Cisco UCS Manager Firmware Management Using the CLI, Release 4.3

First Published: 2023-08-16

Last Modified: 2025-04-30

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

© 2023–2025 Cisco Systems, Inc. All rights reserved.

CONTENTS

PREFACE

Preface ix

Audience ix

Conventions ix

Related Cisco UCS Documentation xi

Documentation Feedback xi

CHAPTER 1

New and Changed Information 1

New and Changed Information 1

CHAPTER 2

Overview 5

Overview 5

Cisco UCS Manager User CLI Documentation 9

Components That Support Firmware Upgrade 10

Firmware Version Terminology 11

Cross-Version Firmware Support 12

Server Pack 12

Light Weight Upgrades 13

Service Packs 13

Service Pack Versions 14

Service Pack Rollback 15

Guidelines and Restrictions for Service Packs 15

Firmware Auto Sync for FI Cluster 16

Options for Firmware Upgrades 16

Options for Service Pack Updates 18

Firmware Upgrades through Auto Install 18

Firmware Upgrades through Firmware Packages in Service Profiles 20

Direct Firmware Upgrade at Endpoints 20
Firmware Upgrade While Migrating from Cisco UCS 6300 Series Fabric Interconnects to Cisco UCS 6500 Series Fabric Interconnects 22
Firmware Upgrade to Cisco UCS Manager Release 4.3 22
Firmware Upgrade to a Minor or a Patch Release 22
Firmware Downgrades 23
Firmware Management in Cisco UCS Central 25

CHAPTER 3 Guidelines and Prerequisites 27
Guidelines, and Best Practices for Firmware Upgrades 27
Configuration Changes and Settings that Can Impact Upgrades 27
Hardware-Related Guidelines for Firmware Upgrades 28
Firmware- and Software-Related Guidelines for Upgrades 29
Fabric Interconnect Traffic Evacuation 30
Secure Firmware Update 35
Cautions, and Guidelines for Upgrading with Auto Install 37
Cautions, and Guidelines Limitations for Managing Firmware in Cisco UCS Central 39
Prerequisites for Upgrading and Downgrading Firmware 40
Pre-Upgrade Validation Checks 41
Create Backup Files 41
Creating an All Configuration Backup File 42
Configuring the Full State Backup Policy 42
Configure Cisco Smart Call Home for Firmware Upgrade 44
Disabling Smart Call Home 45
Fault Suppression During Firmware Upgrade 45
Faults Generated Due to Reboot During the Upgrade of a Fabric Interconnect 45
Modifying Baseline Expiration Interval for Faults 46
Viewing Faults Generated During the Upgrade of a Fabric Interconnect 47
Verifying the Operability of a Fabric Interconnect 48
Verifying the High Availability Status and Roles of a Cluster Configuration 49
Configuring the Default Maintenance Policy 50
Disabling the Management Interface 52
Verifying the Status of an I/O Module 53
Verifying the Status of a Server 54

Verifying the Status of Adapters on Servers in a Chassis 54
UCS Manager Health and Pre-Upgrade Check Tool 55
Verification that the Data Path is Ready 55
Verifying that Dynamic vNICs Are Up and Running 55
Verifying the Ethernet Data Path 56
Verifying the Data Path for Fibre Channel End-Host Mode 57
Verifying the Data Path for Fibre Channel Switch Mode 58

CHAPTER 4 **Manage Firmware through Cisco UCS Manager** 61
Download and Manage Firmware in Cisco UCS Manager 61
Firmware Image Management 61
Firmware Image Headers 63
Firmware Image Catalog 63
Obtaining Software Bundles from Cisco 63
Downloading Firmware Images to the Fabric Interconnect from a Remote Location 65
Displaying the Firmware Package Download Status 67
Canceling an Image Download 67
Displaying All Available Software Images on the Fabric Interconnect 68
Displaying All Available Packages on the Fabric Interconnect 69
Determining the Contents of a Firmware Package 70
Checking the Available Space on a Fabric Interconnect 70
Firmware Upgrades through Auto Install 71
Direct Upgrade After Auto Install 72
Automatic Internal Backup 72
Prepare for Firmware Install 73
Preparing the Infrastructure Firmware Pack for Install 74
Preparing the Chassis Firmware Pack for Install 74
Preparing the Blade Host Firmware Pack for Install 75
Preparing the Rack Host Firmware Pack for Install 76
Install Infrastructure Firmware 77
Install Server Firmware 77
Required Order of Steps for Auto Install 77
Recommended Process for Upgrading Infrastructure Firmware Through Auto Install 78
Upgrade the Infrastructure Firmware with Auto Install 79

Acknowledging the Reboot of the Primary Fabric Interconnect 82
Canceling an Infrastructure Firmware Upgrade 83
Clearing the Startup Version of the Default Infrastructure Pack and the Service Pack 84
Viewing the Status of the FSM During An Infrastructure Firmware Upgrade 85
Firmware Upgrades through Firmware Packages in Service Profiles 86
Host Firmware Package 86
Stages of a Firmware Upgrade through Firmware Packages in Service Profiles 88
Effect of Updates to Firmware Packages in Service Profiles 88
Creating or Updating a Host Firmware Package 91
Firmware Automatic Synchronization 95
Setting the Firmware Auto-Sync Server Policy 95
Acknowledging the Firmware Auto Synchronization for a Server 97
Direct Firmware Upgrade at Endpoints 97
Stages of a Direct Firmware Upgrade 98
Outage Impacts of Direct Firmware Upgrades 100
Recommended Process for Directly Upgrading Infrastructure Firmware at Endpoints 101
Cisco UCS Manager Firmware 102
Activating the Cisco UCS Manager Software 103
Activating a Service Pack for the Cisco UCS Manager Software 104
IOM and IFM (IOM for Cisco UCS X-Series Servers) Firmware 105
Updating and Activating the Firmware on an IOM 106
Fabric Interconnect Firmware 109
Activating the Firmware on a Fabric Interconnect 109
Switching Over Fabric Interconnect Cluster Lead 110
Activating a Service Pack on a Fabric Interconnect 111
Adapter Firmware 113
Updating and Activating the Firmware on an Adapter 114
BIOS Firmware 117
Updating and Activating the BIOS Firmware on a Server 117
CIMC Firmware 119
Updating and Activating the CIMC Firmware on a Server 119
PSU Firmware 121
Updating the Firmware on a PSU 121
Activating the Firmware on a PSU 123

Board Controller Firmware 123

Activating the Board Controller Firmware on Cisco UCS B-Series M3 and Higher Blade Servers 125

Activating the Board Controller Firmware on a Cisco UCS C-Series M3 and Higher Rack Servers 126

CHAPTER 5 **Manage the Capability Catalog in Cisco UCS Manager** 129

Capability Catalog 129

Contents of the Capability Catalog 129

Updates to the Capability Catalog 130

Activating a Capability Catalog Update 130

Verifying that the Capability Catalog is Current 131

Viewing a Capability Catalog Provider 132

Obtaining Capability Catalog Updates from Cisco 133

Updating the Capability Catalog from a Remote Location 134

CHAPTER 6 **Troubleshoot Firmware** 137

Recovering Fabric Interconnect During Upgrade 137

Recovering Fabric Interconnects When You Do Not Have Working Images on the Fabric Interconnect or the Bootflash 137

Recovering Fabric Interconnect During Upgrade When You have Working Images on the Bootflash 141

Recovering Unresponsive Fabric Interconnects During Upgrade or Failover 142

Recovering Fabric Interconnects From a Failed FSM During Upgrade With Auto Install 143

Recovering IO Modules During Firmware Upgrade 144

Resetting an I/O Module from a Peer I/O Module 144

Preface

- Audience, on page ix
- Conventions, on page ix
- Related Cisco UCS Documentation, on page xi
- Documentation Feedback, on page xi

Audience

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

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

Conventions

Text Type	Indication
GUI elements	GUI elements such as tab titles, area names, and field labels appear in **this font**. Main titles such as window, dialog box, and wizard titles appear in **this font**.
Document titles	Document titles appear in *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`.
CLI commands	CLI command keywords appear in **this font**. Variables in a CLI command appear in *this font*.
[ ]	Elements in square brackets are optional.

Text Type	Indication
{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

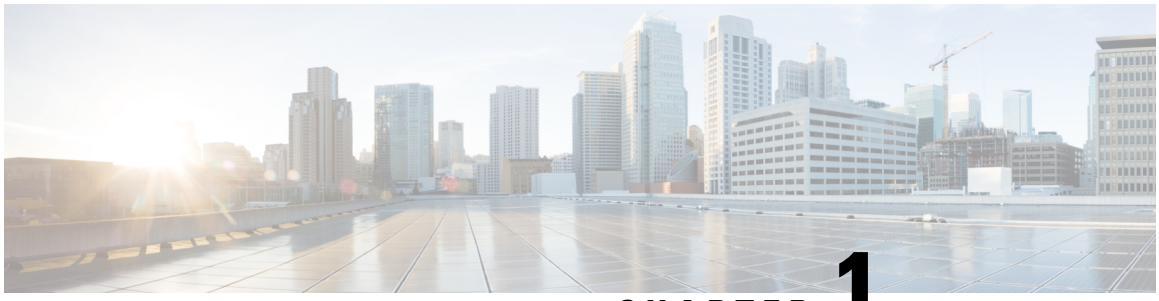
For a complete list of all B-Series documentation, see the *Cisco UCS B-Series Servers Documentation Roadmap* available at the following URL: https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/overview/guide/UCS_roadmap.html

For a complete list of all C-Series documentation, see the *Cisco UCS C-Series Servers Documentation Roadmapdoc roadmap* available at the following URL: https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/overview/guide/ucs_rack_roadmap.html.

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.

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

New and Changed Information

- New and Changed Information, on page 1

New and Changed Information

This section provides information on new feature and changed behavior in Cisco UCS Manager, Release 4.3.

Table 1: New Features and Changed Behavior in Cisco UCS Manager, Release 4.3(6a)

Feature	Description	Where Documented
Support for Cisco UCS C-Series M8 and Cisco UCS X-Series M8 servers	Cisco UCS Manager now supports Cisco UCS C240 M8 Server, Cisco UCS C220 M8 Server, and UCS X210c M8 Compute Node.	Server Pack, on page 12

Table 2: New Features and Changed Behavior in Cisco UCS Manager, Release 4.3(5a)

Feature	Description	Where Documented
Support for Cisco UCS C-Series M8 and X-Series M8 servers	Cisco UCS Manager now supports Cisco UCS C225 M8 Server and Cisco UCS X215c M8 Compute Node.	Server Pack, on page 12

Table 3: New Features and Changed Behavior in Cisco UCS Manager, Release 4.3(4b)

Feature	Description	Where Documented
Support for Cisco UCS Fabric Interconnects 9108 100G	Cisco UCS Manager now supports Cisco UCS Fabric Interconnects 9108 100G (Cisco UCS X-Series Direct).	• Overview, on page 5 • Components That Support Firmware Upgrade, on page 10 • Direct Firmware Upgrade at Endpoints, on page 20 • Verifying the Ethernet Data Path, on page 56 • Firmware Upgrades through Auto Install, on page 71 • Firmware Image Management, on page 61 • Obtaining Software Bundles from Cisco, on page 63

Table 4: New Features and Changed Behavior in Cisco UCS Manager, Release 4.3(4b)

Feature	Description	Where Documented
Support for Cisco UCS C-Series M8 server	Cisco UCS Manager now supports Cisco UCS C245 M8 Server.	Server Pack, on page 12

Table 5: New Features and Changed Behavior in Cisco UCS Manager, Release 4.3(4a)

