure upgrade begins on a Cisco UCS domain.
Start Time field	The date and time that the occurrence will run. To run the schedule immediately, check the check box. To specify a day and time, clear the check box, then enter the day and time in the associated entry field. Click the calendar icon at the end of the field to select the date from a calendar.
Maximum Number of Concurrent Tasks field	The maximum number of tasks that can run concurrently with tasks associated with this schedule. To allow as many tasks to run as the system can handle, check the check box. To limit the number of tasks that can run, clear the check box and enter a value in the associated entry field. You can specify an integer between 1 and 65535.

Step 6 In the **Version** area, select the infrastructure firmware version.

Impacted Endpoints area displays the endpoints that will get impacted by the infrastructure firmware policy. During a firmware upgrade, these endpoints will be rebooted and will therefore be unavailable during part of the upgrade process.

Step 7 Click **Save**.

What to Do Next

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

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

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

Acknowledging a Pending Activity

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

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

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

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Groups Root** > **Firmware Management**.

Step 3 In the **Work** pane, click **Pending Activities** tab.

Step 4 Choose the pending activity from the displayed list, right click and click **Acknowledge**.

Deleting an Infrastructure Firmware Package

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Groups Root** > **Firmware Management**.

Step 3 The **Work** pane displays a list of all created infrastructure firmware packages.

Step 4 Click **Delete**.

Step 5 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Creating a Host Firmware Package

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Groups Root** > **Firmware Management**.

Step 3 Click **Host Firmware**.

Step 4 In the **Work** pane, **Policies** tab, click **Create a Pack**.

Step 5 In **Create a Pack** dialog box, fill in the following fields:

a) Fill in **Name** and **Description**.

Name	Description
Name field	The name of the host firmware package. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object has been saved.
Description field	The description of the host firmware package. Enter up to 256 characters. You can use any characters or spaces except ` (accent mark), \ (backslash), ^ (carat), " (double quote), = (equal sign), > (greater than), < (less than), and ' (single quote).

b) In the **Blade Version** area, choose the blade server version.

c) In the **Rack Version** area, choose the rack server version.

Step 6 The **Impacted Endpoints** dialog box displays the list of end points that will be affected by this host firmware policy.

During a firmware upgrade, these endpoints will be rebooted and will therefore be unavailable during part of the upgrade process

Step 7 Click **OK**.

What to Do Next

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

Deploying a Host Firmware Upgrade

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

Before You Begin

You must have created a host firmware package.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Groups Root** > **Firmware Management**.

Step 3 Click **Host Firmware**.

Step 4 In the **Work** pane, from the displayed list of host firmware packages, choose the firmware version you want to deploy.

Step 5 Click **Install Servers** on the table header.

Step 6 In the **Install Servers** dialog box, select **Blade Version**, **Rack version** and **Impacted Endpoints**.

Step 7 In **Upgrade host Firmware Warning** message dialog box, click **Yes**.
If the servers in the selected endpoints use the global host firmware upgrade policy, they will be upgraded with the host firmware package.

Deleting a Host Firmware Package

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Groups Root** > **Firmware Management**.

Step 3 The **Work** pane displays a list of all created host firmware packages.

Step 4 Click and choose the host firmware package name you want to delete.
The table header area shows action icons.

Step 5 Click **Delete**.

Step 6 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Scheduling Firmware Upgrades

Firmware Upgrade Schedules

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

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

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

Creating a Maintenance Policy

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

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

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

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

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

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** Pane, expand **Domain Groups** > **Domain Group Root** > **Maintenance**.

Step 3 In the **Work** pane, click **Create Maintenance Policy**.

Step 4 In the **Create Maintenance Policy** dialog box, do fill in the following fields:

Name	Description
Name field	The name of the policy. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object has been saved.
Description field	The description of the policy. Enter up to 256 characters. You can use any characters or spaces except ` (accent mark), \ (backslash), ^ (carat), " (double quote), = (equal sign), > (greater than), < (less than), and ' (single quote).
Reboot Policy field	When a service profile is associated with a server, or when changes are made to a service profile that is already associated with a server, the server needs to be rebooted to complete the process. The **Reboot Policy** field determines when the reboot occurs for servers associated with any service profiles that include this maintenance policy. This can be one of the following: • **immediate**—Cisco UCS reboots the server automatically as soon as changes are saved by the user. • **user-ack**—The user must acknowledge the server reboot request manually in Cisco UCS Manager after the changes are made. • **timer-automatic**—Cisco UCS defers all changes until the maintenance window defined by the schedule shown in the **Schedule** field.
Schedule drop-down list	If the **Reboot Policy** is set to **timer-automatic**, the schedule specifies when maintenance operations can be applied to the server. Cisco UCS either reboots the server at the scheduled time or waits for the user to manually acknowledge the reboot request in Cisco UCS Central, depending on the options configured for the selected schedule.

