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

First Published: 2014-07-20

Last Modified: 2015-03-09

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

Preface

Audience

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

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

Conventions

Text Type	Indication
GUI elements	GUI elements such as tab titles, area names, and field labels appear in **this font**. Main titles such as window, dialog box, and wizard titles appear in **this font**.
Document titles	Document titles appear in *this font*.
TUI elements	In a Text-based User Interface, text the system displays appears in `this font`.
System output	Terminal sessions and information that the system displays appear in `this font`.

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

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

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

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

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

Warning IMPORTANT SAFETY INSTRUCTIONS

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

SAVE THESE INSTRUCTIONS

Related Cisco UCS Documentation

Documentation Roadmaps

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

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

For information on supported firmware versions and supported UCS Manager versions for the rack servers that are integrated with the UCS Manager for management, refer to Release Bundle Contents for Cisco UCS Software.

Other Documentation Resources

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

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to ucs-docfeedback@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
- Fabric interconnects
- Endpoints physically located on adapters, including NIC and HBA firmware, and Option ROM (where applicable) that can be upgraded through firmware packages included in a service profile
- Endpoints physically located on servers, such as the BIOS, storage controller (RAID controller), and Cisco Integrated Management Controller (CIMC) that can be upgraded through firmware packages included in a service profile

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

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

This document uses the following definitions for managing firmware:

Upgrade

Changes the firmware running on an endpoint to another image, such as a release or patch. Upgrade includes both update and activation.

Update

Copies the firmware image to the backup partition on an endpoint.

Activate

Sets the firmware in the backup partition as the active firmware version on the endpoint. Activation can require or cause the reboot of an endpoint.

For Management Extensions and Capability Catalog upgrades, update and activate occur simultaneously. You only need to update or activate those upgrades. You do not need to perform both steps.

Firmware Auto Sync for FI Cluster

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

Software and Hardware Requirements

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

Implementation

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

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

Firmware Auto Sync Benefits

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

Firmware Management in Cisco UCS Central

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

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

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

- **Capability Catalog—** One capability catalog per domain group . All Cisco UCS domains registered to a particular domain group will use the capability catalog defined in the domain group.
- **Infrastructure Firmware—** One infrastructure firmware policy per domain group . All Cisco UCS domains registered to a particular domain group will use the same Infrastructure firmware version defined in the domain group.
- **Host Firmware—** You can have more than one host firmware policy for the different host firmware components in a domain group. The Cisco UCS 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.

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

Firmware Versions

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

Firmware Versions in CIMC, and Adapters

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

The following firmware version terminology is used in Cisco UCS Manager:

Running Version

The running version is the firmware that is active and in use by the endpoint.

Startup Version

The startup version is the firmware that will be used when the endpoint next boots up. Cisco UCS Manager uses the activate operation to change the startup version.

Backup Version

The backup version is the firmware in the other slot and is not in use by the endpoint. This version can be firmware that you have updated to the endpoint but have not yet activated, or it can be an older firmware version that was replaced by a recently activated version. Cisco UCS Manager uses the update operation to replace the image in the backup slot.

If the endpoint cannot boot from the startup version, it boots from the backup version.

Firmware Versions in the Fabric Interconnect and Cisco UCS Manager

You can only activate the fabric interconnect firmware and Cisco UCS Manager on the fabric interconnect. The fabric interconnect and Cisco UCS Manager firmware do not have backup versions, because all the images are stored on the fabric interconnect. As a result, the number of bootable fabric interconnect images is not limited to two, like the server CIMC and adapters. Instead, the number of bootable fabric interconnect images is limited by the available space in the memory of the fabric interconnect and the number of images stored there.

The fabric interconnect and Cisco UCS Manager firmware have running and startup versions of the kernel and system firmware. The kernel and system firmware must run the same versions of firmware.

CHAPTER 2

Cautions, Guidelines, and Limitations

This chapter includes the following sections:

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

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.

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

- Review the Release Notes.
- Review the relevant Hardware and Software Interoperability Matrix to ensure the operating systems on all servers have the right driver levels for the release of Cisco UCS to which you plan to upgrade.
- Back up the configuration into an All Configuration backup file.

- For a cluster configuration, verify that the high availability status of the fabric interconnects shows that both are up and running.
- For a standalone configuration, verify that the Overall Status of the fabric interconnect is Operable.
- Verify that the data path is up and running. For more information, see the Verifying that the Data Path is Ready section in the appropriate Firmware Management Guide.
- Verify that all servers, I/O modules, and adapters are fully functional. An inoperable server cannot be upgraded.
- Verify that the Cisco UCS domain does not include any critical or major faults. If such faults exist, you must resolve them before you upgrade the system. A critical or major fault may cause the upgrade to fail.
- Verify that all servers have been discovered. They do not need to be powered on or associated with a service profile.
- If you want to integrate a rack-mount server into the Cisco UCS domain, follow the instructions in the appropriate C-Series Rack-Mount Server Integration Guide for installing and integrating a rack-mount server in a system managed by Cisco UCS Manager.

Creating an All Configuration Backup File

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

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope system**	Enters system mode.
Step 2	UCS-A /system # **create backup** *URL* **all-configuration enabled**	Creates an enabled All Configuration backup operation that runs as soon as you enter the **commit-buffer** command. The **all-configuration** option backs up the server, fabric, and system related configuration. Specify the URL for the backup file using one of the following syntax: • **ftp:**// *username@hostname* / *path* • **scp:**// *username@hostname* / *path* • **sftp:**// *username@hostname* / *path* • **tftp:**// *hostname* **:** *port-num* / *path*
Step 3	UCS-A /system # **commit-buffer**	Commits the transaction.

The following example uses SCP to create an All Configuration backup file on the host named host35 and commits the transaction:

```
UCS-A# scope system
UCS-A /system* # create backup scp://user@host35/backups/all-config.bak all-configuration
enabled
Password:
UCS-A /system* # commit-buffer
UCS-A /system #
```

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

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

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

When a specific interval of time has passed after Cisco UCS Manager created a baseline of the outstanding faults, baselining is cleared and all faults show up as new faults. This interval is called baseline expiration interval. Modifying Baseline Expiration Interval for Faults, on page 11 provides detailed information about modifying a baseline expiration interval in Cisco UCS Manager.

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

Modifying Baseline Expiration Interval for Faults

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

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope monitoring**	Enters monitoring mode.
Step 2	UCS-A /monitoring # **scope fault policy**	Enters monitoring fault policy mode.
Step 3	UCS-A /monitoring/fault-policy # **show**	Displays the details of the fault policy.
Step 4	UCS-A /monitoring/fault-policy # **set baseline-expiration-interval** {*days hours minutes seconds*}	Modifies the baseline expiration interval. The default baseline expiration interval is 24 hours. **Note** After the baseline-expiration-interval expires, all faults are shown as new faults.
Step 5	UCS-A /monitoring/fault-policy* # **commit**	Commits the transaction.
Step 6	UCS-A /monitoring/fault-policy # **show**	Displays the details of the fault policy.

This example shows how to modify the baseline expiration interval for faults:

```
UCS-A# scope monitoring
UCS-A /monitoring # scope fault policy
UCS-A /monitoring/fault-policy # show

Fault Policy:
    Clear Action Clear Interval Retention Interval (dd:hh:mm:ss) Flap Interval (sec)
Baseline Expiration Interval (dd:hh:mm:ss)
    ------------ -------------- ------------------------------- ------------------------
-----------------------------------------
    Retain       00:00:20:00    00:01:00:00                     10
10:00:00:12

UCS-A /monitoring/fault-policy # set baseline-expiration-interval 0 2 24 0
UCS-A /monitoring/fault-policy* # commit
UCS-A /monitoring/fault-policy # show

Fault Policy:
    Clear Action Clear Interval Retention Interval (dd:hh:mm:ss) Flap Interval (sec)
Baseline Expiration Interval (dd:hh:mm:ss)
    ------------ -------------- ------------------------------- ------------------------
-----------------------------------------
    Retain       10:00:00:00    01:01:01:01                     10
00:02:24:00
UCS-A /monitoring/fault-policy #
```

Viewing Faults Generated During the Upgrade of a Fabric Interconnect

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope monitoring**	Enters monitoring mode.
Step 2	UCS-A /monitoring # **show new-faults**	Shows the faults generated after baselining and because of the reboot of the fabric interconnect during upgrade.
Step 3	UCS-A /monitoring # **show baseline-faults**	Shows the faults baselined before the reboot of the fabric interconnect during upgrade.

This example shows how to view faults generated at various stages of the upgrade process:

Faults before reboot of the primary fabric interconnect:

```
UCS-A# show fault
Severity  Code     Last Transition Time     ID       Description
--------- -------- ------------------------ -------- -----------
Major     F0283    2015-06-17T21:08:09.301     57360 fc VIF 687 on server 1 / 6 of switch
A  down, reason: NPV upstream port not available
Warning   F0156    2015-06-17T21:07:44.114     53557 Server, vendor(Cisco Systems Inc),
model(N20-B6620-1), serial(QCI133400WR) in slot 1/3 presence: mismatch
Major     F0283    2015-06-16T21:02:33.014     72467 fc VIF 688 on server 1 / 6 of switch
B  down, reason: NPV upstream port not available
Major     F0207    2015-06-15T22:40:11.636     57312 Adapter  host interface 1/6/1/1 link
state: down
Major     F0479    2015-06-15T22:40:11.635     57311 Virtual interface 687 link state is
down
```

```
Major     F0207    2015-06-15T22:40:11.633     57310 Adapter  host interface 1/6/1/2 link
state: down
Major     F0479    2015-06-15T22:40:11.632     57309 Virtual interface 688 link state is
down
```

Faults after reboot of the primary fabric interconnect:

```
UCS-A# show fault
Severity  Code     Last Transition Time     ID       Description
--------- -------- ------------------------ -------- -----------
Major     F0209    2015-06-17T21:40:49.301     57760 Adapter uplink interface on server 1
/ 6 of switch A  down, Please verify the connectivity to Fabric Interconnect.
Major     F0207    2015-06-17T21:40:11.636     57712 Adapter  host interface 1/6/1/1 link
state: down
Major     F0479    2015-06-17T21:40:11.635     57711 Virtual interface 685 link state is
down
Major     F0283    2015-06-17T21:08:09.301     57360 fc VIF 687 on server 1 / 6 of switch
A  down, reason: NPV upstream port not available
Warning   F0156    2015-06-17T21:07:44.114     53557 Server, vendor(Cisco Systems Inc),
model(N20-B6620-1), serial(QCI133400WR) in slot 1/3 presence: mismatch
Major     F0283    2015-06-16T21:02:33.014     72467 fc VIF 688 on server 1 / 6 of switch
B  down, reason: NPV upstream port not available
Major     F0207    2015-06-15T22:40:11.636     57312 Adapter  host interface 1/6/1/1 link
state: down
Major     F0479    2015-06-15T22:40:11.635     57311 Virtual interface 687 link state is
down
Major     F0207    2015-06-15T22:40:11.633     57310 Adapter  host interface 1/6/1/2 link
state: down
Major     F0479    2015-06-15T22:40:11.632     57309 Virtual interface 688 link state is
down
```