Feature	Description	Where Documented
Cross-Version Firmware Support	The Cisco UCS Manager A bundle software (Cisco UCS Manager, Cisco NX-OS, IOM and FEX firmware) can be mixed with previous B or C bundle releases on the servers (host firmware [FW], BIOS, Cisco IMC, adapter FW and drivers).	Cross-Version Firmware Support
Force option to activate capability catalog.	Introduction of **Force** option to activate capability catalog.	Activating a Capability Catalog Update, on page 130
Deprecated command	The **show cat-updater** command is deprecated.	—

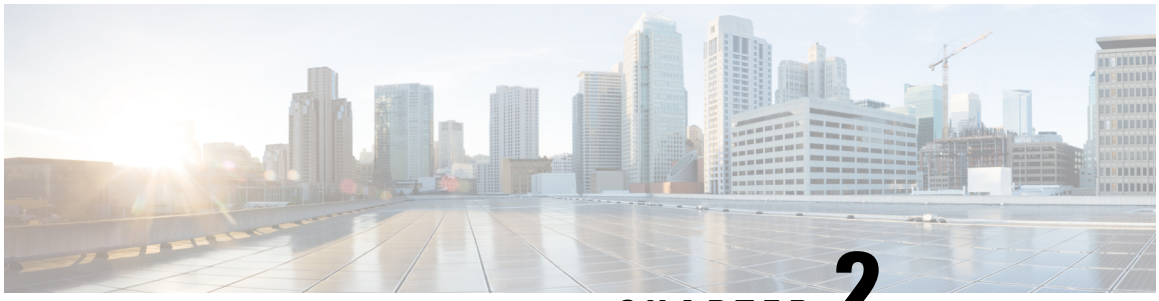
Table 6: New Features and Changed Behavior in Cisco UCS Manager, Release 4.3(2c)

Feature	Description	Where Documented
Support for Cisco UCS X-Series servers	Cisco UCS Manager supports Cisco UCS X410c M7 Compute Node. Cisco UCS X-Series servers support Intelligent Fabric Modules (IFM), which function similarly to the Input/Output Module (IOM) in Cisco UCS B-Series servers.	Server Pack, on page 12

Table 7: New Features and Changed Behavior in Cisco UCS Manager, Release 4.3(2b)

Feature	Description	Where Documented
Support for Firmware Upgrade	Cisco UCS Manager supports Firmware Upgrade to Cisco UCS Manager Release 4.3 version	Firmware Upgrade to Cisco UCS Manager Release 4.3, on page 22
Support for Cisco UCS C-Series M7 servers.	Cisco UCS Manager supports the following C-Series M7 servers: • Cisco UCS C240 M7 Server • Cisco UCS C220 M7 Server	Server Pack, on page 12
Support for Cisco UCS X9508 server chassis with Cisco UCS X-Series servers	Cisco UCS Manager supports Cisco UCSX-9508 Chassis with the following Cisco UCS X-Series servers: • Cisco UCS X210c M7 Compute Node • Cisco UCS X210c M6 Compute Node Cisco UCS X-Series servers support Intelligent Fabric Modules (IFM), which function similarly to the Input/Output Module (IOM) in Cisco UCS B-Series servers.	Server Pack, on page 12
Support for Cisco UCS 6200 Series Fabric Interconnect is deprecated	Cisco UCS Manager deprecates support for Cisco UCS 6200 Series Fabric Interconnects.	Cross-Version Firmware Support, on page 12
Support for Cisco UCS M4 servers are deprecated.	Cisco UCS Manager deprecates support for UCS B-series, C-series, and S-series M4 servers.	—

New and Changed Information



CHAPTER 2

Overview

- Overview, on page 5
- Components That Support Firmware Upgrade, on page 10
- Firmware Version Terminology, on page 11
- Cross-Version Firmware Support, on page 12
- Server Pack, on page 12
- Light Weight Upgrades, on page 13
- Firmware Auto Sync for FI Cluster, on page 16
- Options for Firmware Upgrades, on page 16
- Firmware Upgrade While Migrating from Cisco UCS 6300 Series Fabric Interconnects to Cisco UCS 6500 Series Fabric Interconnects, on page 22
- Firmware Upgrade to Cisco UCS Manager Release 4.3, on page 22
- Firmware Upgrade to a Minor or a Patch Release, on page 22
- Firmware Downgrades, on page 23
- Firmware Management in Cisco UCS Central , on page 25

Overview

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, and requires firmware to function. This guide explains how to obtain firmware and upgrade the endpoints in a Cisco UCS domain by using Cisco UCS Manager. It also details the best practices to be followed while upgrading these endpoints.

Cisco UCS Manager Release 4.3(4b) introduces the support for Cisco UCS Fabric Interconnects 9108 100G (Cisco UCS X-Series Direct) platform offers a compact and integrated solution for smaller-scale data centers by incorporating networking and management directly within the chassis, eliminating the need for separate Fabric Interconnects. It features a single-chassis system with built-in Intelligent Fabric Modules (Cisco UCS 9108 100G Intelligent Fabric Module) for efficient connectivity and high availability, supporting various speeds and allowing flexible port configurations for both LAN and SAN integration.

Cisco UCS Manager Release 4.2(3p) introduces the Cisco UCS 6536 Fabric Interconnect to Cisco UCS 6500 Series Fabric Interconnects. Cisco releases unified Cisco UCS Manager software and firmware upgrades for each of the following platforms with every release of Cisco UCS Manager:

Cisco UCS Manager Release 4.1(1) introduces the Cisco UCS 64108 Fabric Interconnect to Cisco UCS 6400 Series Fabric Interconnects.

Cisco releases unified Cisco UCS Manager software and firmware upgrades for each of the following platforms with every release of Cisco UCS Manager:

- Cisco UCS Fabric Interconnects 9108 100G with Cisco UCS X-Series servers
- Cisco UCS 6500 Series Fabric Interconnect with Cisco UCS B-Series, C-Series, and X-Series servers
- Cisco UCS 6400 Series Fabric Interconnect with Cisco UCS B-Series, and C-Series servers
- Cisco UCS 6300 Series Fabric Interconnect with Cisco UCS B-Series, and C-Series servers
- Cisco UCS 6324 Fabric Interconnect with Cisco UCS B-Series Servers and C-Series servers, which is also known as UCS Mini

The following images display the different platforms and their respective firmware bundles that Cisco UCS Manager supports, serving as illustrative examples.

Figure 1: Cisco UCS 6500 Series Fabric Interconnect with Cisco UCS B-Series, C-Series, and X-Series servers

Figure 2: Cisco UCS 6400 Series Fabric Interconnect with Cisco UCS B-Series and C-Series servers

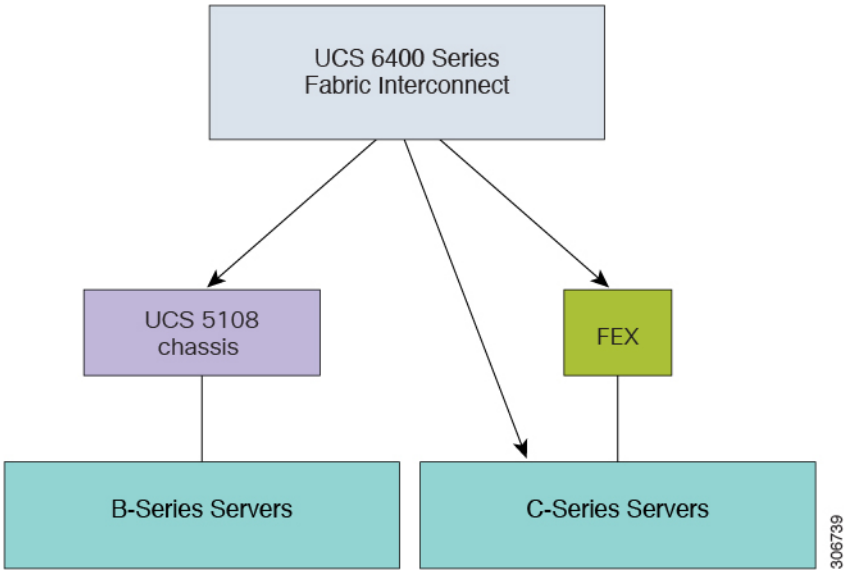


Figure 3: Cisco UCS 6300 Series Fabric Interconnect with Cisco UCS B-Series and C-Series servers

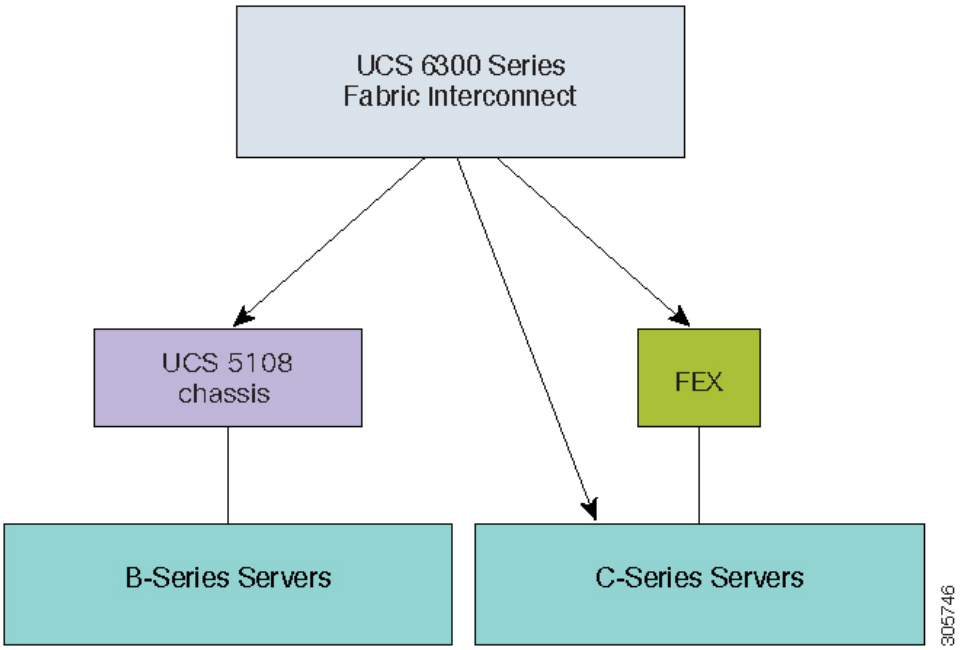
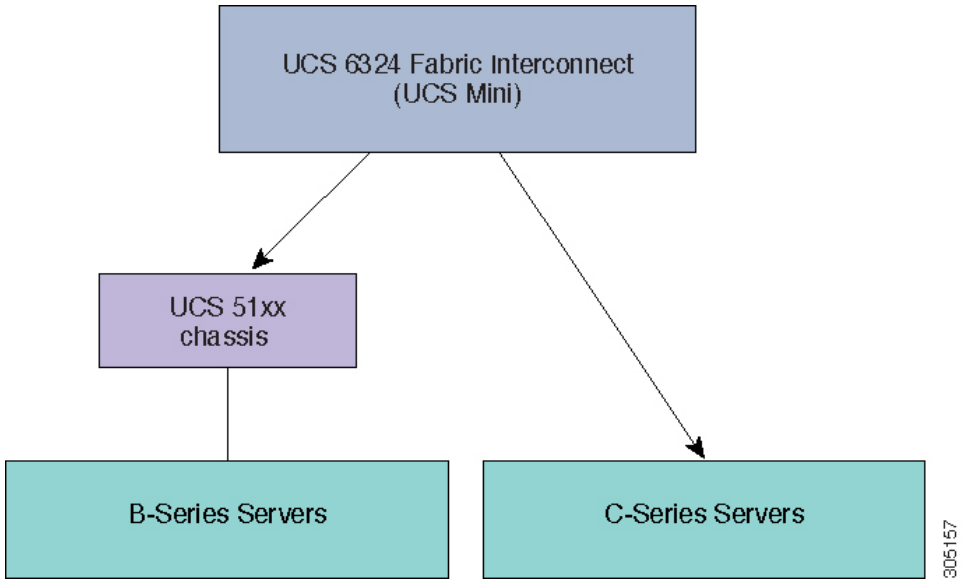


Figure 4: Cisco UCS 6324 Fabric Interconnect with Cisco UCS B-Series Servers and C-Series servers



Each release has the following firmware bundles:

- Infrastructure software bundle—This bundle is also called the A bundle. It contains the firmware images that the fabric interconnects, IO Modules/FI-IO Modules, and Cisco UCS Manager require to function.