Step 5 Click **OK**.

What to Do Next

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

Creating a One Time Occurrence Schedule

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Groups Root** > **Schedules**.

Step 3 In the **Work** pane, click **Create Schedule**.

Step 4 In the **Create Schedule** dialog box, enter the following details in the **Properties** area:

Name	Description
Name field	The name of the schedule. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object has been saved.
Description field	The description of the schedule. We recommend you include information about where and when the schedule should be used. Enter up to 256 characters. You can use any characters or spaces except ` (accent mark), \ (backslash), ^ (carat), " (double quote), = (equal sign), > (greater than), < (less than), and ' (single quote).
User Ack check box	If checked, a user must manually acknowledge any server reboot requests in Cisco UCS Central for all servers associated with the selected schedule.

Step 5 Choose **One Time Occurrences** tab and click **Create One Time Occurrence**.

Step 6 In the **Create One Time Occurrence** dialog box, fill in the following details:

Name	Description
Name field	The name of the occurrence. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object has been saved.
Start Time field	The date and time that the occurrence will run. Click the calendar icon at the end of the field to select the date from a calendar.

Name	Description
Maximum Number of Tasks field	The maximum number of scheduled tasks that can be run during the occurrence. If you check the **unlimited** check box, Cisco UCS runs all scheduled tasks unless those tasks exceed the maximum time specified in the **Max Duration** field. If **Max Duration** is set to **none** and you select this option, the maintenance window continues until all pending activities are completed. If you want to specify the maximum number of tasks, clear the **unlimited** check box and enter an integer between 1 and 65535 in the associated field.
Maximum Number of Concurrent Tasks field	The maximum number of tasks that can run concurrently during the occurrence. If you check the **unlimited** check box, Cisco UCS runs as many concurrent tasks as the system can handle. If you want to specify the maximum number of concurrent tasks, clear the **unlimited** check box and enter an integer between 1 and 65535 in the associated field.
Maximum Duration field	The maximum length of time that the occurrence can run. If you check the **none** check box, Cisco UCS runs the occurrence runs until all tasks are completed. If you want to specify a maximum duration, clear the **none** check box and enter the maximum amount of time that the occurrence can run in the associated field using the format dd:hh:mm:ss. Cisco UCS completes as many scheduled tasks as possible within the specified time. By default, the maximum duration is set to **none**. If you do not change this setting and you do not set a maximum number of tasks, the maintenance window continues until all pending activities are completed.
Minimum Interval Between Tasks field	The minimum length of time that Cisco UCS should wait before starting a new task. This setting is meaningful only if the maximum number of concurrent tasks is set to a value other than **none**. If you check the **unlimited** check box, Cisco UCS runs the next task as soon as possible. If you want to specify the minimum amount of time that Cisco UCS must wait between tasks, clear the **unlimited** check box and enter the minimum wait time in the associated field using the format dd:hh:mm:ss.

Step 7 Click **OK**.

Step 8 Click OK in the **Create Schedule** dialog box.
The one time schedule you created is added to the **Schedules** table.

Creating a Recurring Occurrence Schedule

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Groups Root** > **Schedules**.

Step 3 In the **Work** pane, click **Create Schedule**.

Step 4 In the **Create Schedule** dialog box, enter the following details in the **Properties** area:

Name	Description
Name field	The name of the schedule. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object has been saved.
Description field	The description of the schedule. We recommend you include information about where and when the schedule should be used. Enter up to 256 characters. You can use any characters or spaces except ` (accent mark), \ (backslash), ^ (carat), " (double quote), = (equal sign), > (greater than), < (less than), and ' (single quote).
User Ack check box	If checked, a user must manually acknowledge any server reboot requests in Cisco UCS Central for all servers associated with the selected schedule.

Step 5 Choose **Recurring Occurrences** tab and click **Create Recurring Occurrence**.

Step 6 In the **Create Recurring Occurrence** dialog box, fill in the following details:

Name	Description
Name field	The name of the occurrence. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object has been saved.