To view faults generated because of reboot of the primary fabric interconnect:

```
UCS-A /monitoring # show new-faults
Severity  Code     Last Transition Time     ID       Description
--------- -------- ------------------------ -------- -----------
Major     F0209    2015-06-17T21:40:49.301     57760 Adapter uplink interface on server 1
/ 6 of switch A  down, Please verify the connectivity to Fabric Interconnect.
Major     F0207    2015-06-17T21:40:11.636     57712 Adapter  host interface 1/6/1/1 link
state: down
Major     F0479    2015-06-17T21:40:11.635     57711 Virtual interface 685 link state is
down
```

To view faults before reboot of the primary fabric interconnect:

```
UCS-A# show baseline-faults
Severity  Code     Last Transition Time     ID       Description
--------- -------- ------------------------ -------- -----------
Major     F0283    2015-06-17T21:08:09.301     57360 fc VIF 687 on server 1 / 6 of switch
A  down, reason: NPV upstream port not available
Warning   F0156    2015-06-17T21:07:44.114     53557 Server, vendor(Cisco Systems Inc),
model(N20-B6620-1), serial(QCI133400WR) in slot 1/3 presence: mismatch
Major     F0283    2015-06-16T21:02:33.014     72467 fc VIF 688 on server 1 / 6 of switch
B  down, reason: NPV upstream port not available
Major     F0207    2015-06-15T22:40:11.636     57312 Adapter  host interface 1/6/1/1 link
state: down
Major     F0479    2015-06-15T22:40:11.635     57311 Virtual interface 687 link state is
down
Major     F0207    2015-06-15T22:40:11.633     57310 Adapter  host interface 1/6/1/2 link
state: down
Major     F0479    2015-06-15T22:40:11.632     57309 Virtual interface 688 link state is
down
```

Verifying the Operability of a Fabric Interconnect

If your Cisco UCS domain is running in a high availability cluster configuration, you must verify the operability of both fabric interconnects.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope fabric-interconnect** {**a** | **b**}	Enters fabric interconnect mode for the specified fabric interconnect.
Step 2	UCS-A /fabric-interconnect #**show**	Displays information about the fabric interconnect. Verify that the operability of the fabric interconnects is in the Operable state. If the operability is not in the Operable state, run a **show tech-support** command and contact Cisco Technical Support. Do not proceed with the firmware upgrade. For more information about the **show tech-support** command, see the *Cisco UCS Manager B-Series Troubleshooting Guide*.

The following example displays that the operability for both fabric interconnects is in the Operable state:

```
UCS-A# scope fabric-interconnect a
UCS-A /fabric-interconnect # show
Fabric Interconnect:
    ID OOB IP Addr     OOB Gateway     OOB Netmask     Operability
    -- --------------- --------------- --------------- -----------
    A  192.168.100.10  192.168.100.20  255.255.255.0   Operable

UCS-A /fabric-interconnect # exit
UCS-A# scope fabric-interconnect b
UCS-A /fabric-interconnect # show
Fabric Interconnect:
    ID OOB IP Addr     OOB Gateway     OOB Netmask     Operability
    -- --------------- --------------- --------------- -----------
    B  192.168.100.11  192.168.100.20  255.255.255.0   Operable
```

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

	Command or Action	Purpose
Step 1	UCS-A# **show cluster state**	Displays the operational state and leadership role for both fabric interconnects in a high availability cluster. Verify that both fabric interconnects (A and B) are in the Up state and HA is in the Ready state. If the fabric interconnects are not in the Up state or HA is not in the Ready state, run a **show tech-support** command and contact Cisco Technical Support. Do not proceed with the firmware upgrade. For more information about the **show tech-support** command, see the *Cisco UCS Troubleshooting Guide*. Also note which fabric interconnect has the primary role and which has the subordinate role; you will need to know this information to upgrade the firmware on the fabric interconnects.

	Command or Action	Purpose

The following example displays that both fabric interconnects are in the Up state, HA is in the Ready state, fabric interconnect A has the primary role, and fabric interconnect B has the subordinate role:

```
UCS-A# show cluster state
Cluster Id: 0x4432f72a371511de-0xb97c000de1b1ada4

A: UP, PRIMARY
B: UP, SUBORDINATE

HA READY
```

Verifying the Status of an I/O Module

If your Cisco UCS is running in a high availability cluster configuration, you must verify the status for both I/O modules in all chassis.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope chassis** *chassis-id*	Enters chassis mode for the specified chassis.
Step 2	UCS-A /chassis # **scope iom** *iom-id*	Enters chassis I/O module mode for the selected I/O module.
Step 3	UCS-A # **show**	Shows the status of the specified I/O module on the specified chassis. Verify that the overall status of the I/O module is in the Operable state. If the overall status is not in the Operable state, run a **show tech-support** command and contact Cisco Technical Support. Do not proceed with the firmware upgrade. For more information about the **show tech-support** command, see the *Cisco UCS Troubleshooting Guide*.

The following example displays that the overall status for both I/O modules on chassis 1 is in the Operable state:

```
UCS-A# scope chassis 1
UCS-A /chassis # scope iom 1
UCS-A /chassis/iom # show
IOM:
    ID         Side  Fabric ID Overall Status
    ---------- ----- --------- --------------
              1 Left  A         Operable

UCS-A /chassis/iom # exit
UCS-A /chassis # scope iom 2
UCS-A /chassis/iom # show
IOM:
    ID         Side  Fabric ID Overall Status
```

```
---------- ----- --------- --------------
         2 Right B         Operable
```

Verifying the Status of a Server

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope server** *chassis-id / server-id*	Enters chassis server mode for the specified server in the specified chassis.
Step 2	UCS-A /chassis/server # **show status detail**	Shows the status detail of the server. Verify that the overall status of the server is Ok, Unavailable, or any value that does not indicate a failure. If the overall status is in a state that indicates a failure, such as Discovery Failed, the endpoints on that server cannot be upgraded.

The following example displays that the overall status for server 7 on chassis 1 is in the Ok state:

```
UCS-A# scope server 1/7
UCS-A /chassis/server # show status detail
Server 1/7:
    Slot Status: Equipped
    Conn Path: A,B
    Conn Status: A,B
    Managing Instance: B
    Availability: Unavailable
    Admin State: In Service
    Overall Status: Ok
    Oper Qualifier: N/A
    Discovery: Complete
    Current Task:
```

Verifying the Status of Adapters on Servers in a Chassis

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope server** *chassis-id / server-id*	Enters chassis server mode for the specified server in the specified chassis
Step 2	UCS-A /chassis/server # **show adapter status**	Displays the status of the adapter. Verify that the overall status of the adapter is in the Operable state. If the overall status of the adapter is in any state other than Operable, you cannot upgrade it. However, you can proceed with the upgrade for the other adapters in the Cisco UCS domain.

The following example displays that the overall status for the adapter in server 7 on chassis 1 is in the Operable state:

```
UCS-A# scope server 1/7
UCS-A /chassis/server # show adapter status
Server 1/1:
    Overall Status
    --------------
    Operable
```

Obtaining Cisco UCS PowerTool and Running the Duplicate IQN Script

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

Procedure

Step 1 To download Cisco UCS PowerTool, do the following:

a) In your web browser, navigate to the following website: http://developer.cisco.com/web/unifiedcomputing/microsoft

b) Scroll down to the **Cisco UCS PowerTool (PowerShell Toolkit) Beta Download** area.

c) Download the `CiscoUcs-PowerTool-0.9.6.0.zip` file.

d) Unzip the file and follow the prompts to install Cisco UCS PowerTool.
You can install Cisco UCS PowerTool on any Windows computer. You do not need to install it on a computer used to access Cisco UCS Manager.

Step 2 To launch Cisco UCS PowerTool, enter the following at a command line:
C:\Program Files (x86)\Cisco\Cisco UCS PowerTool>C:\Windows\System32\windowspowe rshell\v1.0\powershell.exe -NoExit -ExecutionPolicy RemoteSigned -File .\StartUc sPS.ps1

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

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

Step 3 In Cisco UCS PowerTool, do the following:

a) Connect to Cisco UCS Manager, as follows:
PS C:\> **Connect-Ucs** *IP_address*

b) Enter your username and password when prompted for your credential as shown in the following example:

```
cmdlet Connect-Ucs at command pipeline position 1
Supply values for the following parameters:
Credential
```

Cisco UCS PowerTool outputs the following to your screen after you log in.

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

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

Step 4 In the Cisco UCS PowerTool, run the following script to validate your iSCSI boot configuration and check for duplicate IQNs :
PS C:\> **Get-UcsServiceProfile -type instance | Get-UcsVnicIScsi | ? { $_.InitiatorName -ne "" } | select Dn,InitiatorName | group InitiatorName | ? { $_.Count -gt 1 } | % { $obj = New-Object PSObject ; $obj | Add-Member Noteproperty Count $_.Count; $obj | Add-Member Noteproperty InitiatorName $_.Name; $obj | Add-Member Noteproperty Dn ($_ | select -exp Group | % { $_.Dn }); $obj }**

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

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

Step 5 (Optional) If you have .NET Frame work 3.5 Service Pack 1 installed, you can use the following script to view the output in the GUI:
PS C:\> **Get-UcsServiceProfile -type instance | Get-UcsVnicIScsi | ? { $_.InitiatorName -ne "" } | select Dn,InitiatorName | group InitiatorName | ? { $_.Count -gt 1 } | % { $obj = New-Object PSObject ; $obj | Add-Member Noteproperty Count $_.Count; $obj | Add-Member Noteproperty InitiatorName $_.Name; $obj | Add-Member Noteproperty Dn ($_ | select -exp Group | % { $_.Dn }); $obj } | ogv**

Step 6 Disconnect from Cisco UCS Manager, as follows:
PS C:\>**Disconnect-Ucs**

What to Do Next

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

CHAPTER 4

Downloading and Managing Firmware in Cisco UCS Manager

This chapter includes the following sections:

Firmware Image Management

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

Cisco UCS Infrastructure Software Bundle

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

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

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

Cisco UCS B-Series Blade Server Software Bundle

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

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

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

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

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

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

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

Firmware Image Headers

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

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

Firmware Image Catalog

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

Packages

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

Images

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

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

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

Firmware Image Management for Cisco UCS Mini

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

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

Obtaining Software Bundles from Cisco

Before You Begin

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

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

Procedure

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

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

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

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

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

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

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

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

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

a) Click the link for the latest software bundle for the release you want to download.

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

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

Before You Begin

Obtain the required firmware bundles from Cisco.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope firmware**	Enters firmware mode.
Step 2	UCS-A /firmware # **download image** *URL*	Downloads the firmware bundle. Using the download path provided by Cisco, specify the URL with one of the following syntax: • **ftp:**// *server-ip-addr* / *path* • **scp:**// *username@server-ip-addr* / *path* • **sftp:**// *username@server-ip-addr* / *path* • **tftp:**// *server-ip-addr* **:** *port-num* / *path* • **usbA:**/ *path*

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

The following example uses SCP to download the firmware package.

```
UCS-A# scope firmware
UCS-A /firmware # download image
scp://user1@192.168.10.10/images/ucs-mini-k9-bundle-infra.3.0.1a.A.bin
OR
download image usbB:/username/ucs-k9-bundle-b-series.3.0.1a.B.bin
UCS-A /firmware # show download-task
UCS-A /firmware #
```

What to Do Next

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

Displaying the Firmware Package Download Status

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

Procedure

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

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

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

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

Download task:
File Name                        Protocol     Server          Userid      State
---------                         -------- --------------- ---------      -----
ucs-mini-k9-bundle-infra.3.0.1a.A.bin Scp    209.165.201.15  user1 Downloading

UCS-A /firmware # show download-task

Download task:
File Name                        Protocol     Server          Userid      State
---------                         -------- --------------- ---------      -----
ucs-mini-k9-bundle-infra.3.0.1a.A.bin Scp    209.165.201.15  user1 Downloading

UCS-A /firmware # show download-task

Download task:
File Name                        Protocol     Server          Userid      State
---------                         -------- --------------- ---------      -----
ucs-mini-k9-bundle-infra.3.0.1a.A.bin Scp    209.165.201.15   user1 Downloaded
```

Canceling an Image Download

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

Procedure

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

The following example cancels an image download:

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

Displaying All Available Software Images on the Fabric Interconnect

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

Procedure

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

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

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

Name                                Type              Version
----------------------------------  --------------------       ------------------
mini-ucs-6100-k9-system.5.0.3.N2.3.0.1a.A.gbin    FI System     5.0(3)N2(3.0(1a)A)
mini-ucs-6100-k9-kickstart.5.0.3.N2.3.0.1a.A.gbin FI Kernel     5.0(3)N2(3.0(1a)A)
ucs-mini-k9-manager.3.0.1a.A.gbin                 System        5.0(3)N2(3.0(1a)A)
```

Displaying All Available Packages on the Fabric Interconnect

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

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope firmware**	Enters firmware mode.
Step 2	UCS-A /firmware # **show package**	Displays all software packages downloaded onto the fabric interconnect.