  Cisco UCS Manager 4.1 and later releases contain three separate infrastructure bundles:

  - Cisco UCS X-Series Direct—ucs-x-direct-k9-infra.4.x.x.xxxxxx.A.bin
  - Cisco UCS 6500 Series Fabric Interconnect—ucs-6500-k9-bundle-infra.4.x.x.xxx.A.bin

- Cisco UCS 6400 Series Fabric Interconnect—ucs-6400-k9-bundle-infra.4.x.x.xxx.A.bin
- Cisco UCS 6300 Series Fabric Interconnect—ucs-6300-k9-bundle-infra.4.x.x.xxx.A.bin
- Cisco UCS 6324 Fabric Interconnect—ucs-mini-k9-bundle-infra.4.x.x.xxx.A.bin

- B-Series server software bundle—Also called the B bundle, this bundle contains the firmware images that the B-Series blade servers require to function, such as adapter, BIOS, CIMC, and board controller firmware. *Release Bundle Contents for Cisco UCS Manager*for the appropriate 4.x release provides details about the contents of the B-Series server software bundle.

Note Starting with Cisco UCS Manager Release 3.1(2), the firmware for endpoints that are common to both the B-Series and C-Series server software bundles, such as local disk, is available in both the B-Series and C-Series server software bundles.

- C-Series server software bundle—Also called the C bundle, this bundle contains the firmware images that the C-Series rack-mount servers require to function, such as adapter, BIOS, CIMC, and board controller firmware. The C bundle also contains the firmware images for Cisco UCS S3260 storage servers. *Release Bundle Contents for Cisco UCS Manager* for the appropriate 4.1 or later release provides details about the contents of the C-Series server software bundle.

Note Starting with Cisco UCS Manager Release 3.1(2), the firmware for endpoints that are common to both the B-Series and C-Series server software bundles, such as local disk, is available in both the B-Series and C-Series server software bundles.

- Capability catalog software bundle—Also called the T bundle, this bundle specifies implementation-specific tunable parameters, hardware specifics. and feature limits.

  Cisco UCS Manager uses the capability catalog to update the display and configurability of server components such as newly qualified DIMMs and disk drives. The Cisco UCS Manager Capability Catalog is a single image, but it is also embedded in Cisco UCS Manager software. Cisco UCS Manager Release 4.1 and later releases work with any 4.1 or later catalog file, but not with 4.0 or 3.2 catalog versions. If a server component is not dependent on a specific BIOS version, using it and having it recognized by Cisco UCS Manager is primarily a function of the catalog version. In addition to the catalog being bundled with UCS infrastructure releases, it can, sometimes, also be released as a standalone image.

The upgrade order for the endpoints in a Cisco UCS domain depends upon the upgrade path.

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:

- 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.

Note For 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.

Cisco UCS Manager User CLI Documentation

Cisco UCS Manager offers you a set of smaller, use-case based documentation described in the following table:

Guide	Description
Cisco UCS Manager Getting Started Guide	Discusses Cisco UCS architecture and Day 0 operations, including Cisco UCS Manager initial configuration, and configuration best practices.
Cisco UCS Manager Administration Guide	Discusses password management, role-based access configuration, remote authentication, communication services, CIMC session management, organizations, backup and restore, scheduling options, BIOS tokens and deferred deployments.
Cisco UCS Manager Infrastructure Management Guide	Discusses physical and virtual infrastructure components used and managed by Cisco UCS Manager.
Cisco UCS Manager Firmware Management Guide	Discusses downloading and managing firmware, upgrading through Auto Install, upgrading through service profiles, directly upgrading at endpoints using firmware auto sync, managing the capability catalog, deployment scenarios, and troubleshooting.
Cisco UCS Manager Server Management Guide	Discusses the new licenses, registering Cisco UCS domains with Cisco UCS Central, power capping, server boot, server profiles and server-related policies.
Cisco UCS Manager Storage Management Guide	Discusses all aspects of storage management such as SAN and VSAN in Cisco UCS Manager.
Cisco UCS Manager Network Management Guide	Discusses all aspects of network management such as LAN and VLAN connectivity in Cisco UCS Manager.
Cisco UCS Manager System Monitoring Guide	Discusses all aspects of system and health monitoring including system statistics in Cisco UCS Manager.
Cisco UCS S3260 Server Integration with Cisco UCS Manager	Discusses all aspects of management of UCS S-Series servers that are managed through Cisco UCS Manager.

Components That Support Firmware Upgrade

The various platforms that are supported by Cisco UCS Manager have different components that support firmware upgrade.

- Fabric Interconnects:
  - Cisco UCS X-Series Direct (UCSX-S9108-100G)
  - Cisco UCS 6536
  - Cisco UCS 64108
  - Cisco UCS 6454
  - Cisco UCS 6332
  - Cisco UCS 6332-16 UP
  - Cisco UCS 6324
- Chassis components:
  - Blade server chassis:
    - I/O Modules/FI-IO Modules

Note

- I/O Modules are not supported on the primary Cisco UCS Mini chassis. However, they are supported on the secondary Cisco UCS Mini chassis.
- I/O Modules are not supported on the Cisco UCS X-Series Direct, which uses the FI-I/O Modules instead.

    - Power Supply Unit
  - Cisco UCS S3260 chassis:
    - Chassis Management Controller (CMC)
    - Chassis Adapter
    - SAS Expander
    - Board Controller
- Server components:
  - Blade and Rack server:
    - Adapter
    - Cisco Integrated Management Controller (CIMC)
    - BIOS

- Storage Controller

Note Storage controller is not a supported server component in Cisco UCS Mini.

- Board Controller

- Cisco UCS S3260 storage server node:
  - Cisco Integrated Management Controller (CIMC)
  - BIOS
  - Board Controller
  - Storage Controller

Firmware Version Terminology

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

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

Each CIMC, I/O module, BIOS, CIMC, and Cisco 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.

Cross-Version Firmware Support

The Cisco UCS Manager A bundle software (Cisco UCS Manager, Cisco NX-OS, IOM and FEX firmware) can be mixed with previous B or C bundle releases on the servers (host firmware [FW], BIOS, Cisco IMC, adapter FW and drivers). To help you quickly verify valid combinations, this release includes an interactive compatibility tool, available here:

Cisco UCS Manager Cross Version Firmware Matrix

By selecting a Fabric Interconnect model along with the desired Infrastructure (A Bundle) and Host Firmware (B and C Bundles) releases, the tool dynamically displays whether each combination is a supported configuration.

You may also view the extended version of the Mixed Cisco UCS Releases Supported on Cisco UCS Fabric Interconnects at Cisco UCS Manager Cross-Version Firmware Support, Release 4.3.

For reference, the Cisco UCS Equivalency Matrix for Cisco Intersight, Cisco IMC, and Cisco UCS Managementoutlines the release timeline for Cisco Intersight, Cisco Integrated Management Controller (Cisco IMC), and Cisco UCS Manager. It includes essential information such as the date each patch was posted, the specific patch version, and the platforms that are supported by each release. By referring to this matrix, you can identify the appropriate firmware and software versions required for your servers before migrating them to Cisco Intersight. This ensures that your server infrastructure remains supported and operates efficiently during and after the transition.

Important If you implement cross-version firmware, you must ensure that the configurations for the Cisco UCS domain are supported by the firmware version on the server endpoints.

Server Pack

Server Pack allows you to dynamically support new server platforms[1] on existing infrastructure without requiring a complete firmware upgrade. This support is provided by a Cisco UCS Manager catalog image. Through this model, new B-Series, or C-Series server bundles that enable the new servers are supported on the previous infrastructure A bundle.

For example, in Release 3.1(1) and later releases, B, or C server bundles will be supported with Release 3.1(1) infrastructure A bundle. However, B, or C server bundles in Release 3.1(1) and later releases are not supported with the infrastructure A bundle of any release earlier than Release 3.1(1).

The *Release Notes for Cisco UCS Manager* for a particular release provides the complete matrix of cross-version firmware support for that release. New features introduced in the B, or C server bundles may only become available after upgrading the infrastructure A bundle to the respective version.

[1] This feature will apply to select server platforms.

The following servers currently support Server Pack:

- X-Series Servers—Cisco UCS X210c M6, UCS X210c M7, UCS X410c M7UCS X210c M8, and UCS X215c M8
- B-Series Servers—Cisco UCS B200 M5, UCS B480 M5, and UCS B200 M6
- C-Series Servers—Cisco UCS C220 M5, C240 M5, C480 M5, C220 M6, C240 M6, C225 M6, C245 M6, C220 M7, C240 M7, C225 M8, C245 M8, C240 M8, and C220 M8

If a peripheral is not supported by the existing infrastructure bundle, it will not be supported through the Server Pack feature. You must upgrade the infrastructure bundle to support this peripheral. For example, if a server is installed with new adapters that are not supported by the existing infrastructure bundle, support for these adapters requires an upgrade to the infrastructure bundle. These adapters cannot be supported through the Server Pack feature.

Because a new catalog image can be used without disrupting any hardware or software components, Server Pack provides the additional flexibility of adding new server platforms to active UCS domains without incurring the operational overhead of upgrading firmware across the whole domain.

Light Weight Upgrades

Until Cisco UCS Manager Release 3.1(3), upgrading the firmware to a patch release involved downloading and activating the complete firmware bundle even when changes were made only to specific components. The firmware versions of all components were modified even though there were no fixes made to some components. This triggered unnecessary updates for that component firmware.

Security updates to the system were also delivered through patches and lead to rebooting of the fabric interconnect and downtime.

Cisco UCS Manager Release 3.1(3) introduces light weight upgrades, which enhances firmware upgrade in the following ways:

- The firmware version of a component will be updated only if it has been modified.
- Security updates will be provided through service packs. In Release 3.1(3), light weight upgrade supports only security updates.
- Within a service pack, updates may only apply to certain components. These components may, at times, be upgraded without a fabric interconnect reboot.
- Infrastructure and server components updates are delivered through a common service pack bundle. For servers components, only the modified firmware images will be part of the service pack bundle. This results in smaller-sized service pack bundles, compared to the traditional B-Series and C-Series bundles.

Service Packs

Service packs are patches that you can use to apply security updates to Cisco UCS Manager infrastructure and server components. Service packs are specific to a base release. You can apply a service pack on a base release, but you cannot install the service pack independently.

A service pack is provided as a single bundle for infrastructure and server components. You can update all relevant infrastructure, chassis and server components by applying the service pack through Infrastructure, Chassis and Server Auto Install. In Cisco UCS Manager Release 3.1(3), the service pack bundle provides

non-disruptive updates only for infrastructure components. Among the infrastructure components, the fabric interconnect update to a service pack may require fabric interconnect rebooting in some specific scenarios such as OpenSSL fixes. The updates for server components are disruptive and will involve application downtime.

Service packs are cumulative for a maintenance release. The latest service pack will contain all the fixes from the previous service packs released for the specific maintenance release.