Name	Description
Start Day field	The day on which Cisco UCS runs an occurrence of this schedule. This can be one of the following: • **every-day** • **Monday** • **Tuesday** • **Wednesday** • **Thursday** • **Friday** • **Saturday** • **Sunday** • **odd-day** • **even-day**
Hour field	The hour of the specified day at which this occurrence of the schedule starts. This can be an integer between 0 and 24, where 0 and 24 are both equivalent to midnight. **Note** Cisco UCS ends all recurring occurrences on the same day in which they start, even if the maximum duration has not been reached. For example, if you specify a start time of 11 p.m. and a maximum duration of 3 hours, Cisco UCS starts the occurrence at 11 p.m. but ends it at 11:59 p.m. after only 59 minutes. Ensure that the start time you specify is early enough so that the recurring occurrence finishes before 11:59 p.m.
Minute field	The minute of the hour at which the schedule occurrence starts. This can be an integer between 0 and 60.
Maximum Number of Tasks field	The maximum number of scheduled tasks that can be run during the occurrence. If you check the **unlimited** check box, Cisco UCS runs all scheduled tasks unless those tasks exceed the maximum time specified in the **Max Duration** field. If **Max Duration** is set to **none** and you select this option, the maintenance window continues until all pending activities are completed. If you want to specify the maximum number of tasks, clear the **unlimited** check box and enter an integer between 1 and 65535 in the associated field.

Name	Description
Maximum Number of Concurrent Tasks field	The maximum number of tasks that can run concurrently during the occurrence. If you check the **unlimited** check box, Cisco UCS runs as many concurrent tasks as the system can handle. If you want to specify the maximum number of concurrent tasks, clear the **unlimited** check box and enter an integer between 1 and 65535 in the associated field.
Maximum Duration field	The maximum length of time that the occurrence can run. If you check the **none** check box, Cisco UCS runs the occurrence runs until all tasks are completed. If you want to specify a maximum duration, clear the **none** check box and enter the maximum amount of time that the occurrence can run in the associated field using the format dd:hh:mm:ss. Cisco UCS completes as many scheduled tasks as possible within the specified time. By default, the maximum duration is set to **none**. If you do not change this setting and you do not set a maximum number of tasks, the maintenance window continues until all pending activities are completed.
Minimum Interval Between Tasks field	The minimum length of time that Cisco UCS should wait before starting a new task. This setting is meaningful only if the maximum number of concurrent tasks is set to a value other than **none**. If you check the **unlimited** check box, Cisco UCS runs the next task as soon as possible. If you want to specify the minimum amount of time that Cisco UCS must wait between tasks, clear the **unlimited** check box and enter the minimum wait time in the associated field using the format dd:hh:mm:ss.

Step 7 Click **OK**.

Step 8 Click OK in the **Create Schedule** dialog box.
The recurring schedule you created is added to the table.

Deleting a Firmware Upgrade Schedule

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Groups Root** > **Schedules**.

Step 3 The **Work** pane displays a list of all scheduled firmware events.

Step 4 Click and choose the schedule name you want to delete.

The table header area shows action icons.

Step 5 Click **Delete**.

Step 6 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

CHAPTER 12

Managing the Capability Catalog in Cisco UCS Central

This chapter includes the following sections:

Capability Catalog

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

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

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

Contents of the Capability Catalog

The contents of the Capability Catalog include the following:

Implementation-Specific Tunable Parameters

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

Hardware-Specific Rules

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

User Display Strings

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

Updates to the Capability Catalog

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

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

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

Note The Capability Catalog version is determined by the version of Cisco UCS that you are using. For example, Cisco UCS 2.0 releases work with any 2.0 release of the Capability Catalog, but not with 1.0 releases of the Capability Catalog. For information about Capability Catalog releases supported by specific Cisco UCS releases, see the *Release Notes for Cisco UCS Manager* accessible through the *Cisco UCS B-Series Servers Documentation Roadmap* available at the following URL: http://www.cisco.com/go/unifiedcomputing/b-series-doc.

Configuring a Capability Catalog Update for a Cisco UCS Domain

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

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

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Groups Root** > **Firmware Management**.

Step 3 Click **Capability Catalog**.

Step 4 In the **Work** pane, click **Create**.

Step 5 In the **Version** table, select the version of the capability catalog you want to associate with the Cisco UCS domains included in the selected Cisco UCS Central domain group.
The capability catalog version selected here overrides the version inherited from any parent groups, if an inherited version exists.

Step 6 Click **Save**.

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