	Command or Action	Purpose
		Note You must provide the software version number when directly updating an endpoint. If you intend to directly update firmware at an endpoint, note its version number in the right column.

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

```
UCS-A# scope firmware
UCS-A /firmware # show package
Name                          Version
---------------------------------------   ---------
ucs-catalog.3.0.1a.T.gbin                  3.0(1a)T
ucs-mini-k9-bundle-infra.3.0.1a.A.bin      3.0(1a)A
ucs-k9-bundle-b-series.3.0.1a.B.bin        3.0(1a)B
ucs-k9-bundle-c-series.3.0.1a.C.bin        3.0(1a)C


Pubs-A /firmware #
```

Determining the Contents of a Firmware Package

Procedure

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

The following example displays the contents of a firmware package:

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

UCS-A# scope firmware
UCS-A /firmware # show package ucs-mini-k9-bundle-infra.3.0.1a.A.gbin expand
Package ucs-mini-k9-bundle-infra.3.0.1a.A.bin:
    Images:
        ucs-mini-k9-kickstart.5.0.3.N2.3.0.1a.A.gbin
        ucs-mini-k9-manager.3.0.1a.A.gbin
        ucs-mini-k9-system.5.0.3.N2.3.0.1a.A.gbin
```

Checking the Available Space on a Fabric Interconnect

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

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope fabric-interconnect** {**a** | **b**}	Enters fabric interconnect mode for the specified fabric.
Step 2	UCS-A /fabric-interconnect # **show storage** [**detail** | **expand**}	Displays the available space for the specified fabric. **Note** When you download a firmware image bundle, a fabric interconnect needs at least twice as much available space as the size of the firmware image bundle. If the bootflash does not have sufficient space, delete the obsolete firmware, core files, and other unneeded objects from the fabric interconnect.

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

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

Deleting Firmware Packages from a Fabric Interconnect

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

Procedure

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

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

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

```
UCS-A# scope firmware
UCS-A /firmware # delete package ucs-k9-bundle-c-series.3.0.1a.C.bin
UCS-A /firmware* # commit-buffer
UCS-A /firmware #
```

Deleting Firmware Images from a Fabric Interconnect

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

Procedure

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

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

```
UCS-A# scope firmware
UCS-A /firmware # delete image ucs-mini-k9-manager.3.0.1a.A.gbin
UCS-A /firmware* # commit-buffer
UCS-A /firmware #
```

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, after you upgrade Cisco UCS Manager to Release 2.1(1) or greater, you can use Auto Install to upgrade the remaining components in a Cisco UCS domain that is at the minimum required firmware level. For more information, see *Cautions, Guidelines, and Limitations for Upgrading with Auto Install* and the appropriate Cisco UCS upgrade guide.

Direct Upgrade After Auto Install

During Auto Install, the startup version of the default infrastructure pack is configured. To successfully complete a direct upgrade or activation of Cisco UCS Manager, Fabric Interconnects, and IOMs after Auto Install, ensure that the startup version is cleared before starting direct upgrade or activation. If the startup version of the default infrastructure pack is configured, you cannot directly upgrade or activate Cisco UCS Manager, Fabric Interconnects, and IOMs. Clearing the Startup Version of the Default Infrastructure Pack, on page 37 provides detailed steps for clearing the startup version.

Install Infrastructure Firmware

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

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

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

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

Install Server Firmware

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

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

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

Automatic Internal Backup

While the Infrastructure firmware is being upgraded, an automatic full state backup file is created. Cisco UCS Manager Release 2.2(4) introduces two new backup stages that are visible in the FSM status. These are:

1. **InternalBackup—**Backs up the configuration.
2. **PollInternalBackup—**Waits for the backup to complete.

After the backup is successfully completed, the backup file, named as "bkp.*timestamp*.tgz", is stored within the `/workspace/backup` directory of both the Fabric Interconnects. This location contains only the latest backup file.

If the backup fails, a minor fault stating "**internal backup failed**" is logged. This fault is not logged in case of downgrade to a release prior to Cisco UCS Manager Release 2.2(4).

Before restoring the configuration for a Fabric Interconnect from this backup file, copy it from the Fabric Interconnect to a file server by using the **copy** command from local-mgmt.

This example shows how to copy the automatic internal backup file to a file server:

```
UCS-A# connect local-mgmt
UCS-A (local-mgmt) # copy workspace:/backup/bkp.1429690478.tgz
scp://builds@10.190.120.2://home/builds/
```

Cisco UCS Manager CLI Configuration Guide, Release 2.2 provides more details about restoring the configuration for a Fabric Interconnect.

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

The **auto-install** scope is not available if the Cisco UCS Manager CLI is at a release lower than 2.1(1).

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

Before You Begin

Complete all prerequisites listed in Prerequisites for Upgrading and Downgrading Firmware, on page 9.

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

Procedure

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

	Command or Action	Purpose

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

```
UCS-A# scope firmware
UCS-A /firmware # scope auto-install
UCS-A /firmware/auto-install # install infra infra-vers 3.0(1e)a
This operation upgrades firmware on UCS Infrastructure Components
(UCS manager, Fabric Interconnects and IOMs).
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup
(3) Check if Management Interface Monitoring Policy is enabled
(4) Check if there is a pending Fabric Interconnect Reboot activitiy
(5) Ensure NTP is configured
Do you want to proceed? (yes/no): yes

Triggering Install-Infra with:
   Infrastructure Pack Version: 3.0(1e)A
UCS-A /firmware/auto-install #
```

What to Do Next

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

Acknowledging the Reboot of the Primary Fabric Interconnect

Before You Begin

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

- Ensure that all the IOMs that are attached to the Fabric Interconnect are up before you acknowledge the reboot of the Fabric Interconnect. If all IOMs are not up, all the servers connected to the Fabric Interconnect will immediately be re-discovered and cause a major disruption.
- Ensure that both of the Fabric Interconnects and the service profiles are configured for failover.
- Verify that the data path has been successfully restored from the secondary Fabric Interconnect before you acknowledge the reboot of the primary Fabric Interconnect. For more information, see Verifying that the Data Path is Ready, on page 85.

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

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope firmware**	Enters firmware mode.
Step 2	UCS-A /firmware # **scope auto-install**	Enters auto-install mode for infrastructure firmware upgrades.
Step 3	UCS-A /firmware/auto-install # **acknowledge primary fabric-interconnect reboot**	Acknowledges the pending reboot of the primary fabric interconnect.
Step 4	UCS-A /firmware/auto-install # **commit-buffer**	Commits the transaction to the system configuration. Cisco UCS Manager immediately reboots the primary fabric interconnect. You cannot stop this reboot after you commit the transaction.

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

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

Canceling an Infrastructure Firmware Upgrade

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

Procedure

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

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

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

Clearing the Startup Version of the Default Infrastructure Pack

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

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters the organization mode for the specified organization. To enter the root organization mode, enter / as the *org-name*.
Step 2	UCS-A /org # **scope fw-infra-pack** *name*	Enters the organization infrastructure firmware policy mode.
Step 3	UCS-A /org/fw-infra-pack # **set infra-bundle-version** "*version*"	Specifies the infrastructure policy version for the update. To clear the startup version, specify **""** as the startup version.
Step 4	UCS-A /org/fw-infra-pack* # **commit-buffer**	Commits the transaction.

This example shows how to clear the startup version of the default infrastructure pack.

```
UCS-A# scope org
UCS-A /org # scope fw-infra-pack default
UCS-A /org/fw-infra-pack # set infra-bundle-version ""
UCS-A /org/fw-infra-pack* # commit-buffer
```

Viewing the Status of the FSM During An Infrastructure Firmware Upgrade

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope firmware**	Enters firmware mode.
Step 2	UCS-A /firmware # **scope auto-install**	Enters auto-install mode for infrastructure firmware upgrades.

	Command or Action	Purpose
Step 3	UCS-A /firmware/auto-install # **show fsm status expand**	Displays the status of the FSM.

The following example displays the status of the FSM:

```
UCS-A /firmware/auto-install # show fsm status expand

    FSM Status:

        Affected Object: sys/fw-system/fsm
        Current FSM: Deploy
        Status: In Progress
        Completion Time:
        Progress (%): 92

        FSM Stage:

        Order  Stage Name                                Status       Try
        ------ ---------------------------------------- ------------ ---
        1      DeployWaitForDeploy                       Success      0
        2      DeployResolveDistributableNames           Skip         0
        3      DeployResolveDistributable                Skip         0
        4      DeployResolveImages                       Skip         0
        5      DeployInternalBackup                      Skip         0
        6      DeployPollInternalBackup                  Success      0
        7      DeployActivateUCSM                        Skip         0
        8      DeployPollActivateOfUCSM                  Success      0
        9      DeployUpdateIOM                           Success      0
        10     DeployPollUpdateOfIOM                     Success      0
        11     DeployActivateIOM                         Success      0
        12     DeployPollActivateOfIOM                   Success      0
        13     DeployActivateRemoteFI                    Success      0
        14     DeployPollActivateOfRemoteFI              In Progress  1
        15     DeployWaitForUserAck                      Pending      0
        16     DeployPollWaitForUserAck                  Pending      0
        17     DeployActivateLocalFI                     Pending      0
        18     DeployPollActivateOfLocalFI               Pending      0
```

CHAPTER 6

Using Firmware Automatic Synchronization Server Policy

This chapter includes the following sections:

Firmware Automatic Synchronization

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

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

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

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

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

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

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

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

Setting the Firmware Auto-Sync Server Policy

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

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

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the org-name.
Step 2	UCS-A /org # **scope fw-autosync-policy**	Enters the firmware auto synchronization policy mode.
Step 3	UCS-A /org/fw-autosync-policy # **set** {*user-ack*| *no-actions*}	Set one of the following values to set the policy: • **User Acknowledge**--Firmware on the server is not synchronized until the administrator acknowledges the discovered server in the **server** command mode. • **No Action—**No firmware upgrade is initiated on the server.
Step 4	UCS-A /org/fw-autosync-policy # **commit-buffer**	Commits the transaction to the system configuration.

This example shows how to set the **Firmware Auto Sync Server** policy and commit the transaction to the system:

```
UCS-A # scope org sample
UCS-A /org # scope fw-autosync-policy
UCS-A /org/fw-autosync-policy # set user-ack
```

```
UCS-A /org/fw-autosync-policy* # commit-buffer
UCS-A /org/fw-autosync-policy #
```

What to Do Next

If you set the value to **User Acknowledge**, then you must acknowledge pending activity for the server for the firmware synchronization to occur.

Acknowledging the Firmware Auto Synchronization for a Server

If you have set the Firmware Auto-Sync Server policy to **User Acknowledge**, then you will have to acknowledge the pending activities for a server. If you do not acknowledge this pending activity for the server, then the firmware version of the server or the endpoints in the server are not updated to match with the firmware versions defined in the default host firmware pack.

Before You Begin

- You should have logged in as an administrator to complete this task.

Procedure

Step 1 UCS-A# **scope chassis**
Enters the chassis command mode.

Step 2 UCS-A /chassis # **scope server** *server ID*
Enters the server command mode.

Step 3 UCS-A /chassis/server # **fw-sync** {*acknowledge discard*}
Acknowledges or discards the pending firmware synchronization for the server.

Step 4 UCS-A /chassis/server # **commit-buffer**
Commits the transaction to the server.

This example shows how to acknowledge the pending firmware update for a server and commit the transaction:

```
UCS-A # scope chassis
UCS-A /chassis # scope server 1
UCS-A /chassis/server # fw-sync acknowledge
UCS-A /chassis/server* # commit-buffer
UCS-A /chassis/server #
```

CHAPTER 7

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 completes. If the hardware is removed or otherwise unavailable due to maintenance, the firmware update fails. This failure might corrupt the backup partition. You cannot update the firmware on an endpoint with a corrupted backup partition.

Activate

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

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

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

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

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

Outage Impacts of Direct Firmware Upgrades

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

Outage Impact of a Fabric Interconnect Firmware Upgrade

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

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

Outage Impact of a Cisco UCS Manager Firmware Upgrade

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

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

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

Outage Impact of an I/O Module Firmware Upgrade

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

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

Outage Impact of a CIMC Firmware Upgrade

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

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

Outage Impact of an Adapter Firmware Upgrade

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

- The server reboots.
- Server traffic is disrupted.

Adapter Firmware

Updating and Activating the Firmware on an Adapter

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

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope adapter** *chassis-id / blade-id / adapter-id*	Enters chassis server adapter mode for the specified adapter.
Step 2	UCS-A /chassis/server/adapter # **show image**	Displays the available software images for the adapter.
Step 3	UCS-A /chassis/server/adapter # **update firmware** *version-num*	Updates the selected firmware version on the adapter.
Step 4	UCS-A /chassis/server/adapter # **commit-buffer**	(Optional) Commits the transaction. Use this step only if you intend to use the **show firmware** command in Step 5 to verify that the firmware update completed successfully before activating the firmware in Step 6. You can skip this step and

	Command or Action	Purpose
		commit the **update-firmware** and **activate-firmware** commands in the same transaction; however, if the firmware update does not complete successfully, the firmware activation does not start. Cisco UCS Manager copies the selected firmware image to the backup memory partition and verifies that image is not corrupt. The image remains as the backup version until you explicitly activate it.
Step 5	UCS-A /chassis/server/adapter # **show firmware**	(Optional) Displays the status of the firmware update. Use this step only if you want to verify that the firmware update completed successfully. The firmware update is complete when the update status is Ready. The CLI does not automatically refresh, so you may have to enter the **show firmware** command multiple times until the task state changes from Updating to Ready. Continue to Step 6 when the update status is Ready.
Step 6	UCS-A /chassis/server/adapter # **activate firmware** *version-num* [**set-startup-only**]	Activates the selected firmware version on the adapter. Use the **set-startup-only** keyword if you want to move the activated firmware into the pending-next-boot state and not immediately reboot the server. The activated firmware does not become the running version of firmware on the adapter until the server is rebooted. You cannot use the **set-startup-only** keyword for an adapter in the host firmware package.
Step 7	UCS-A /chassis/server/adapter # **commit-buffer**	Commits the transaction. 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.
Step 8	UCS-A /chassis/server/adapter # **show firmware**	(Optional) Displays the status of the firmware activation. Use this step only if you want to verify that the firmware activation completed successfully. The CLI does not automatically refresh, so you may have to enter the **show firmware** command multiple times until the task state changes from Activating to Ready.

The following example updates and activates the adapter firmware to version 2.2(1b) in the same transaction, without verifying that the firmware update and firmware activation completed successfully:

```
UCS-A# scope adapter 1/1/1
UCS-A# /chassis/server/adapter # show image
Name                                               Type                  Version       State
-------------------------------------------------- --------------------- ------------- -----
ucs-m81kr-vic.2.2.1b.bin                            Adapter               2.2(1b)
Active
```

```
UCS-A# /chassis/server/adapter # update firmware 2.2(1b)
UCS-A# /chassis/server/adapter* # activate firmware 2.2(1b) set-startup-only
UCS-A# /chassis/server/adapter* # commit-buffer
UCS-A# /chassis/server/adapter #
```

The following example updates the adapter firmware to version 2.2(1b), verifies that the firmware update completed successfully before starting the firmware activation, activates the adapter firmware, and verifies that the firmware activation completed successfully:

```
UCS-A# scope adapter 1/1/1
UCS-A# /chassis/server/adapter # show image
Name                                                Type                  Version       State
--------------------------------------------------- --------------------- ------------- -----
ucs-m81kr-vic.2.2.1b.bin                             Adapter               2.2(1b)
Active

UCS-A# /chassis/server/adapter # update firmware 2.2(1b)
UCS-A# /chassis/server/adapter* # commit-buffer
UCS-A# /chassis/server/adapter # show firmware
Adapter 1:
    Running-Vers: 2.1(2a)
    Package-Vers: 2.1(2a)B
    Update-Status: Updating
    Activate-Status: Ready

UCS-A# /chassis/server/adapter # show firmware
Adapter 1:
    Running-Vers: 2.1(2a)
    Package-Vers: 2.1(2a)B
    Update-Status: Ready
    Activate-Status: Ready

UCS-A# /chassis/server/adapter # activate firmware 2.2(1b)
Warning: When committed this command will reset the end-point
UCS-A# /chassis/server/adapter* # commit-buffer
UCS-A# /chassis/server/adapter # show firmware
Adapter 1:
    Running-Vers: 2.1(2a)
    Package-Vers: 2.1(2a)B
    Update-Status: Ready
    Activate-Status: Activating

UCS-A# /chassis/server/adapter # show firmware
Adapter 1:
    Running-Vers: 2.1(2a)
    Package-Vers: 2.1(2a)B
    Update-Status: Ready
    Activate-Status: Pending Next Boot

UCS-A# /chassis/server/adapter # exit
UCS-A# /chassis/server # cycle cycle-immediate
UCS-A# /chassis/server* # commit-buffer
UCS-A# /chassis/server # scope adapter 1
UCS-A# /chassis/server/adapter # show firmware
Adapter 1:
    Running-Vers: 2.2(1b)
    Package-Vers: 2.2(1b)B
    Update-Status: Ready
    Activate-Status: Ready
UCS-A# /chassis/server/adapter #
```

BIOS Firmware

Updating and Activating the BIOS Firmware on a Server

Important You can update and activate BIOS firmware on a server using the Cisco UCS Manager CLI on all M3 generation servers. The earlier servers do not support BIOS firmware update using the Cisco UCS Manager CLI.

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

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope server** *chassis-id | blade-id*	Enters chassis server mode for the specified server.
Step 2	UCS-A /chassis/server # scope bios	Enters chassis server BIOS mode.
Step 3	UCS-A /chassis/server/bios # **show image**	Displays the available BIOS firmware images.
Step 4	UCS-A /chassis/server/bios # **update firmware** *version-num*	Updates the selected BIOS firmware for the server.
Step 5	UCS-A /chassis/server/bios # **commit-buffer**	(Optional) Commits the transaction. Use this step only if you intend to use the **show firmware** command in Step 6 to verify that the firmware update completed successfully before activating the firmware in Step 7. You can skip this step and commit the **update-firmware** and **activate-firmware** commands in the same transaction; however, if the firmware update does not complete successfully, the firmware activation does not start. Cisco UCS Manager copies the selected firmware image to the backup memory partition and verifies that image is not corrupt. The image remains as the backup version until you explicitly activate it.
Step 6	UCS-A /chassis/server/bios # **show firmware**	(Optional) Displays the status of the firmware update.

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

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

```
UCS-A# scope server 1/1
UCS-A# /chassis/server # scope bios
UCS-A# /chassis/server/bios # show image
Name                                 Type         Version
------------------------------------ ------------ -------
ucs-b230-m1-bios.B230.2.0.1.1.49.gbin Server Bios  B230.2.0.1.1.49
ucs-b230-m1-bios.B230.2.0.2.0.00.gbin Server Bios  B230.2.0.2.0.00

UCS-A# /chassis/server/bios # update firmware B230.2.0.2.0.00
UCS-A# /chassis/server/bios* # activate firmware B230.2.0.2.0.00
UCS-A# /chassis/server/bios* # commit-buffer
UCS-A# /chassis/server/bios #
```

CIMC Firmware

Updating and Activating the CIMC Firmware on a Server

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

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

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope server** *chassis-id / blade-id*	Enters chassis server mode for the specified server.
Step 2	UCS-A /chassis/server # **scope cimc**	Enters chassis server CIMC mode.
Step 3	UCS-A /chassis/server/cimc # **show image**	Displays the available software images for the adapter.
Step 4	UCS-A /chassis/server/cimc # **update firmware** *version-num*	Updates the selected firmware version on the CIMC in the server.
Step 5	UCS-A /chassis/server/cimc # **commit-buffer**	(Optional) Commits the transaction. Use this step only if you intend to use the **show firmware** command in Step 6 to verify that the firmware update completed successfully before activating the firmware in Step 7. You can skip this step and commit the **update-firmware** and **activate-firmware** commands in the same transaction; however, if the firmware update does not complete successfully, the firmware activation does not start. Cisco UCS Manager copies the selected firmware image to the backup memory partition and verifies that image is not corrupt. The image remains as the backup version until you explicitly activate it.
Step 6	UCS-A /chassis/server/cimc # **show firmware**	(Optional) Displays the status of the firmware update. Use this step only if you want to verify that the firmware update completed successfully. The firmware update is complete when the update status is Ready. The CLI does not automatically refresh, so you may have to enter the **show firmware** command multiple times until the task state changes from Updating to Ready. Continue to Step 7 when the update status is Ready.
Step 7	UCS-A /chassis/server/cimc # **activate firmware** *version-num*	Activates the selected firmware version on the CIMC in the server.
Step 8	UCS-A /chassis/server/cimc # **commit-buffer**	Commits the transaction.

	Command or Action	Purpose
Step 9	UCS-A /chassis/server/cimc # **show firmware**	(Optional) Displays the status of the firmware activation. Use this step only if you want to verify that the firmware activation completed successfully. The CLI does not automatically refresh, so you may have to enter the **show firmware** command multiple times until the task state changes from Activating to Ready.

The following example updates and activates the CIMC firmware to version 2.2(1b) in the same transaction, without verifying that the firmware update and firmware activation completed successfully:

```
UCS-A# scope server 1/1
UCS-A# /chassis/server # scope cimc
UCS-A# /chassis/server/cimc # show image
Name                                        Type               Version
------------------------------------------- ----------------- -------------
ucs-b200-m1-k9-cimc.2.2.1b.bin              CIMC               2.2(1b)
ucs-b200-m3-k9-cimc.2.2.1b.bin              CIMC               2.2(1b)
ucs-b22-m3-k9-cimc.2.2.1b.bin               CIMC               2.2(1b)
...