You can remove or update a previously applied service pack through the Cisco UCS Manager GUI and the Cisco UCS Manager CLI. Consequently, the component firmware version will be from the base release bundle.

Service packs are not applicable to maintenance releases earlier than Cisco UCS Manager Release 3.1(3).

Service Pack Versions

The following guidelines apply to service pack versions:

- A service pack can be applied only on its base bundle. For example, service pack 3.1(3)SP2 can be applied only on a 3.1(3) release. It is not compatible with a 3.1(4) release, and hence, cannot be applied on it.
- Service pack version numbering in separate maintenance releases are unrelated. For example, service packs 3.1(3)SP2 and 3.1(4)SP2 are separate and unrelated.
- The same fix can be made available for separate maintenance releases through separate service packs. For example, the same fix can be made available in 3.1(3)SP2 and 3.1(4)SP3.
- Service packs are cumulative. You can use the latest service pack version with any patch version within the same maintenance release. For example, 3.1(3)SP3 will contain all the fixes that went into 3.1(3)SP2 and 3.1(3)SP1. You can apply 3.1(3)SP3 on any 3.1(3) release.
- You cannot downgrade service packs to versions below the default service pack version for a maintenance release.
- When an upgrade or downgrade of a service pack fails, the default service pack version for that maintenance release becomes the running service pack version. For example:

  Base Bundle Version: 3.1(3b)

  Default Service Pack Version: 3.1(3)SP2(Default)

  Running Service Pack Version: 3.1(3)SP3

  While upgrading from 3.1(3)SP3 to 3.1(3)SP4, if the upgrade fails, the running service pack version displayed is 3.1(3)SP2(Default).

The following table illustrates the Release Version and Running Version Displayed in the different situations that a service pack is applied.

Release Version	Running Version Displayed
3.1(3a)	Base Bundle Version: 3.1(3a) Service Pack Version: 3.1(3)SP0(Default)
3.1(3)SP1	Base Bundle Version: 3.1(3a) Service Pack Version: 3.1(3)SP1

Release Version	Running Version Displayed
3.1(3)SP2	Base Bundle Version: 3.1(3a) Service Pack Version: 3.1(3)SP2
3.1(3b)	Base Bundle Version: 3.1(3b) Service Pack Version: 3.1(3)SP2(Default)
3.1(3)SP3	Base Bundle Version: 3.1(3b) Service Pack Version: 3.1(3)SP3

Service Pack Rollback

You can roll back a service pack that was applied to a base release. The following sections describe the changes made to the bundle version and the service pack version during various rollback scenarios.

Remove Service Pack

Bundle Version	Service Pack Version
No change is made to the bundle version.	Service pack is the default version that comes with the bundle.

Downgrade Infrastructure Bundle to an Earlier Maintenance Release

Bundle Version	Service Pack Version
Infrastructure bundle changes to the version of the earlier maintenance release.	Service pack is removed because it is not valid for the earlier maintenance release.

Downgrade Infrastructure Bundle Within the Same Maintenance Release, But with an Earlier Service Pack Version

Bundle Version	Service Pack Version
Infrastructure bundle changes to the version of the maintenance release patch.	Service pack is removed during any infrastructure upgrade or downgrade, if a corresponding service pack version is not specified during Auto-Install.

Guidelines and Restrictions for Service Packs

- When you upgrade from one service pack that requires FI reboot to another service pack that requires FI reboot, the FI is rebooted twice - once for each service pack.
- Server Auto Sync Policy is not supported for service packs.
- Auto sync of a service pack is not supported if the subordinate FI is running on a release earlier than Release 3.1(3).

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 6200 and 6300 Series FI models that are being set up for HA.

Implementation

With the earlier implementation, the user would compulsorily configure the replacement FI as non-cluster setup 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.

You are 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 as the survivor. The whole process requires minimal end user interaction while providing clear and concise feedback.

Options for Firmware Upgrades

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

Note For the steps required to upgrade one or more Cisco UCS domains to a later release, see the appropriate Cisco UCS upgrade guide. If no upgrade guide is provided, contact Cisco Technical Assistance Center. A direct upgrade from that release may not be supported.

Upgrading a Cisco UCS domain through Cisco UCS Manager

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

- Upgrade infrastructure, chassis and servers with Auto Install—This option enables you to upgrade all infrastructure components in the first stage of upgrade by using Auto Install. Then you can upgrade all chassis components through chassis firmware packages and all server endpoints through host firmware packages.
- Upgrade servers through firmware packages in service profiles—This option enables you to upgrade all server endpoints in a single step, reducing the amount of disruption caused by a server reboot. You can combine this option with the deferred deployment of service profile updates to ensure that server reboots occur during scheduled maintenance windows.
- Direct upgrades of infrastructure and server endpoints—This option enables you to upgrade many infrastructure and server endpoints directly, including the fabric interconnects, I/O modules/FI-IO modules, adapters, and board controllers. However, direct upgrade is not available for all endpoints, including the storage controller, HBA firmware, HBA option ROM and local disk. You must upgrade those endpoints through the host firmware package included in the service profile associated with the server.
- Upgrade chassis through chassis firmware packages in chassis profiles—This option enables you to upgrade all S3260 Chassis endpoints in a single step.

Note Chassis profiles and chassis firmware packages are applicable only to S3260 Chassis.

Upgrading S3X60 Server Nodes in a Cisco UCS domain through Cisco UCS Manager

You can upgrade a Cisco UCS domain with a S3260 Chassis and servers through Cisco UCS Manager in the following ways:

- Upgrade infrastructure components through Auto Install—You can upgrade the infrastructure components, such as the Cisco UCS Manager software and the fabric interconnects, in a single step by using Auto Install.
- Upgrade chassis through chassis firmware packages in chassis profiles—This option enables you to upgrade all chassis endpoints in a single step.

  Cisco UCS S3260 Server Integration with Cisco UCS Manager provides detailed information about chassis profiles and chassis firmware packages.
- Upgrade servers through firmware packages in service profiles—This option enables you to upgrade all server endpoints in a single step, reducing the amount of disruption caused by a server reboot. You can combine this option with the deferred deployment of service profile updates to ensure that server reboots occur during scheduled maintenance windows.

You can also directly upgrade the firmware at each infrastructure, chassis, and server endpoint. This option enables you to upgrade many infrastructure, chassis, and server endpoints directly, including the fabric interconnects, SAS expanders, CMCs, chassis adapters, storage controllers, and board controllers. However, direct upgrade is not available for all endpoints, including the storage controller, HBA firmware, HBA option ROM and local disk.

Cisco UCS S3260 Server Integration with Cisco UCS Manager provides detailed information about firmware management for S3X60 Server Nodes

Upgrading a Cisco UCS domain through Cisco UCS Central

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

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

You cannot directly upgrade the firmware at each endpoint. In Cisco UCS Central, you must use host firmware policy within a global service profile to upgrade host firmware components.

Options for Service Pack Updates

You can upgrade Cisco UCS firmware to a service pack through one of the following methods:

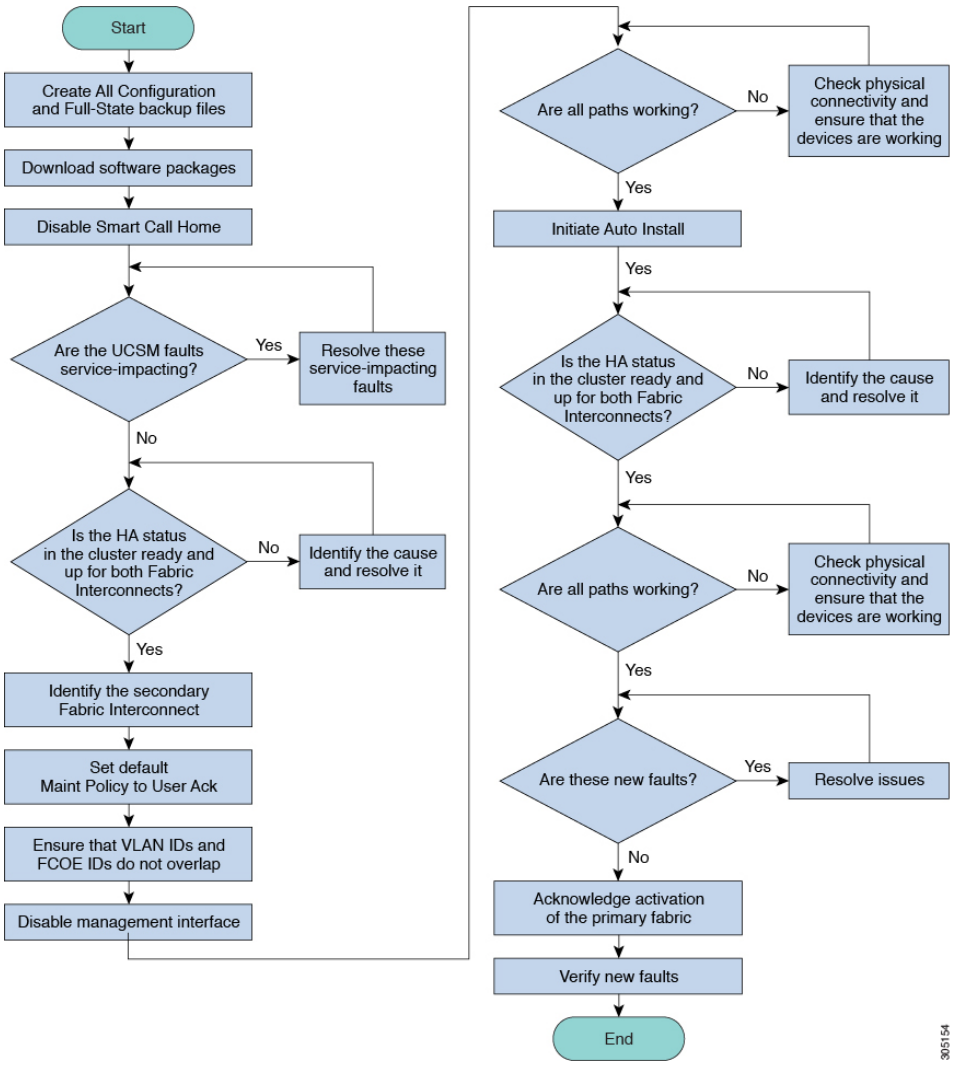
- Upgrade to a service pack through Infrastructure Auto Install
- Upgrade to a service pack through Chassis Auto Install
- Upgrade to a service pack through Server Auto Install
- Upgrade to a service pack through firmware packages in service profiles
- Upgrade to a service pack through chassis firmware packages in chassis profiles
- Directly activate a Cisco UCS Manager service pack on a base maintenance release
- Directly activate a fabric interconnect service pack on a base maintenance release

Firmware Upgrades through Auto Install

Auto Install enables you to automatically upgrade a Cisco UCS domain to the firmware versions contained in a single package, in the following 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/FI-IO modules, and Cisco UCS Manager. Figure 5: Process Flow for Automatically Installing Infrastructure Firmware , on page 19, illustrates the recommended process flow to automatically install infrastructure firmware.

Figure 5: Process Flow for Automatically Installing Infrastructure Firmware



- Install Chassis Firmware—Uses the Cisco UCS C-Series Rack-Mount UCS-Managed Server Software Bundle to upgrade the chassis components.
- Install Server Firmware—As necessary, uses the Cisco UCS B-Series Blade Server Software Bundle to upgrade all blade servers in the Cisco UCS domain; the Cisco UCS C-Series Rack-Mount UCS-Managed Server Software Bundle to upgrade all rack servers.

These 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 upgrade the chassis and server components to a different version.

Cisco strongly recommends that you use Auto Install and Fabric Evacuation to upgrade a Cisco UCS domain.