UCS-A# /chassis/server/cimc # update firmware 2.2(1b)
UCS-A# /chassis/server/cimc* # activate firmware 2.2(1b) set-startup-only
UCS-A# /chassis/server/cimc* # commit-buffer
UCS-A# /chassis/server/cimc #
```

The following example updates the CIMC firmware to version 2.2(1b), verifies that the firmware update completed successfully before starting the firmware activation, activates the CIMC firmware, and verifies that the firmware activation completed successfully:

```
UCS-A# scope server 1/1
UCS-A# /chassis/server # scope cimc
UCS-A# /chassis/server/cimc # show image
Name                                        Type               Version
------------------------------------------- ----------------- -------------
ucs-b200-m1-k9-cimc.2.2.1b.bin              CIMC               2.2(1b)
ucs-b200-m3-k9-cimc.2.2.1b.bin              CIMC               2.2(1b)
ucs-b22-m3-k9-cimc.2.2.1b.bin               CIMC               2.2(1b)
...

UCS-A# /chassis/server/cimc # update firmware 2.2(1b)
UCS-A# /chassis/server/cimc* # commit-buffer
UCS-A# /chassis/server/cimc # show firmware
Running-Vers    Update-Status   Activate-Status
--------------- --------------- ---------------
2.1(1)          Updating        Ready

UCS-A# /chassis/server/cimc # show firmware
Running-Vers    Update-Status   Activate-Status
--------------- --------------- ---------------
2.1(1)          Ready           Ready

UCS-A# /chassis/server/cimc # activate firmware 2.2(1b)
UCS-A# /chassis/server/cimc* # commit-buffer
UCS-A# /chassis/server/cimc # show firmware
Running-Vers    Update-Status   Activate-Status
--------------- --------------- ---------------
2.1(1)          Ready           Activating
```

```
UCS-A# /chassis/server/cimc # show firmware
Running-Vers    Update-Status   Activate-Status
--------------- --------------- ---------------
2.2(1b)          Ready           Ready
```

IOM Firmware

PSU Firmware Update

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

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

Updating the Firmware on a PSU

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

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope chassis** *chassis-id*	Enters chassis mode for the specified chassis.
Step 2	UCS-A /chassis # **scope psu** *psu-id*	Enters PSU mode for the specified PSU.
Step 3	UCS-A /chassis/psu # **show detail**	Displays the available software images for the PSU.
Step 4	UCS-A /chassis/psu # **update firmware** *version-num* [**force**]	Updates the selected firmware version on the PSU. You can use the optional **force** keyword to activate the firmware regardless of any possible incompatibilities or currently executing tasks. **Caution** Review the checklist that displays and ensure you have met all the requirements before you continue with the upgrade.
Step 5	UCS-A /chassis/psu # **commit-buffer**	(Optional) Commits the transaction. Cisco UCS Manager copies the selected firmware image to the backup memory partition and verifies that image is not

	Command or Action	Purpose
		corrupt. The image remains as the backup version until you explicitly activate it.

The following example shows how to update the PSU firmware and commit the transaction:

```
UCS-A# scope chassis 1
UCS-A# /chassis # scope psu 2
UCS-A# /chassis/psu # show detail
PSU:
    PSU: 2
    Overall Status: Operable
    Operability: Operable
    Threshold Status: OK
    Power State: On
    Presence: Equipped
    Thermal Status: OK
    Voltage Status: OK
    Product Name: Platinum II AC Power Supply for UCS 5108 Chassis
    PID: UCSB-PSU-2500ACDV
    VID: V00
    Part Number: 341-0571-01
    Vendor: Cisco Systems Inc
    Serial (SN): AZS1705000B
    HW Revision: 0
    Firmware Version: 05.11
    Type: DV
    Wattage (W): 0
    Input Source: Unknown
    Current Task:
UCS-A# /chassis/psu # update firmware 05.10
UCS-A# /chassis/psu* # commit-buffer
UCS-A# /chassis/psu #
```

Activating the Firmware on a PSU

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

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope chassis** *chassis-id*	Enters chassis mode for the specified chassis.
Step 2	UCS-A /chassis # **scope psu** *psu-id*	Enters PSU mode for the specified PSU.
Step 3	UCS-A /chassis/psu # **activate firmware** *version-num*	Activates the selected firmware version on the PSU.
Step 4	UCS-A /chassis/psu # **commit-buffer**	Commits the transaction.

	Command or Action	Purpose
		Note Committing the transaction resets the end points.

The following example activates the PSU firmware and commits the transaction:

```
UCS-A# scope chassis 1
UCS-A# /chassis # scope psu 2
UCS-A# /chassis/psu # activate firmware 02.08.05
Warning: When committed this command will reset the end-point
UCS-A# /chassis/psu* # commit-buffer
UCS-A# /chassis/psu #
```

Board Controller Firmware

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

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

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

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

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

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

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

You can apply the capability catalog update as follows:

1. Download 2.2(4c) Infra/Catalog or 2.2(5b) Infra/Catalog software bundle. Downloading and Managing Firmware in Cisco UCS Manager, on page 19 provides detailed information about downloading software bundles.

2. Load catalog version 2.2(4c)T or 2.2(5b)T (or the catalog version included) and activate the catalog. Activating a Capability Catalog Update, on page 77 provides detailed information about activating a capability catalog through Cisco UCS Manager.
3. Decommission the newly inserted blade server.
4. Associate the service profile with the host firmware pack policy that has the earlier board controller version.

   When the service profile is associated with the updated host firmware pack policy, any false mismatch alert (such as the one caused by the CSCuu15465 bug) will not be raised any more.
5. Click **Save**.
6. Re-discover the blade server.

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

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

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

  ```
  Board controller upgraded, manual a/c power cycle required on server x
  ```

  This alarm, documented in CSCuv45173, is incorrectly categorized as a critical alarm. It does not impact the functionality of the server, and can be ignored.

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

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

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

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

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

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

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

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope server** *chassis-id* / *server-id*	Enters chassis server mode for the specified server.
Step 2	UCS-A /chassis/server # **scope boardcontroller**	Enters board controller mode for the server.
Step 3	UCS-A /chassis/server/boardcontroller # **show image**	(Optional) Displays the available software images for the board controller.
Step 4	UCS-A /chassis/server/boardcontroller # **show firmware**	(Optional) Displays the current running software image for the board controller.
Step 5	UCS-A /chassis/server/boardcontroller # **activate firmware** *version-num*	Activates the selected firmware version on the board controller in the server.
Step 6	UCS-A /chassis/server/boardcontroller # **commit-buffer**	Commits the transaction to the system configuration.

The following example activates the board controller firmware:

```
UCS-A# scope server 1/1
UCS-A# /chassis/server # scope boardcontroller
UCS-A# /chassis/server/boardcontroller # show image
Name                                   Type               Version            State
-------------------------------------- ------------------ ------------------ -----
ucs-b440-m1-pld.B440100C-B4402006.bin  Board Controller  B440100C-B4402006  Active

UCS-A# /chassis/server/boardcontroller # show firmware
BoardController:
    Running-Vers: B440100C-B4402006
    Activate-Status: Ready

UCS-A# /chassis/server/boardcontroller # activate firmware B440100C-B4402006
UCS-A# /chassis/server/boardcontroller* # commit-buffer
```

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

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

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

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

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

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

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

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

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

You can apply the capability catalog update as follows:

1. Download the 2.2(4c) Infra/Catalog or 2.2(5b) Infra/Catalog software bundle. Downloading and Managing Firmware in Cisco UCS Manager, on page 19 provides detailed information about downloading software bundles.
2. Load catalog version 2.2(4c)T or 2.2(5b)T (or the catalog version included) and activate the catalog. Activating a Capability Catalog Update, on page 77 provides detailed information about activating a capability catalog through Cisco UCS Manager.
3. Decommission the newly inserted blade server.
4. Associate the blade server with the host firmware pack policy that has the earlier board controller version.

   No false mismatch alerts are raised because the catalog has the fix for CSCuu15465.

Note This is a catalog-only fix.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope server** *chassis-id* / *server-id*	Enters chassis server mode for the specified server.
Step 2	UCS-A /chassis/server # **scope boardcontroller**	Enters board controller mode for the server.
Step 3	UCS-A /chassis/server/boardcontroller # **show image**	(Optional) Displays the available software images for the board controller.
Step 4	UCS-A /chassis/server/boardcontroller # **show firmware**	(Optional) Displays the current running software image for the board controller.
Step 5	UCS-A /chassis/server/boardcontroller # **activate firmware** *version-num*	Activates the selected firmware version on the board controller in the server.
Step 6	UCS-A /chassis/server/boardcontroller # **commit-buffer**	Commits the transaction to the system configuration.

The following example activates the M3 board controller firmware:

```
UCS-A# scope server 1/1
UCS-A# /chassis/server # scope boardcontroller
UCS-A# /chassis/server/boardcontroller # show image
Name                                  Type               Version     State
------------------------------------- ------------------ ---------   -----
ucs-b200-m3-brdprog.11.0.bin          Board Controller    11.0       Active
ucs-b22-m3-brdprog.8.0.bin            Board Controller    8.0        Active

UCS-A# /chassis/server/boardcontroller # show firmware
BoardController:
    Running-Vers: 11.0
    Package-Vers:
    Activate-Status: Ready

UCS-A# /chassis/server/boardcontroller # activate firmware 11.0
UCS-A# /chassis/server/boardcontroller* # commit-buffer
```

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

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

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

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

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

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope server** *server-id*	Enters chassis server mode for the specified server.
Step 2	UCS-A /server # **scope boardcontroller**	Enters board controller mode for the server.
Step 3	UCS-A /server/boardcontroller # **show image**	(Optional) Displays the available software images for the board controller.
Step 4	UCS-A /server/boardcontroller # **show firmware**	(Optional) Displays the current running software image for the board controller.
Step 5	UCS-A /server/boardcontroller # **activate firmware** *version-num*	Activates the selected firmware version on the board controller in the server.
Step 6	UCS-A /server/boardcontroller # **commit-buffer**	Commits the transaction to the system configuration.

The following example activates the M3 board controller firmware:

```
UCS-A# scope server 7
UCS-A# /server # scope boardcontroller
UCS-A# /server/boardcontroller # show image
Name                                    Type               Version     State
--------------------------------------- ------------------ ---------   -----
ucs-c220-m3-brdprog.3.0.bin            Board Controller    3.0       Active
ucs-c220-m3-brdprog.3.0.bin            Board Controller    3.0        Active

UCS-A# /server/boardcontroller # show firmware
BoardController:
    Running-Vers: N/A
    Package-Vers:
    Activate-Status: Ready
```

```
UCS-A# /server/boardcontroller # activate firmware 3.0 force
Warning: When committed this command will reset the end-point.