Firmware Upgrades through Firmware Packages in Service Profiles

Server firmware and BIOS versions need periodic updating across multiple servers. If this is done manually, it must be done serially and involves many hours of downtime.

You can use host firmware packages by defining a host firmware policy as an attribute of a service profile template, which is an updating template. Any change made to the service profile template is automatically made to its instantiated service profiles. Subsequently, the servers associated with the service profiles are also upgraded in parallel with the firmware version.

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.

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.

Depending on the target chassis that you use, you can directly upgrade the firmware on various components:

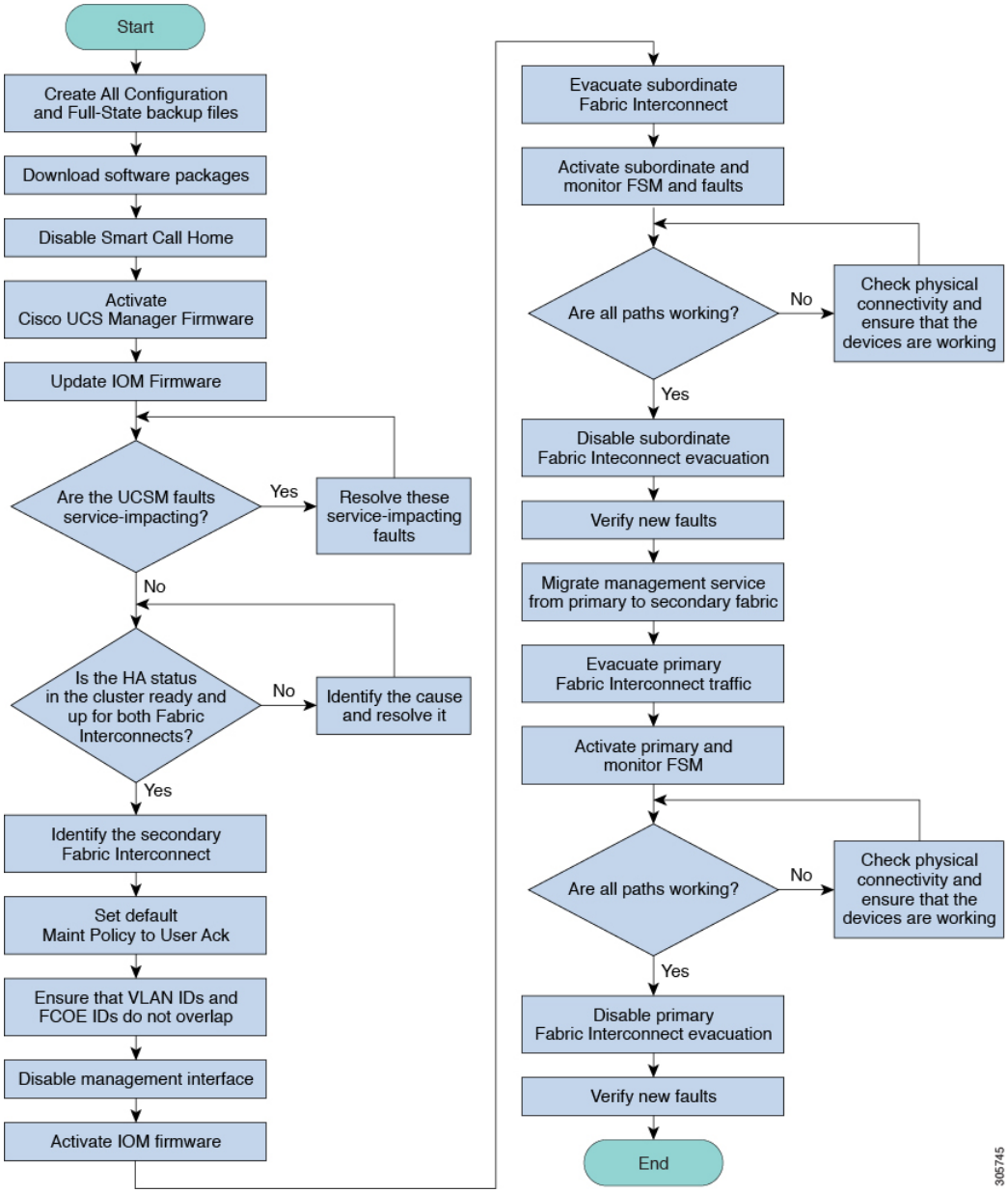
Infrastructure	UCS 5108 Chassis	UCS Rack Server	Cisco UCS S3260 Chassis

• Cisco UCS Manager
• Fabric interconnects
 	
Ensure that you upgrade Cisco UCS Manager first and then the fabric interconnects.
	• I/O modules
	• Power supply unit
	• Server:
	  • Adapter
	  • CIMC
	  • BIOS
	  • Storage controller
	  • Board controller
		• Adapter
		• CIMC
		• BIOS
		• Storage controller
		• Board controller
			• CMC
			• Chassis adapter
			• SAS expander
			• Chassis board controller
			• Server:
			  • CIMC
			  • BIOS
			  • Board controller
			  • Storage controller

Note Directly upgrading firmware on server endpoints is possible only on discovered, unassociated servers and Cisco adapters.

Figure 6: Process Flow for Manually Installing Infrastructure Firmware, on page 21, illustrates the recommended process flow.

Figure 6: Process Flow for Manually Installing Infrastructure Firmware



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 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.

Firmware Upgrade While Migrating from Cisco UCS 6300 Series Fabric Interconnects to Cisco UCS 6500 Series Fabric Interconnects

For guidelines and procedures on migrating to Cisco UCS 6500 Series Fabric Interconnect, refer the **Migration Guide for Cisco UCS Fabric Interconnects** of appropriate release version available on the Cisco UCS Manager Configuration Guides listing page.

Firmware Upgrade to Cisco UCS Manager Release 4.3

Scenarios for Firmware Upgrade to Cisco UCS Manager Release 4.3

Upgrading the Infrastructure software bundle (A bundle) directly to Cisco UCS Manager Release 4.3 is supported from Release 4.3(2b) and later releases.

The Cisco UCS Manager Upgrade/Downgrade Support Matrix lists the supported upgrade release versions and recommended upgrade path for various Cisco UCS Manager releases.

Cisco UCS Manager also supports Board Management Controller (BMC) Auto Upgrade functionality. If you migrate Cisco UCS X-Series Servers running Cisco IMC release lower than 4.3(2b) from Cisco Intersight to Cisco UCS Manager Managed mode, then Cisco UCS Manager auto upgrades Cisco IMC version to 4.3(2b).

Note Before initiating the release upgrade, refer the Firmware Management guides of respective version to understand the limitations and the correct path to perform the upgrade.

Firmware Upgrade to a Minor or a Patch Release

The release number of Cisco UCS Manager software consists of a major release identifier, minor release identifier, and patch release identifier. The minor release identifier and patch release identifier are listed together in parentheses. For example, if the software version number is **4.3(2b)**:

- **4.3** is the major release identifier
- **2** is the minor release identifier
- **b** is the patch release identifier

Read together, it indicates the **b** patch of the **first** release of the **4.3** release train.

Firmware upgrade to maintenance releases and patches within a major release are released in the same way as for the major release.

For more information about what is in each maintenance release and patch, see Release Notes for Cisco UCS Manager, Release 4.3.

Firmware Downgrades

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

Note The Cisco UCS Manager CLI does not allow you to downgrade hardware that is not supported in the release to which you are downgrading, Cisco UCS Manager CLI displays an error message if you attempt to downgrade hardware to an unsupported release.

Downgrade From Cisco UCS Manager Release 4.2

In a system with Cisco UCS 64108 Fabric Interconnects, you cannot downgrade from Cisco UCS Manager Release 4.1.

MD5 SNMPv3 User Authentication

When downgrading to a release earlier than Cisco UCS Manager Release 3.2(3), SNMPv3 users with MD5 authentication will not be deployed. To deploy such a user, do one of the following:

- Modify the **Auth Type** field to **SHA**.
- Delete the user and recreate it.

AES Privacy Protocol for SNMPv3 Users

Cisco UCS Manager Release 3.2(3) and later releases do not support SNMPv3 users without AES encryption. Hence, when downgrading to a release earlier than Cisco UCS Manager Release 3.2(3), SNMPv3 users without AES encryption will not be deployed. To deploy such a user, do one of the following:

- Enable **AES-128** encryption.
- Delete the user and recreate it.

Cisco UCS Domain with UCS M5 Servers

In a Cisco UCS domain with UCS M5 servers, when you downgrade from Cisco UCS Manager Release 3.2(1) to earlier releases, ensure that you decommission the UCS M5 servers. This is because UCS M5 servers are supported only by Cisco UCS Manager Release 3.2(1) and later releases.

If you downgrade from Cisco UCS Manager Release 3.2(1) to earlier releases without decommissioning UCS M5 servers, upgrade validation will fail and Cisco UCS Manager will prompt you to decommission the servers before continuing with the downgrade operation.

Board Controller Firmware for Blade Servers

Important

- You never need to downgrade the board controller firmware.

  The board controller firmware in Cisco UCS B-Series blade servers is not designed to be downgraded. When you are performing a full system firmware downgrade operation, if the system displays this error message “Error: Update failed: Server does not support board controller downgrade”, it is safe to ignore the error message and continue with downgrading system firmware. Cisco UCS Manager will automatically skip over the board controller firmware and continue with the downgrade of the other firmware components.

- 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.

Unsupported Features Must Be Unconfigured Before Downgrade

If you plan to downgrade a Cisco UCS domain to an earlier release, you must first unconfigure all features from the current release that are not supported in the earlier release and correct all failed configurations. If you downgrade B, or C server bundles without unconfiguring unsupported features, the feature may not work in the downgraded release. For example, the On Next Reboot maintenance policy is supported by the 3.1 B, and C bundles. If you downgrade any server bundle, this maintenance policy option will not work for the corresponding server.

If you attempt to downgrade the infrastructure bundle without unconfiguring all features that are not supported in the earlier release, the downgrade may fail.

SNMP Must be Disabled Before Downgrade

You must disable SNMP before downgrading from Cisco UCS Manager Release 3.2 to an earlier release. The downgrade process does not begin until SNMP is disabled.

Recommended Order of Steps for Firmware Downgrades

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

1. Retrieve the configuration backup from the release to which you want to downgrade. This is the backup you created when you upgraded to the current release.
2. Unconfigure the features that are not supported in the release to which you want to downgrade.
3. Create Full State and All Configuration backup files.
4. Downgrade Cisco UCS Manager.
5. Perform an erase-config.
6. Import the configuration backup from the release to which you downgraded.

Note Steps 5 and 6 are optional. Perform these steps only if the existing configuration becomes unusable. In this case, import the configuration backup either from Step 1 or Step 3.

Firmware Management in Cisco UCS Central

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

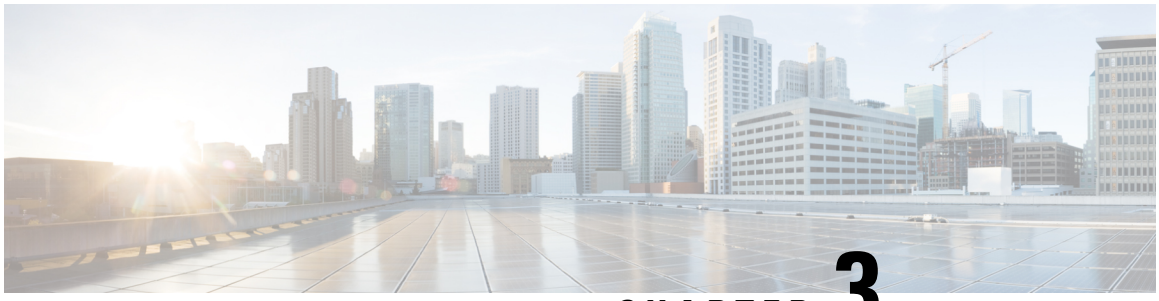
Note To manage Cisco UCS domains firmware from Cisco UCS Central, you must enable the global firmware management option in Cisco UCS Manager. You can enable the global firmware management option when you register Cisco UCS Manager with Cisco UCS Central. You can also turn the global management option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

Important Do not unregister a Cisco UCS domain from Cisco UCS Central.