UCS-A# /server/boardcontroller* # commit-buffer
```

Cisco UCS Manager Firmware

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

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

Upgrade Validation

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

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

Activating the Cisco UCS Manager Software

Procedure

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

	Command or Action	Purpose
Step 4	UCS-A /system # **commit-buffer**	Commits the transaction. Cisco UCS Manager makes the selected version the startup version and schedules the activation to occur when the fabric interconnects are upgraded.

The following example upgrades Cisco UCS Manager to version 2.2(1b) and commits the transaction:

```
UCS-A# scope system
UCS-A# /system # show image
Name                                               Type             Version     State
-------------------------------------------------- ---------------- ----------- -----
ucs-manager-k9.2.2.1b.bin                          System           2.2(1b)      Active

UCS-A# /system # activate firmware 2.2(1b)
UCS-A# /system* # commit-buffer
UCS-A# /system #
```

Fabric Interconnect Firmware

Activating the Firmware on a Fabric Interconnect

When updating the firmware on two fabric interconnects in a high availability cluster configuration, you must activate the subordinate fabric interconnect before activating the primary fabric interconnect. For more information about determining the role for each fabric interconnect, see Verifying the High Availability Status and Roles of a Cluster Configuration, on page 14.

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

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

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope fabric-interconnect** {**a** | **b**}	Enters fabric interconnect mode for the specified fabric interconnect.
Step 2	UCS-A /fabric-interconnect # **show image**	Displays the available software images for the fabric interconnect.

	Command or Action	Purpose
Step 3	UCS-A /fabric-interconnect # **activate firmware** {**kernel-version** *kernel-ver-num* | **system-version** *system-ver-num*}	Activates the selected firmware version on the fabric interconnect.
Step 4	UCS-A /fabric-interconnect # **commit-buffer**	Commits the transaction. Cisco UCS Manager updates and activates the firmware, and then reboots the fabric interconnect and any I/O module in the data path to that fabric interconnect, disrupting data traffic to and from that fabric interconnect.

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

```
UCS-A# scope fabric-interconnect a
UCS-A /fabric-interconnect # show image
Name                                          Type                 Version
--------------------------------------------- -------------------- -----------------
ucs-6100-k9-kickstart.5.2.3.N2.2.21b.bin      Fabric Interconnect  5.2(3)N2(2.21.92)
ucs-6100-k9-system.5.2.3.N2.2.21b.bin         Fabric Interconnect  5.2(3)N2(2.21.92)

UCS-A /fabric-interconnect # activate firmware kernel-version 5.2(3)N2(2.21.92) system-version
 5.2(3)N2(2.21.92)
UCS-A /fabric-interconnect* # commit-buffer
UCS-A /fabric-interconnect #
```

Forcing a Fabric Interconnect Failover

This operation can only be performed in the Cisco UCS Manager CLI.

You must force the failover from the primary fabric interconnect.

Important During a cluster failover, the virtual IP address will be unreachable until a new primary fabric interconnect is elected.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **show cluster state**	Displays the state of fabric interconnects in the cluster and whether the cluster is HA ready.
Step 2	UCS-A# **connect local-mgmt**	Enters local management mode for the cluster.
Step 3	UCS-A (local-mgmt) # **cluster** {**force primary** | **lead** {**a** | **b**}}	Changes the subordinate fabric interconnect to primary using one of the following commands:

	Command or Action	Purpose
		force Forces local fabric interconnect to become the primary. **lead** Makes the specified subordinate fabric interconnect the primary.

The following example changes fabric interconnect b from subordinate to primary:

```
UCS-A# show cluster state
Cluster Id: 0xfc436fa8b88511e0-0xa370000573cb6c04

A: UP, PRIMARY
B: UP, SUBORDINATE

HA READY
UCS-A# connect local-mgmt
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2011, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php

UCS-A(local-mgmt)# cluster lead b
UCS-A(local-mgmt)#
```

CHAPTER 8

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.

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

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

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

Host Firmware Package

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

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

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

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

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

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

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

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

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

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

This policy ensures that the host firmware is identical on all servers associated with service profiles which use the same policy. Therefore, if you move the service profile from one server to another, the firmware versions are maintained. Also, if you change the firmware version for an endpoint in the firmware package, new versions are applied to all the affected service profiles immediately, which could cause server reboots.

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

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

Management Firmware Package

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

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

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

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

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

Stages of a Firmware Upgrade through Firmware Packages in Service Profiles

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

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

New Service Profile

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

Firmware Package Policy Creation

During this stage, you create the host firmware packages.

Service Profile Association

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

Existing Service Profile

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

Effect of Updates to Firmware Packages in Service Profiles

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

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

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

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

Creating or Updating a Host Firmware Package

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

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

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

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

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 2	UCS-A org/ # **create fw-host-pack** *pack-name*	Creates a host firmware package with the specified package name and enters organization firmware host package mode.
Step 3	UCS-A /org/fw-host-pack # **set descr** *description*	(Optional) Provides a description for the host firmware package. **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any **show** command output.
Step 4	UCS-A org/fw-host-pack # **create pack-image** "*hw-vendor-name*" "*hw-model*" {**adapter** | **board-controller** | **cimc** | **graphics-card** | **host-hba** |	Creates a package image for the host firmware package and enters organization firmware host package image mode. The *hw-vendor-name* must match the full name of the vendor, and must begin and end with quotation marks. The *hw-vendor-name* and *hw-model* values are

	Command or Action	Purpose
	host-hba-optionrom | **host-nic** | **local-disk** | **raid-controller** | **server-bios**} "*version-num*"	labels that help you easily identify the package image when you enter the **show image detail** command. The *version-num* value specifies the version number of the firmware being used for the package image. The model and model number (PID) must match the servers that are associated with this firmware package. If you select the wrong model or model number, Cisco UCS Manager cannot install the firmware update.
Step 5	UCS-A org/fw-host-pack # **create exclude-server-component** {**adapter** | **board-controller** | **cimc** | **flexflash-controller** | **graphics-card** | **host-hba** | **host-hba-optionrom** | **host-nic** | **host-nic-optionrom** | **local-disk** | **psu** | **raid-controller** | **sas-expander** | **server-bios** | **storage-controller-onboard-device** | **storage-controller-onboard-device-cpld** | **storage-device-bridge** | **unspecified**	Excludes the specified component from the host firmware package. **Note** **local-disk** is excluded from the host firmware package by default.
Step 6	UCS-A org/fw-host-pack/pack-image # **set version** *version-num*	(Optional) Specifies the package image version number. Changing this number triggers firmware updates on all components using the firmware through a service profile. Use this step only when updating a host firmware package, not when creating a package. **Note** The host firmware package can contain multiple package images. Repeat Step 4, and Step 5, to create additional package images for other components.
Step 7	UCS-A org/fw-host-pack/pack-image # **commit-buffer**	Commits the transaction. Cisco UCS Manager verifies the model numbers and vendor against all servers associated with service profiles that include this policy. If the model numbers and vendor match a firmware version in the policy, Cisco UCS Manager updates the firmware according to the settings in the maintenance policies included in the service profiles.

The following example creates the app1 host firmware package, creates an adapter package image with version 02.00.77 firmware, and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # create fw-host-pack app1
UCS-A /org/fw-host-pack* # set descr "This is a host firmware package example."
UCS-A /org/fw-host-pack* # create pack-image "Cisco Systems Inc" "N20-AQ0102" adapter
"02.00.77"
UCS-A /org/fw-host-pack/pack-image* # commit-buffer
UCS-A /org/fw-host-pack/pack-image #
```

The following example excludes the server BIOS component from the app1 host firmware package, and commits the transaction:

```
UCS-A# scope org
UCS-A /org # enter fw-host-pack app1
UCS-A /org/fw-host-pack* # create exclude-server-component server-bios
UCS-A /org/fw-host-pack/exclude-server-component* # commit-buffer
UCS-A /org/fw-host-pack/exclude-server-component #
```

What to Do Next

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

Updating a Management Firmware Package

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

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

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 2	UCS-A org/ # **scope fw-mgmt-pack** *pack-name*	Scope to a management firmware package with the specified package name and enters organization firmware management package mode.
Step 3	UCS-A /org/fw-mgmt-pack # **set descr** *description*	(Optional) Provides a description for the management firmware package. **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any **show** command output.
Step 4	UCS-A org/fw-mgmt-pack # **create pack-image**	Creates a package image for the management firmware package and enters organization firmware management package image mode. The *hw-vendor-name* and *hw-model* values are labels that help

	Command or Action	Purpose
	"*hw-vendor-name*" "*hw-model*" **cimc** "*version-num*"	you easily identify the package image when you enter the **show image detail** command. The *version-num* value specifies the version number of the firmware being used for the package image. The model and model number (PID) must match the servers that are associated with this firmware package. If you select the wrong model or model number, Cisco UCS Manager cannot install the firmware update.
Step 5	UCS-A org/fw-mgmt-pack/pack-image # **set version** *version-num*	(Optional) Specifies the package image version number. Changing this number triggers firmware updates on all components using the firmware through a service profile. Use this step only when updating a firmware package, not when creating a package.
Step 6	UCS-A org/fw-mgmt-pack/pack-image # **commit-buffer**	Commits the transaction. Cisco UCS Manager verifies the model numbers and vendor against all servers associated with service profiles that include this policy. If the model numbers and vendor match a firmware version in the policy, Cisco UCS Manager updates the firmware according to the settings in the maintenance policies included in the service profiles.

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

```
UCS-A# scope org /
UCS-A /org # scope fw-mgmt-pack cimc1
UCS-A /org/fw-mgmt-pack* # set descr "This is a management firmware package example."
UCS-A /org/fw-mgmt-pack* # create pack-image "Cisco Systems Inc" "SB-1600-CTRL" cimc
"2.3(200.166)"
UCS-A /org/fw-mgmt-pack/pack-image* # commit-buffer
UCS-A /org/fw-mgmt-pack/pack-image #
```

What to Do Next

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

CHAPTER 9

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

The Cisco UCS Infrastructure Software Bundle includes capability catalog updates. Unless otherwise instructed by Cisco Technical Assistance Center, you only need to activate the capability catalog update after you've downloaded, updated, and activated a Cisco UCS Infrastructure Software Bundle.

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

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

For information about capability catalog releases supported by specific Cisco UCS releases, see the *Release Notes for Cisco UCS Software* accessible through the *Cisco UCS B-Series Servers Documentation Roadmap* available at the following URL: http://www.cisco.com/go/unifiedcomputing/b-series-doc.

Activating a Capability Catalog Update

Procedure

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

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

```
UCS-A# scope system
UCS-A /system # scope capability
UCS-A /system/capability # activate firmware 3.0(1a)T
UCS-A /system/capability* # commit-buffer
UCS-A /system/capability #
```

Verifying that the Capability Catalog is Current

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope system**	Enters system mode.
Step 2	UCS-A /system # **scope capability**	Enters system capability mode.
Step 3	UCS-A /system/capability # **show version**	Displays the current Capability Catalog version.
Step 4	On Cisco.com, determine the most recent release of the Capability Catalog available.	For more information about the location of Capability Catalog updates, see Obtaining Capability Catalog Updates from Cisco, on page 80.
Step 5	If a more recent version of the Capability Catalog is available on Cisco.com, update the Capability Catalog with that version.	

The following example displays the current Capability Catalog version:

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

```
UCS-A /system/capability # show version
Catalog:
    Running-Vers: 1.0(8.35)Running-Vers: 3.0(1a)T
     Package-Vers: 3.0(1a)A
    Activate-Status: Ready
UCS-A /system/capability #
```

Restarting a Capability Catalog Update

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

Procedure

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

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

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

```
ucs-catalog.3.0.1a.T.bin

Catalog Updater:
    File Name                Protocol Server          Userid          Status
    ---------                -------- --------------- --------------- ------
    ucs-catalog.1.0.0.4.binucs-catalog.3.0.1a.T.bin   Scp      192.0.2.111     user1
     Applied

UCS-A /system/capability # scope cat-updater ucs-catalog.1.0.0.4.binscope cat-updater
ucs-catalog.3.0.1a.T.bin
UCS-A /system/capability/cat-updater # set server 192.0.2.112
UCS-A /system/capability/cat-updater # restart
UCS-A /system/capability/cat-updater #
```

Viewing a Capability Catalog Provider

Procedure

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

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

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

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

Fan Module:
    Vendor                   Model                    Revision
    ------------------------ ------------------------ --------
    Cisco Systems, Inc.      N10-FAN1                 0
    Cisco Systems, Inc.      N10-FAN2                 0
    Cisco Systems, Inc.      N20-FAN5                 0

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

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

```
    Revision: 0

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

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

UCS-A /system/capability #
```

Downloading Individual Capability Catalog Updates

Obtaining Capability Catalog Updates from Cisco

Procedure

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

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

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

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

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

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

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

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

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

What to Do Next

Update the Capability Catalog.

Updating the Capability Catalog from a Remote Location

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

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope system**	Enters system command mode.
Step 2	UCS-A /system # **scope capability**	Enters capability command mode.
Step 3	UCS-A /system/capability # **update catalog** *URL*	Imports and applies the specified Capability Catalog file. Specify the URL for the operation using one of the following syntax: • **ftp:**// *username@hostname* / *path* • **scp:**// *username@hostname* / *path* • **sftp:**// *username@hostname* / *path* • **tftp:**// *hostname* **:** *port-num* / *path* • **usbA:**/ *path* • **usbB:**/ *path* When a username is specified, you are prompted for a password.
Step 4	UCS-A /system/capability # **show version**	(Optional) Displays the catalog update version.
Step 5	UCS-A /system/capability # **show cat-updater** [*filename*]	(Optional) Displays the update history for a Capability Catalog file, if specified, or for all Capability Catalog file update operations.

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

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

```
UCS-A# scope system
UCS-A /system # scope capability
UCS-A /system/capability # update catalog
scp://user1@192.0.2.111/catalogs/ucs-catalog.3.0.1a.T.bin
Password:
UCS-A /system/capability # show version
Catalog:
    Update Version: 3.0(1a)T

UCS-A /system/capability # show cat-updater ucs-catalog.3.0.1a.T.bin

Catalog Updater:
    File Name                Protocol Server          Userid          Status
    ---------                -------- --------------- --------------- ------
    ucs-catalog.3.0.1a.T.bin  Scp      192.0.2.111     user1           Success

UCS-A /system/capability #
```

CHAPTER 10

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.

To verify the Management Extension version, issue the **show version** command.

Procedure

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

	Command or Action	Purpose
Step 2	UCS-A /system # **scope management-extension**	Enters system Management Extension mode.
Step 3	UCS-A /system/management-extension # **activate firmware** *firmware-version* **[force-activation]**	Activates the specified Management Extension. Use the **force-activation** keyword to activate the firmware regardless of any possible incompatibilities or currently executing tasks.
Step 4	UCS-A /system/management-extension # **commit-buffer**	Commits the transaction to the system configuration.

The following example activates the Management Extension and commits the transaction:

```
UCS-A# scope system
UCS-A /system # scope management-extension
UCS-A /system/management-extension # activate firmware 1.0(4)
CS-A /system/management-extension* # commit-buffer
```

CHAPTER 11

Verifying that the Data Path is Ready

This chapter includes the following sections:

Verifying that Dynamic vNICs Are Up and Running

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

Perform this step in the Cisco UCS Manager GUI.

Procedure

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

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

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

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

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

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

Verifying the Ethernet Data Path

Procedure

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

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

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

Verifying the Data Path for Fibre Channel Switch Mode

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

Procedure

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

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

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

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

PART II

Managing Firmware through Cisco UCS Central

CHAPTER 12

Downloading and Managing Firmware in Cisco UCS Central

This chapter includes the following sections:

Downloading Firmware from Cisco.com

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

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

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

Deleting Images from the Firmware Library

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 by selecting it and clicking delete.
- **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 Image Download from Cisco

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect operation-mgr**	Enters operations manager mode.
Step 2	UCSC(ops-mgr)# **connect policy-mgr**	Enters policy manager mode from operations manager mode.
Step 3	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a sub-domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 4	UCSC(policy-mgr) /domain-group # **scope download-policy cisco**	Enters the configuration mode.
Step 5	UCSC(policy-mgr) /domain-group/download-policy # **set**	**1** **set admin-state** **2** **set downloadinterval**dayweekon-demand **3** **set http-proxy***server:port* **4** **username***username* **5** **set password***password* **6** **set proxy-password***password* **7** **set proxy-username***username* Enters the configuration details to the system.

	Command or Action	Purpose
Step 6	UCSC(policy-mgr) /domain-group/download-policy/set # **commit-buffer**	Commits the transaction to the system.

The following example shows how to configure firmware download to Cisco UCS Central from Cisco:

```
UCSC# (ops-mgr)# connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope download-policy cisco
UCSC(policy-mgr) /domain-group/download-policy # set
admin-state  enable
downloadinterval 1 day
http-proxy  Server[:Port]
username          Username
password          Password
proxy-password    HTTP Proxy Password
proxy-username    HTTP Proxy Username
UCSC(policy-mgr) /domain-group/download-policy # commit-buffer
UCSC(policy-mgr) /domain-group/download-policy* #
```

Downloading Firmware Image from Cisco

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect operation-mgr**	Enters operations manager mode.
Step 2	UCSC(ops-mgr)# **scope firmware**	Enters the firmware management mode.
Step 3	UCSC(ops-mgr) /firmware# **scope download-source cisco**	Accesses the image metadata downloaded from Cisco website.
Step 4	UCSC(ops-mgr) /firmware/download-source# **download list**	Downloads the available firmware image metadata from Cisco.com.

The following example shows how to download a firmware image from Cisco.com to Cisco UCS Central:

```
UCSC# connect operation-mgr
UCSC(ops-mgr)# scope firmware
UCSC(ops-mgr) /firmware # scope download-source cisco
UCSC(ops-mgr) /firmware/download-source # download list
```

Viewing Image Download Status

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect operation-mgr**	Enters operations manager mode.
Step 2	UCSC(ops-mgr)# **scope firmware**	Enters the firmware management mode.
Step 3	UCSC (ops-mgr)/firmware# **show download-task detail**	Displays the details of the download task.

The following example shows how to view the download task details in Cisco UCS Central:

```
UCSC# connect operation-mgr
UCSC(ops-mgr)# scope firmware
UCSC(ops-mgr) /firmware # show download-task detail
 Download task:
File Name: mini-ucs-k9-bundle-infra.3.0.0.106.A.gbin
Protocol: Ftp
Server:
Userid: User
Path: /automation/miniucs/
Downloaded Image Size (KB): 0
Image Url:
Image Url:
Proxy Userid:
State: Downloaded
Owner: Management
Current Task:
```

Viewing Downloaded Firmware Image Bundles

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect operation-mgr**	Enters operations manager mode.
Step 2	UCSC(ops-mgr)# **scope firmware**	Enters the firmware management mode.
Step 3	UCSC(ops-mgr) /firmware # **show package**	Displays the downloaded firmware image bundles. You can view the Cisco UCS Manager and Cisco UCS Central bundles. **Note** The classic UCS Infra bundle is not provided as an option for auto-install.

The following example shows how to view the downloaded firmware image bundles in Cisco UCS Central:

```
UCSC# connect operation-mgr
UCSC(ops-mgr)# scope firmware
```

```
UCSC(ops-mgr) /firmware # show package

Name                                        Version      Download Status
-------------------------------------------  ----------  ---------------
mini-ucs-k9-bundle-infra.3.0.0.106.A.gbin 3.0(0.106)A  Downloaded
mini-ucs-k9-bundle-infra.3.0.0.153.A.gbin 3.0(0.153)A  Downloaded
mini-ucs-k9-bundle-infra.3.0.0.88.A.gbin  3.0(0.88)A   Downloaded
ucs-central-bundle.1.2.0.98.debug.bin     1.2(0.98)    Downloaded
ucs-k9-bundle-b-series.2.1.3a.B.gbin      2.1(3a)B     Downloaded
ucs-k9-bundle-b-series.2.1.3b.B.bin       2.1(3b)B     Downloaded
ucs-k9-bundle-infra.2.1.3a.A.gbin         2.1(3a)A     Downloaded
ucs-k9-bundle-infra.2.2.1.236.A.gbin      2.2(1.236)A  Downloaded
update.bin                                1.2(0.105)   Downloaded

UCSC(ops-mgr) /firmware #
```

Configuring Firmware Image Download from a Remote File System

You can download firmware image from one of the following remote file systems:

- ftp
- scp
- sftp
- tftp

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect operation-mgr**	Enters operations manager mode.
Step 2	UCSC(ops-mgr)# **scope firmware**	Enters the firmware management mode.
Step 3	UCSC (ops-mgr)/firmware# **download image**ftpscpsftptftp*image file location*	Enters firmware image download configuration and mode and specifies the remote location for firmware image.
Step 4	UCSC(ops-mgr) /firmware # download image ftp: image file location /**Password:**	Authenticates access to the remote file system.

The following example shows how to configure firmware download to Cisco UCS Central from a remote file system:

```
UCSC# connect operation-mgr
UCSC(ops-mgr)# scope firmware
UCSC(ops-mgr) /firmware # download image ftp:  Enter URL ftp:[//[username@]server][/path]
UCSC(ops-mgr) /firmware # download image ftp://image download path/Password:
UCSC(ops-mgr) /firmware #
```

Deleting Image Metadata from the Library of Images

You can only purge metadata through the CLI.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect operation-mgr**	Enters operations manager mode.
Step 2	UCSC(ops-mgr)# **scope firmware**	Enters the firmware management mode.
Step 3	UCSC(ops-mgr) /firmware# **scope download-source cisco**	Accesses the image metadata downloaded from Cisco website.
Step 4	UCSC(ops-mgr) /firmware/download-source# **purge list**	Deletes the firmware images metadata from the library of images.

The following example shows how to delete the image metadata from the library of images:

```
UCSC# connect operation-mgr
UCSC(ops-mgr)# scope firmware
UCSC(ops-mgr) /firmware # scope download-source cisco
UCSC(ops-mgr) /firmware/download-source # purge list
```

CHAPTER 13

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.

Scheduling an Infrastructure Firmware Policy Update for UCS Domains

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.

	Command or Action	Purpose
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a sub-domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope fw-infra-pack** *name*	Enters the infrastructure firmware policy mode in the domain group.
Step 4	UCSC(policy-mgr) /domain-group/fw-infra-pack # **set** *infrabundleversion*	Specifies the infrastructure policy version for the update.
Step 5	UCSC(policy-mgr) /domain-group/fw-infra-pack # **commit-buffer**	Commits the transaction to the system.