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

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

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



CHAPTER 3

Guidelines and Prerequisites

- Guidelines, and Best Practices for Firmware Upgrades, on page 27
- Cautions, and Guidelines Limitations for Managing Firmware in Cisco UCS Central, on page 39
- Prerequisites for Upgrading and Downgrading Firmware, on page 40
- Pre-Upgrade Validation Checks, on page 41
- Verification that the Data Path is Ready, on page 55

Guidelines, and Best Practices for Firmware Upgrades

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

Configuration Changes and Settings that Can Impact Upgrades

Depending on the configuration of your Cisco UCS domain, the upgrade process may require you to make additional changes.

Default Maintenance Policy Should be Configured for User Acknowledgment

The default maintenance policy is configured to immediately reboot the server when disruptive changes are made to the service profile, such as server firmware upgrades through a host maintenance policy. We recommend that you change the reboot policy setting in the default maintenance policy to **user acknowledgment** to avoid unexpected disruption of server traffic.

When you configure the reboot policy in the default maintenance policy to **user acknowledgment**, the list of disruptive changes are listed with the pending activities. You can then control when the servers are rebooted.

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

Caution In Cisco UCS 1.4 and earlier releases, Ethernet VLANs and FCoE VLANs could have overlapping VLAN IDs. However, starting with Cisco UCS release 2.0, overlapping VLAN IDs are not allowed. If Cisco UCS Manager detects overlapping VLAN IDs during an upgrade, it raises a critical fault. If you do not reconfigure your VLAN IDs, Cisco UCS Manager raises a critical fault and drops Ethernet traffic from the overlapped VLANs. Therefore, we recommend that you ensure there are no overlapping Ethernet and FCoE VLAN IDs before you upgrade to Cisco UCS Release 3.1 and later releases.

Be aware that when an uplink trunk is configured with VLAN ID 1 defined and set as the native VLAN, changing the Ethernet VLAN 1 ID to another value can cause network disruption and flapping on the fabric interconnects, resulting in an HA event that introduces a large amount of traffic and makes services temporarily unavailable.

For a new installation of Cisco UCS Release 3.1 and later releases, the default VLAN IDs are as follows:

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

Note If a Cisco UCS domain uses one of the default VLAN IDs, which results in overlapping VLANs, you can change one or more of the default VLAN IDs to any VLAN ID that is not used or reserved. From release 2.0 and higher, VLANs with IDs from 4043 to 4047 are reserved.

VSANs with IDs in the Reserved Range are not Operational

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

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

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

Hardware-Related Guidelines for Firmware Upgrades

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

No Server or Chassis Maintenance

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

Avoid Replacing RAID-Configured Hard Disks During or Prior to Upgrade

During or prior to Cisco UCS infrastructure and server firmware upgrades:

- Do not remove, insert or replace any local storage hard disks or SSDs in the servers.
- Ensure that no storage operations are running, including Rebuild, Association, Copyback, BGI, and so on.

Always Upgrade Third-Party Adapters through a Host Firmware Package

You cannot upgrade third-party adapters directly at the endpoints. You must upgrade the firmware on those adapters through a host firmware package.

Configure the Fabric Interconnects

The clustered fabric interconnects provide data path redundancy by design. However, to ensure that data traffic is not disrupted, you must configure redundant Ethernet and storage (FC/FCoE) interfaces within the service profile. You must also ensure that the corresponding Operating System is configured correctly to handle one fabric path outage.

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

Firmware- and Software-Related Guidelines for Upgrades

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

Determine the Appropriate Type of Firmware Upgrade for Each Endpoint

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

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

Do Not Activate All Endpoints Simultaneously in Cisco UCS Manager GUI

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

Determine Available Bootflash and Workspace Partition

The bootflash partition is dedicated solely to firmware images managed by Cisco UCS Manager. To initiate upgrade or downgrade, at least 20 percent of the bootflash partition must be available. When the bootflash partition exceeds 70 percent, faults are raised, but Auto Install proceeds. When the bootflash partition exceeds 80 percent, faults are raised and Auto Install does not proceed.

The workspace partition on the fabric interconnect stores tech support files, core files, and the debug plugin. To initiate upgrade or downgrade, at least 20 percent of the workspace partition must be available.

Determine the Impact of Activation for Adapters and I/O Modules

During a direct upgrade, you should configure **Set Startup Version Only** for an adapter. With this setting, the activated firmware moves into the pending-next-boot state, and the server is not immediately rebooted. The activated firmware does not become the running version of firmware on the adapter until the server is rebooted. You cannot configure **Set Startup Version Only** for an adapter in the host firmware package.

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

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

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

When you upgrade a Cisco UCS domain, Cisco UCS Manager restarts the components to complete the upgrade process. This restart causes events that are identical to the service disruptions and component failures that trigger Call Home alerts to be sent. If you do not disable Call Home before you begin the upgrade, alerts will be generated by the upgrade-related component, restarts and notifications will be sent out based on your Call Home configuration.

Fabric Interconnect Traffic Evacuation

Fabric interconnect traffic evacuation, introduced in Release 2.2(4), is the ability to evacuate all traffic that flows through a fabric interconnect from all servers attached to it through an IOM or FEX, while upgrading a system.

Upgrading the subordinate fabric interconnect in a system disrupts the traffic that is active on the fabric interconnect. This traffic fails over to the primary fabric interconnect.

Important

- Fabric interconnect traffic evacuation is supported only in a cluster configuration.
- You can evacuate traffic only from the subordinate fabric interconnect.
- The IOM or FEX backplane ports of the fabric interconnect on which evacuation is configured will go down, and their state will appear as **Admin down**. During the manual upgrade process, to move these backplane ports back to the **Up** state and resume traffic flow, you must explicitly configure **Admin Evac Mode** as **Off**.

You can perform fabric evacuation as follows during the manual upgrade process:

1. Stop all the traffic that is active through a fabric interconnect by configuring **Admin Evac Mode** as **On**.
2. For vNICs configured with failover, verify that the traffic has failed over by using Cisco UCS Manager or tools such as vCenter.
3. Upgrade the subordinate fabric interconnect.
4. Restart all the stopped traffic flows by configuring **Admin Evac Mode** as **Off**.
5. Change the cluster lead to the subordinate fabric interconnect.
6. Repeat steps 1 to 4 and upgrade the other fabric interconnect.

Fabric Evacuation with Auto Install

Starting with Cisco UCS Manager Release 3.1(3), you can use fabric evacuation during Auto Install. While initiating Auto Install, when you enable fabric evacuation and then begin Auto Install, the following sequence of events occur:

1. The subordinate fabric interconnect (FI-B) is evacuated and activated.
2. Failover occurs and the primary fabric interconnect (FI-A) becomes the subordinate fabric interconnect. FI-B now becomes the cluster lead.
3. FI-A is now evacuated and activated.

If you use fabric evacuation with Auto Install, and fabric evacuation was enabled on the fabric interconnect before Auto Install, fabric evacuation is disabled after Auto Install is complete.

Ensure that you do not initiate Auto Install with fabric evacuation enabled on the primary fabric interconnect. If fabric evacuation was manually enabled on the primary fabric interconnect before Auto Install, it must be manually disabled before initiating Auto Install.

Note

- Fabric interconnect traffic evacuation is supported only in a cluster configuration.
- You can evacuate traffic only from the subordinate fabric interconnect.
- The IOM or FEX backplane ports of the fabric interconnect on which evacuation is configured will go down, and their state will appear as **Admin down**. These backplane ports will move back to **Up** state after Auto Install is complete.

Stopping Traffic on a Fabric Interconnect

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 # **stop server traffic** [**force**]	Stops all the traffic that is active through the specified Fabric Interconnect. Use the **force** option to evacuate a Fabric Interconnect irrespective of its current evacuation state.
Step 3	UCS-A /fabric-interconnect # **commit-buffer**	Commits the transaction to the system configuration.

Example

This example shows how to stop all traffic that is active through Fabric Interconnect B:

```
UCS-A# scope fabric-interconnect b
UCS-A /fabric-interconnect # stop server traffic
Warning: Enabling fabric evacuation will stop all traffic through this Fabric Interconnect
 from servers attached through IOM/FEX. The traffic will fail over to the Primary Fabric
Interconnect for fail over vnics.
UCS-A /fabric-interconnect # commit-buffer
```

Restarting Traffic on a Fabric Interconnect

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 # **start server traffic**	Restarts traffic through the specified Fabric Interconnect.
Step 3	UCS-A /fabric-interconnect # **commit-buffer**	Commits the transaction to the system configuration.

Example

This example shows how to restart traffic through Fabric Interconnect B:

```
UCS-A# scope fabric-interconnect b
UCS-A /fabric-interconnect # start server traffic
```

```
Warning: Resetting fabric evacuation will cause server traffic that failed over to the
Primary Fabric Interconnect to fail back to this Fabric Interconnect.
UCS-A /fabric-interconnect # commit-buffer
```

Verifying Fabric Evacuation

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **show service-profile circuit server** *server-id*	Shows the network circuit information for the service profile associated with the specified server.

Example

This example shows the VIF paths before fabric evacuation.

Note

- VIF at Fabric Interconnect A shows that traffic is initially active through the Fabric interconnect.
- VIF at Fabric Interconnect B is passive before evacuation.

```
UCS-A# show service-profile circuit server 1/6
Service Profile: test1
Server: 1/6
    Fabric ID: A
        Path ID: 1
        VIF        vNIC            Link State  Oper State Prot State    Prot Role   Admin
Pin  Oper Pin   Transport
       ---------- --------------- ----------- ---------- ------------ ----------- ----------
 ---------- ---------
               692 eth0            Up          Active     Active        Primary     0/0
     1/15       Ether
    Fabric ID: B
        Path ID: 1
        VIF        vNIC            Link State  Oper State Prot State    Prot Role   Admin
Pin  Oper Pin   Transport
       ---------- --------------- ----------- ---------- ------------ ----------- ----------
 ---------- ---------
               693 eth0            Up          Active     Passive       Backup      0/0
     1/15       Ether
UCS-A#
```

This example shows the VIF paths after Fabric Interconnect A is evacuated.

Note
- After fail over, the VIF state at Fabric Interconnect A goes into error.
- VIF at Fabric Interconnect B takes over as active.

```
UCS-A# show service-profile circuit server 1/6
Service Profile: test1
Server: 1/6
    Fabric ID: A
        Path ID: 1
        VIF        vNIC            Link State  Oper State Prot State    Prot Role   Admin
Pin  Oper Pin   Transport
      ---------- --------------- ----------- ---------- ------------- ----------- ----------
 ---------- ---------
              692 eth0            Error       Error      Active        Primary     0/0
     0/0        Ether
    Fabric ID: B
        Path ID: 1
        VIF        vNIC            Link State  Oper State Prot State    Prot Role   Admin
Pin  Oper Pin   Transport
      ---------- --------------- ----------- ---------- ------------- ----------- ----------
 ---------- ---------
              693 eth0            Up          Active     Passive       Backup      0/0
     1/15       Ether
UCS-A#
```

Displaying the Status of Evacuation at a Fabric Interconnect

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 detail**	Displays details about the specified Fabric Interconnect.