The following example shows how to schedule an infrastructure firmware policy update for a domain group from Cisco UCS Central CLI:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope fw-infra-pack default
UCSC(policy-mgr) /domain-group/fw-infra-pack # set infrabundleversion 2.1(0.475)T
UCSC(policy-mgr) /domain-group/fw-infra-pack* # commit-buffer
UCSC(policy-mgr) /domain-group/fw-infra-pack #
```

Acknowledging a Pending Activity

This procedure describes the process to acknowledge an fabric interconnect reboot pending activity from Cisco UCS Central CLI.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect operation-mgr**	Enters operations manager mode.
Step 2	UCSC(ops-mgr)# **scope domain-group** *Marketing*	Enters the domain group.
Step 3	UCSC(ops-mgr) /domain-group # **scope schedule fi-reboot**	Enters the scheduled task mode.
Step 4	UCSC(ops-mgr) /domain-group/schedule # **show token-request**	Displays the pending activities in the system.
Step 5	UCSC(ops-mgr) /domain-group/schedule # **scope token-request id sys-fw-system-ack**	Finds the pending activity.
Step 6	UCSC(ops-mgr) /domain-group/schedule/token-request # **acknowledge token-request**	Acknowledges the specified pending activity.

	Command or Action	Purpose
Step 7	UCSC(ops-mgr) /domain-group/schedule/token-request* # **commit-buffer**	Commits the transaction to the system.

The following example shows how to acknowledge a pending activity in Cisco UCS Central CLI:

```
UCSC# connect operation-mgr
UCSC(ops-mgr)# scope domain-group Marketing
UCSC(ops-mgr) /domain-group # scope schedule fi-reboot
UCSC(ops-mgr) /domain-group/schedule # show token-request
Token Request:
ID    Name        Client IP       Admin State     Oper State
----- ---------- --------------- --------------- ----------
1033 sys-fw-system-ack 10.193.23.150   Auto Scheduled  Pending Ack
UCSC(ops-mgr) /domain-group/schedule # scope token-request id sys-fw-system-ack
UCSC(ops-mgr) /domain-group/schedule/token-request # acknowledge token-request
UCSC(ops-mgr) /domain-group/schedule/token-request* # commit-buffer
UCSC(ops-mgr) /domain-group/schedule/token-request #
```

Viewing Infrastructure Firmware Packages

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a sub-domain group under the domain group root. To enter the domain group root mode, type **/** as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope fw-infra-pack** *name*	Enters the infrastructure firmware policy mode in the domain group.
Step 4	UCSC(policy-mgr) /domain-group/fw-infra-pack #**show**	Displays the infrastructure firmware packages available in the system.

The following example shows how to view the available infrastructure packages using Cisco UCS Central CLI:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope fw-infra-pack default
UCSC(policy-mgr) /domain-group/fw-infra-pack # show
Infra Pack:
Name                  Mode     Infra Bundle Version
-------------------- -------- --------------------
root/default          Staged   2.1(0.480)A
UCSC(policy-mgr) /domain-group/fw-infra-pack #
```

Creating a Host Firmware Package

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters the organizations mode for the specified organization. To enter the root mode type/ as the*org-name*.
Step 3	UCSC(policy-mgr) /org # **create fw-host-pack***policy name*	Creates the specified host firmware pack.
Step 4	UCSC(policy-mgr) /org/fw-host-pack # **set descr** *description*	Specifies the description for the host firmware policy.
Step 5	UCSC(policy-mgr) /org/fw-host-pack # **set bladebundleversion** *version number*	Specifies the blade server bundle version for the host firmware policy.
Step 6	UCSC(policy-mgr) /org/fw-host-pack # **set rackbundleversion** *version number*	Specifies the rack server bundle version for the host firmware policy.
Step 7	UCSC(policy-mgr) /org/fw-host-pack # **set mseriesbundleversion** *version number*	Specifies the M-series modular server bundle version for the host firmware policy.
Step 8	UCSC(policy-mgr) /org/fw-host-pack #**create exclude-server-component** {**adapter** | **board-controller** | **cimc** | **flexflash-controller** | **graphics-card** | **host-hba** | **host-hba-optionrom** | **host-nic** | **host-nic-optionrom** | **local-disk** | **psu** | **raid-controller** | **sas-expander** | **server-bios**}	Creates an excluded component and enters exclude server component mode. **Note** You must repeat the **exclude-server-component** command for each component that you want to exclude from the host firmware package.
Step 9	UCSC(policy-mgr) /org/fw-host-pack/exclude-server-component #**exit**	Returns to host firmware pack mode.
Step 10	UCSC(policy-mgr) /org/fw-host-pack # **commit-buffer**	Commits the transaction to the system.

The following example shows how to create a host firmware pack called FWPack1, add a blade server bundle version, exclude the psu and server-bios, and commit the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org # create fw-host-pack FWPack1
UCSC(policy-mgr) /org/fw-host-pack* # create exclude-server-component psu
UCSC(policy-mgr) /org/fw-host-pack* # create exclude-server-component psu
UCSC(policy-mgr) /org/fw-host-pack/exclude-server-component* # exit
UCSC(policy-mgr) /org/fw-host-pack* # create exclude-server-component server-bios
UCSC(policy-mgr) /org/fw-host-pack/exclude-server-component* # commit-buffer
UCSC(policy-mgr) /org/fw-host-pack/exclude-server-component #
```

Viewing Host Firmware Packages

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a sub-domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **show fw-host-pack detail**	Displays a list of host firmware packages.

The following example shows how to display available host firmware packages in Cisco UCS Central CLI:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # show fw-host-pack detail
Compute Host Pack:

Name: root/Default
Mode: Staged
Blade Bundle Version: 2.1(0.469)B
Rack Bundle Version: 2.1(0.469)C
Description: UCSC

Name: root/default
Mode: Staged
Blade Bundle Version: 2.1(0.474)B
Rack Bundle Version: 2.1(0.474)C
Description: default from UCSC

Name: root/latest
Mode: Staged
Blade Bundle Version: 2.1(0.469)B
Rack Bundle Version: 2.1(0.469)C
Description: latest

Name: root/Marketing/mytest
Mode: Staged
Blade Bundle Version: 2.1(0.469)B
Rack Bundle Version: 2.1(0.469)C
Description: Test
UCSC(policy-mgr) /domain-group #
```

Scheduling Firmware Upgrades

Firmware Upgrade Schedules

When upgrading the firmware, 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 does not reboot without explicit acknowledgment.

Creating a One Time Occurrence Schedule

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a sub-domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **create schedule onetime**	Creates a one time occurrence schedule.
Step 4	UCSC(policy-mgr) /domain-group/schedule* # **set admin-state user-ack**	Specifies user acknowledgment for the specified one time update task.
Step 5	UCSC(policy-mgr) /domain-group/schedule # **create occurrence one-time** *name*	Specifies the time for one time occurrence.
Step 6	UCSC(policy-mgr) /domain-group/schedule/one-time* # **set**	1 **concur-tasks***Maximum number of concurrent tasks* 2 **date***Start Date* 3 **max-duration***Max Duration (dd:hh:mm:ss)* 4 **min-interval***Minimum Interval Between Tasks Execution* 5 **proc-cap***Maximum Number of Tasks to Execute* Sets other related details for one time occurrence.

	Command or Action	Purpose
Step 7	UCSC(policy-mgr) /domain-group/schedule/one-time* # **commit-buffer**	Commits the transaction to the system.

The following example shows how to schedule a one time occurrence firmware update in Cisco UCS Central CLI:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # create schedule onetime
UCSC(policy-mgr) /domain-group/schedule* # set admin-state user-ack
UCSC(policy-mgr) /domain-group/schedule* # commit-buffer
UCSC(policy-mgr) /domain-group/schedule # create occurrence one-time Nov172012
UCSC(policy-mgr) /domain-group/schedule/one-time* # set
concur-tasks  Maximum Number of Concurrent Tasks
date          Start Date
max-duration  Max Duration (dd:hh:mm:ss)
min-interval  Minimum Interval Between Tasks Execution
proc-cap      Maximum Number of Tasks to Execute
UCSC(policy-mgr) /domain-group/schedule/one-time* # set date nov 17 2012 16 00 00
UCSC(policy-mgr) /domain-group/schedule/one-time* # commit-buffer
UCSC(policy-mgr) /domain-group/schedule/one-time* #
```

Viewing One Time Occurrence Schedule

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a sub-domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group/schedule* # **scope schedule one-time**	Enters the schedule mode.
Step 4	UCSC(policy-mgr) /domain-group/schedule/one-time # **show detail**	Displays the one-time schedule.

The following example shows how to display the scheduled one time occurrence in Cisco UCS Central CLI:

```
UCSC#connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope schedule onetime
UCSC(policy-mgr) /domain-group/schedule/one-time # show detail
One-Time Occurrence:
Name: Friday
Start Date: 2012-11-17T16:00:00.000
Max Duration (dd:hh:mm:ss): None
```

```
Max Concur Tasks: Unlimited
Max Tasks: Unlimited
Min Interval (dd:hh:mm:ss): None
Executed Tasks: 0
UCSC(policy-mgr) /domain-group/schedule/one-time #
```

CHAPTER 14

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

The Cisco UCS Infrastructure Software Bundle includes capability catalog updates. Unless otherwise instructed by Cisco Technical Assistance Center, you only need to activate the capability catalog update after you've downloaded, updated, and activated a Cisco UCS Infrastructure Software Bundle.

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

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

For information about capability catalog releases supported by specific Cisco UCS releases, see the *Release Notes for Cisco UCS Software* accessible through the *Cisco UCS B-Series Servers Documentation Roadmap* available at the following URL: http://www.cisco.com/go/unifiedcomputing/b-series-doc.

Configuring a Capability Catalog Upgrade

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a sub-domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr)/domain-group# **scope fw-catalog-pack**	Enters the capability catalog packages mode.

	Command or Action	Purpose
Step 4	UCSC(policy-mgr) /domain-group/fw-catalog-pack # **set catalogversion** <*catalogversion*>	Specifies the capability catalog version for this update.
Step 5	UCSC(policy-mgr) /domain-group/fw-catalog-pack* # **commit-buffer**	Commits the transaction to the system.

The following example shows how to configure a capability catalog update for a domain group from Cisco UCS Central:

```
UCSC# connect policy-mgr
UCSC(policy-mgr) /domain-group # fw-catalog-pack
UCSC(policy-mgr) /domain-group/fw-catalog-pack # set catalogversion 3.0(0.163)A
UCSC(policy-mgr) /domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group* #
```

Viewing a Capability Catalog in a Domain Group

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a sub-domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr)/domain-group# **scope fw-catalog-pack** *default*	Enters the capability catalog packages mode.
Step 4	UCSC(policy-mgr) /domain-group/fw-catalog-pack # **show detail**	Specifies the capability catalog version for this update.

The following example shows how to view the capability catalog in a domain group from Cisco UCS Central CLI:

```
UCSC# connect policy-mgr
UCSC(policy-mgr) /domain-group # fw-catalog-pack default
UCSC(policy-mgr) /domain-group/fw-catalog-pack # show detail
Catalog Pack:
Name: root/default
Mode: Staged
Catalog Version: 3.0(0.163)T
Description: default
UCSC(policy-mgr) /domain-group* #
```

CHAPTER 15

Upgrading Cisco UCS Central Firmware

This chapter includes the following sections:

Cisco UCS Central Firmware Update

You can update Cisco UCS Central firmware using the Cisco UCS Central CLI.

Upgrading Cisco UCS Central Firmware

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect local-mgmt**	Enters the local management mode.
Step 2	UCSC(local-mgmt)# **update-repository-package** *bundle name with version*	Upgrades the Cisco UCS Central firmware version to the specified level.

The following example shows how to upgrade Cisco UCS Central firmware:

```
UCSC#Connect local-mgmt
UCSC(local-mgmt)#update-repository-package <ucs-central-bundle.1.0.1S2.bin>
```