Example

This example shows how to display the detailed status of a Fabric Interconnect.

Note Admin Evacuation and Oper Evacuation show the status of evacuation at the Fabric Interconnect.

```
 UCS-A /fabric-interconnect # show detail

Fabric Interconnect:
    ID: B
    Product Name: Cisco UCS 6248UP
    PID: UCS-FI-6248UP
    VID: V01
```

```
Vendor: Cisco Systems, Inc.
Serial (SN): SSI171400HG
HW Revision: 0
Total Memory (MB): 16165
OOB IP Addr: 10.193.32.172
OOB Gateway: 10.193.32.1
OOB Netmask: 255.255.255.0
OOB IPv6 Address: ::
OOB IPv6 Gateway: ::
Prefix: 64
Operability: Operable
Thermal Status: Ok
Admin Evacuation: On
Oper Evacuation: On
Current Task 1:
Current Task 2:
Current Task 3:
```

Secure Firmware Update

Cisco UCS Manager, Release 3.1(2) introduces secure firmware update, which enables you to update the adapter firmware securely for third-party Intel network and storage adapters. Only server administrators can upgrade or downgrade firmware for the adapters. OS administrators with root privileges are not allowed to downgrade the adapter firmware.

The following Cisco UCS servers support secure firmware update:

Secure Firmware Update Supported Network Adapters and Storage Disks

Supported Storage Disks on Cisco Blade Servers

The following Intel NVMe storage disks support secure firmware update on Cisco UCS B200 M5 Server and Cisco UCS B480 M5 Server.

Table 8: Supported NVMe Storage Disks

NVMe Storage Disks
UCSC-NVMEHW-H800
UCSC-NVMEHW-H1600
UCSC-NVMEHW-H3200
UCSC-NVMEHW-H6400
UCSC-NVMEHW-H7680

Supported Network Adapters and Storage Disks on Cisco Rack Servers

The following NVMe storage disks support secure firmware update on Cisco UCS C220 M5 Server, Cisco UCS C240 M5 Server, and Cisco UCS C480 M5 Server servers:

Table 9: Supported NVMe Storage Disks

NVMe Storage Disks
UCSC-NVMEHW-H800
UCSC-NVMEHW-H1600
UCSC-NVMEHW-H3200
UCSC-NVMEHW-H6400
UCSC-NVMEHW-H7680
UCSC-NVME-H16003 to UCSC-F-H16003
UCSC-NVME-H32003
UCSC-NVME-H38401
UCSC-NVME-H64003
UCSC-NVME-H76801

Guidelines for Secure Firmware Support on Cisco UCS Servers

Cisco UCS Manager Release 3.1(2) introduces support for secure firmware update. For Cisco UCS M5 servers, secure firmware update is introduced in Cisco UCS Manager Release 3.2(2).

Important Ensure that CIMC is running Version 2.0(13) or later and Cisco UCS Manager is running Release 3.1(2) or later releases. Secure firmware update cannot be done when the CIMC is running a version earlier than 2.0(13) and Cisco UCS Manager is running a release earlier than Release 3.1(2).

Guidelines for Blade Servers

For secure firmware update on , B200 M5, and B480 M5 servers, do the following:

- Install the UCSB-LSTOR-PT storage controller and insert the NVMe disks on a Cisco UCS B200 M5 or B480 M5 server.
- Reacknowledge the server. Refer to the *Reacknowledging a Blade Server* section in the *Cisco UCS Manager Infrastructure Management Guide, Release 3.2*.

Note Ensure that server discovery does not fail and the NVMe disks are identified by CIMC and BIOS. After the server is associated to the service profile with the default host firmware package, Auto Install is triggered. NVMe disks can be updated with the latest firmware during Auto Install.

Cisco UCS Manager, Release 3.2(1) supports NVMe boot.

Guidelines for Rack Servers

For secure firmware update on Cisco UCS C460, C240, C220 M5 servers and C480 M5 servers, do the following:

- Reacknowledge the Cisco UCS servers. Refer to the *Reacknowledging a Rack Server* section in the *Cisco UCS Manager Infrastructure Management Guide, Release 3.2*.

Note Ensure that server discovery does not fail and the NVMe disks are identified by CIMC and BIOS. After the server is associated to the service profile with the default host firmware package, Auto Install is triggered. NVMe disks can be updated with the latest firmware during Auto Install.

Cisco UCS Manager, Release 3.2(1) supports NVMe boot.

Cautions, and Guidelines for Upgrading with Auto Install

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

Note These guidelines are specific to Auto Install and are in addition to those listed in Guidelines, and Best Practices for Firmware Upgrades, on page 27.

State of the Endpoints

Before you begin an upgrade, all affected endpoints must be as follows:

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

Recommendations for the Default Host Firmware Policy

After you upgrade Cisco UCS Manager, a new host firmware policy named "default" is created, and is assigned to all service profiles that did not already include a host firmware policy. The default host firmware policy is blank. It does not contain any firmware entries for any components. This default policy is also configured for an immediate reboot rather than waiting for user acknowledgment before rebooting the servers.

During the upgrade of server firmware, you can modify the default host firmware policy to add firmware for the blade and rack-mount servers in the Cisco UCS domain. To complete the upgrade, all servers must be rebooted.

Every service profile that is assigned to the default host firmware policy reboots the associated server according to the maintenance policy included in the service profile. If the maintenance policy is set to immediate reboot, you cannot cancel the upgrade or prevent the servers from rebooting after you complete the configuration in the **Install Server Firmware** wizard. We recommend that you verify the maintenance policy associated with these service profiles to ensure that they are set for a timed reboot or for user acknowledgment.

Time, Date, and Time Zone on Fabric Interconnects Must Be Identical

To ensure that the fabric interconnects in a cluster configuration are in sync, you must ensure that they are configured for the same date, time, and time zone. We recommend that you configure an NTP server and the correct time zone in both fabric interconnects. If the date, time or time zone in the fabric interconnects are out of sync, the Auto Install might fail.

Cannot Upgrade Infrastructure and Server Firmware Simultaneously

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

Required Privileges

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

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

Impact of Host Firmware Packages on Install Server Firmware

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

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

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

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

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

Upgrading Server Firmware on Newly Added Servers

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

Note After you finish the upgrade, you can use the **Firmware Auto Sync Server** policy in Cisco UCS Manager to automatically update newly discovered servers.

Cautions, and Guidelines 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 from global to local.
- 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 associated 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.

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

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 tasks:

- Review the release notes for the Cisco UCS Manager version you plan to upgrade/downgrade.

Note Ensure to check the section titled **Deprecated Hardware and Software in Cisco UCS Manager** in the Release Notes. This section identifies hardware and software features that are no longer supported, helping you avoid issues with unsupported components during your upgrade or operations.

- Ensure that 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 non-cluster 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 Verification that the Data Path is Ready, on page 55 section.

- Verify that all servers, I/O modules, and adapters are fully functional. An inoperable server cannot be upgraded.
- Verify that the Cisco UCS domain does not include any critical or major faults. If such faults exist, you must resolve them before you upgrade the system. A critical or major fault may cause the upgrade to fail.
- Verify that all servers have been discovered. They do not need to be powered on or associated with a service profile.
- If you want to integrate a rack-mount server into the Cisco UCS domain, follow the instructions in the appropriate C-Series Rack-Mount Server Integration Guide for installing and integrating a rack-mount server in a system managed by Cisco UCS Manager.
- For Cisco UCS domains that are configured for iSCSI boot, do the following before you upgrade to Cisco UCS, Release 3.1(1) or higher:
  - Ensure that all iSCSI vNICs used across multiple service profiles have unique initiator names.
  - If any iSCSI vNICs have the same initiator name within a service profile, Cisco UCS reconfigures the service profile to have a single unique initiator name.
  - Make the corresponding IQN initiator name changes on any network storage devices to ensure that the boot LUNs are visible to the new IQN.

If Fibre Channel ports on Cisco UCS Fabric Interconnect are connected to non-Cisco products, ensure that these Fibre Channel ports are operating as individual Fibre Channel links and not aggregated into a port channel.

Note Fibre Channel port channels are not compatible with non-Cisco technology.

Pre-Upgrade Validation Checks

Ensure that you complete the following pre-upgrade validation checks before installing firmware:

Create Backup Files

When you perform a backup through Cisco UCS Manager, you take a snapshot of all or part of the system configuration and export the file to a location on your network. You can perform a backup while the system is up and running. The backup operation only saves information from the management plane. It does not have any impact on the server on network traffic.

Cisco recommends that you create the following backup files before beginning a Cisco UCS firmware upgrade:

- **All Configuration** backup file—An XML backup of all the system and logical configuration
- **Full State** backup file—A binary snapshot of the entire system

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.

Example

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 #
```

Configuring the Full State Backup Policy

Before you begin

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

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 backup-policy default**	Enters the all configuration export policy mode.
Step 3	UCS-A /org/backup-policy # **set hostname** {*hostname* | *ip-addr* | *ip6-addr*}	Specifies the hostname, IPv4 or IPv6 address of the location where the backup policy is stored. This can be a server, storage array, local drive, or any read/write media that the fabric interconnect can access through the network. **Note** If you use a hostname rather than an IPv4 or IPv6 address, you must configure a DNS server. If the Cisco UCS domain is not registered with Cisco UCS Central or DNS management is set to **local**, configure a DNS server in Cisco UCS Manager. If the Cisco UCS domain is registered with Cisco UCS Central and DNS management is set to **global**, configure a DNS server in Cisco UCS Central.
Step 4	UCS-A /org/backup-policy # **set protocol** {**ftp** | **scp** | **sftp** | **tftp**}	Specifies the protocol to use when communicating with the remote server.
Step 5	UCS-A /org/backup-policy # **set user** *username*	Specifies the username the system should use to log in to the remote server. This step does not apply if the TFTP protocol is used.
Step 6	UCS-A /org/backup-policy # **set password**	After you press **Enter**, you are prompted to enter the password. Specifies the password for the remote server username. This step does not apply if the TFTP protocol is used.
Step 7	UCS-A /org/backup-policy # **set remote-file** *filename*	Specifies the full path to the backup file. This field can contain the filename as well as the path. If you omit the filename, the backup procedure assigns a name to the file.
Step 8	UCS-A /org/backup-policy # **set adminstate** {**disable** | **enable**}	Specifies the admin state for the policy. This can be one of the following: • **enable**—Cisco UCS Manager exports the backup file using the schedule specified in the **Schedule** field.

	Command or Action	Purpose
		• **disable**—Cisco UCS Manager does not export the file.
Step 9	UCS-A /org/backup-policy # **set schedule** {**daily** | **weekly** | **bi-weekly**}	Specifies the frequency with which Cisco UCS Manager exports the backup file.
Step 10	UCS-A /org/backup-policy # **set descr** *description*	Specifies a description for the backup policy. Enter up to 256 characters. You can use any characters or spaces except ` (accent mark), \ (backslash), ^ (carat), " (double quote), = (equal sign), > (greater than), < (less than), or ' (single quote).
Step 11	UCS-A /org/backup-policy # **commit-buffer**	Commits the transaction.

Example

The following example shows how to configure the full state backup policy for a weekly backup and commit the transaction:

```
UCS-A# scope org /
UCS-A /org # scope backup-policy default
UCS-A /org/backup-policy # set hostname host35
UCS-A /org/backup-policy* # set protocol scp
UCS-A /org/backup-policy* # set user UserName32
UCS-A /org/backup-policy* # set password
Password:
UCS-A /org/backup-policy* # set remote-file /backups/full-state1.bak
UCS-A /org/backup-policy* # set adminstate enable
UCS-A /org/backup-policy* # set schedule weekly
UCS-A /org/backup-policy* # set descr "This is a full state weekly backup."
UCS-A /org/backup-policy* # commit-buffer
UCS-A /org/backup-policy #
```

Configure Cisco Smart Call Home for Firmware Upgrade

Cisco Smart Call Home is a web application that leverages the Call Home feature of Cisco UCS. Smart Call Home offers proactive diagnostics and real-time email alerts of critical system events, which results in higher network availability and increased operational efficiency. Smart Call Home is a secure connected service offered by Cisco Unified Computing Support Service and Cisco Unified Computing Mission Critical Support Service for Cisco UCS. The *Cisco UCS Manager Administration Management Guide* provides detailed information about configuring Smart Call Home.

When you upgrade firmware, Cisco UCS Manager restarts the components to complete the upgrade process. This restart can trigger email alerts. Disabling Smart Call Home will avoid creating such alerts and automatic support cases with TAC during the firmware upgrade process.

Disabling Smart Call Home

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope monitoring**	Enters monitoring mode.
Step 2	UCS-A /monitoring # **scope callhome**	Enters monitoring call home mode.
Step 3	UCS-A /monitoring/callhome # **disable**	Enables Call Home.
Step 4	UCS-A /monitoring/callhome # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example disables Smart Call Home and commits the transaction:

```
UCS-A# scope monitoring
UCS-A /monitoring # scope callhome
UCS-A /monitoring/callhome # disable
UCS-A /monitoring/callhome* # commit-buffer
UCS-A /monitoring/callhome #
```

Fault Suppression During Firmware Upgrade

Fault suppression allows you to suppress SNMP trap and Call Home notifications during a planned maintenance time. You can create a fault suppression task to prevent notifications from being sent whenever a transient fault is raised or cleared.

Faults remain suppressed until the time duration has expired, or the fault suppression tasks have been manually stopped by the user. After the fault suppression has ended, Cisco UCS Manager will send notifications for any outstanding suppressed faults that have not been cleared.

Enabling fault suppression for any component during firmware upgrade suppresses the faults related to that component until the time duration has expired, or until the component comes back up after upgrade. For example, if fabric interconnect faults are configured to be suppressed during firmware upgrade, no faults triggered by the fabric interconnect going down during upgrade will be displayed.

Faults Generated Due to Reboot During the Upgrade of a 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.

Starting with Cisco UCS Manager Release 3.1, 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 46, 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.

Example

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.

Example

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*.

Example

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.

	Command or Action	Purpose
		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.

Example

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
```

Configuring the Default Maintenance Policy

Some modifications to a service profile or to an updating service profile template can be disruptive and require a reboot of the server. A maintenance policy determines how Cisco UCS Manager reacts when a change that requires a server reboot is made to a service profile associated with a server or to an updating service profile bound to one or more service profiles.

The maintenance policy specifies how Cisco UCS Manager deploys the service profile changes. The deployment can occur in one of the following ways:

- Immediately
- When acknowledged by a user with admin privileges
- Automatically at the time specified in a schedule
- When the server boots again

Before you begin

If you plan to configure this maintenance policy for deferred deployment, create a schedule.

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 maint-policy default**	Enters the maintenance policy mode for the default maintenance policy.
Step 3	UCS-A /org/maint-policy # **set reboot-policy** {**immediate** | **timer-automatic** | **user-ack**}	When a service profile is associated with a server, the server needs to be rebooted to complete the association. Specifying the reboot-policy command determines when the reboot occurs for all service profiles that include this maintenance policy. Possible values include: • **immediate**--The server reboots as soon as the change is made to the service profile. • **timer-automatic** --You select the schedule that specifies when maintenance operations can be applied to the server using the **`set scheduler`** command. Cisco UCS reboots the server and completes the service profile changes at the scheduled time. • **user-ack** --The user must explicitly acknowledge the changes by using the **apply pending-changes** command before changes are applied. Cisco recommends that you set the reboot policy of the default maintenance policy to **user-ack**.
Step 4	(Optional) UCS-A /org/maint-policy # **set scheduler** *scheduler-name*	If the reboot-policy property is set to timer-automatic, you must select the schedule that specifies when maintenance operations can be applied to the server. Cisco UCS reboots the server and completes the service profile changes at the scheduled time.
Step 5	UCS-A /org/maint-policy # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example modifies the reboot policy of the default maintenance policy, and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # scope maint-policy default
UCS-A /org/maint-policy* # set reboot-policy user-ack
UCS-A /org/maint-policy* # commit-buffer
UCS-A /org/maint-policy #
```

Disabling the Management Interface

Before firmware upgrade, you could shut down the management interface of the secondary fabric interconnect. This ensures that any active KVM connections between any server and the management interface will reset. The GUI flow fails over to the primary fabric interconnect and reduces the time that you are disconnected from the GUI.

If Cisco UCS Manager detects a management interface failure, a failure report is generated. If the configured number of failure reports is reached, the system assumes that the management interface is unavailable and generates a fault. By default, the management interfaces monitoring policy is enabled. The *Cisco UCS Manager System Monitoring Guide* provides more details about the Management Interfaces Monitoring Policy.

Procedure

Step 1 Enter monitoring mode.

UCS-A# **scope monitoring**

Step 2 Enable or disable the management interfaces monitoring policy.

UCS-A /monitoring # **set mgmt-if-mon-policy admin-state** {**enabled** | **disabled**}

Step 3 UCS-A /monitoring # **commit-buffer**

Commits the transaction to the system configuration.

Step 4 Open a Telnet session to the upstream switch connected to the fabric interconnect.

Step 5 Verify the configuration of the interface to which the fabric interconnect management port is connected, and disable it using the shut command on the switch.

Any KVM session that is open through this interface terminates.

Step 6 Reconnect KVM sessions to ensure that these sessions are not impacted by upgrade of the secondary fabric interconnect.

Example

The following example disables the monitoring interface management policy and commits the transaction:

```
UCS-A# scope monitoring
UCS-A /monitoring # set mgmt-if-mon-policy admin-state enabled
UCS-A /monitoring* # commit-buffer
UCS-A /monitoring #
```

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*.

Example

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.

Example

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.

Example

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
```

UCS Manager Health and Pre-Upgrade Check Tool

The UCS Manager Health and Pre-Upgrade Check Tool provides automated health and pre-upgrade checks that are designed to ensure your clusters are healthy before you upgrade. It is imperative that this healthcheck is not just performed, but that you take corrective action on any cluster that is found to be unhealthy. Correct all issues reported by the UCS Manager health check before continuing.

Verification that the Data Path is Ready

Note We recommend that you follow the guidelines prior to any processes that require reboot of both Fabric Interconnects.

Ensure that you monitor the VIF paths and counts only from the CLI and not within the Cisco UCS Manager GUI.

The following sections detail the steps to verify that the data path is ready.

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. Ensure that the vNICs are up and running 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 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	Use the following command: **Option** / **Description** **show platform fwm info hw-stm | grep '1.' | wc –l** — Returns the total number of MAC addresses on UCS 6332, and UCS 6332-16UP Fabric Interconnects. **show hardware internal libsdk mtc l2 mac-table-ce valid-only | egrep "^ *[0-9]" | wc -l** — Returns the total number of MAC addresses on UCS 6324 (UCS Mini) Fabric Interconnects. **show hardware mac address-table 1 | wc -l** — Returns the total number of MAC addresses on Cisco UCS 6600 Series Fabric Interconnect, Cisco UCS X-Series Direct, Cisco UCS 6500 Series, and Cisco UCS 6400 Series Fabric Interconnects.	Verify that this number matches the number of MAC addresses prior to the upgrade.

Example

The following example returns the number of active Ethernet interfaces and MAC addresses for subordinate UCS 6332 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
```

The following example returns the number of active Ethernet interfaces and MAC addresses for subordinate UCS 6400 Series 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 hardware mac address-table 1 | wc -l
80
```

Verifying the Data Path for Fibre Channel End-Host 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 npv flogi-table**	Displays a table of flogi sessions.
Step 3	UCS-A(nxos)# **show npv flogi-table | grep fc | wc -l**	Returns the number of servers logged into the fabric interconnect. The output should match the output you received when you performed this verification prior to beginning the upgrade.

Example

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

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

Total number of flogi = 3.

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

Verifying the Data Path for Fibre Channel Switch Mode

For best results when upgrading a Cisco UCS 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.

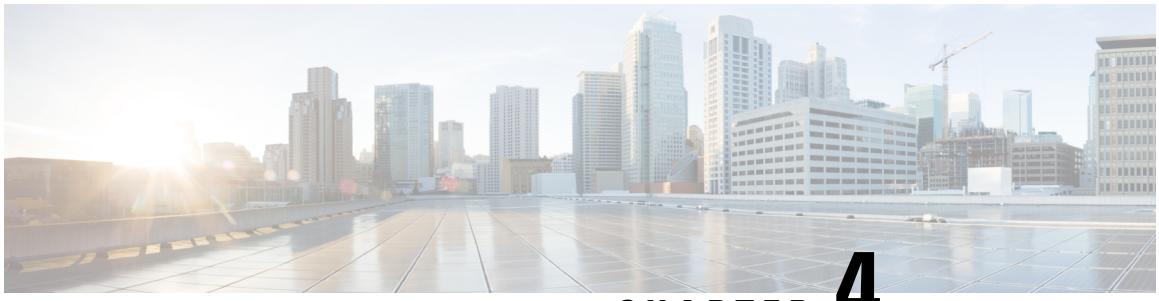
Example

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
```



CHAPTER 4

Manage Firmware through Cisco UCS Manager

- Download and Manage Firmware in Cisco UCS Manager, on page 61
- Firmware Upgrades through Auto Install, on page 71
- Firmware Upgrades through Firmware Packages in Service Profiles , on page 86
- Firmware Automatic Synchronization, on page 95
- Direct Firmware Upgrade at Endpoints, on page 97

Download and Manage Firmware in Cisco UCS Manager

Firmware Image Management

Cisco delivers all firmware updates to Cisco UCS components in bundles of images. Each image represents an individual firmware package specific to one hardware component. For example: IOM image, Cisco UCS Manager image, and so on.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

Cisco UCS Manager includes infrastructure bundles that contain firmware images required to update components such as:

- Cisco UCS Manager software
- Kernel and system firmware for the fabric interconnects
- I/O module/FI-IO module firmware

Note Cisco UCS X-Series Direct, Cisco UCS 6500 Series Fabric Interconnects, Cisco UCS 6400 Series Fabric Interconnects do not have separate kickstart and system images.

Note The UCS infrastructure bundle for one platform cannot be used to activate another platform.

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.

Caution Ensure that before starting the auto-install process, you capture the data according to Verification that the Data Path is Ready, on page 55.

- Before acknowledging the pending activity during auto-install, it is important to confirm that all the subordinate VIF paths are rebuilt.
- Ensure that you monitor the UCS VIF paths only from the CLI and not from the faults within the UCS Manager GUI.
- If you fail to monitor the UCS VIF paths, it may result in partial or complete "All Paths Down" state.

We recommend that you follow the guidelines prior to any processes that require reboot of both Fabric Interconnects.

Note For more information, see Cisco UCS Manager Release Bundle Contents.

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 maintains an inventory of all available images. The image catalog contains a list of images and packages. A package is a read-only object that is created when it is downloaded. It does not occupy disk space and represents a list or collection of images that were unpacked as part of the package download. When an individual image is downloaded, the package name remains the same as the image name.

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. After all the images in the package have been deleted, Cisco UCS Manager deletes the package itself.

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. Faults are raised when the bootflash partition exceeds 70 percent and total used space exceeds 90 percent. If Cisco UCS Manager generates such a fault, delete obsolete images to free up space.

Obtaining Software Bundles from Cisco

Before you begin

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

- Cisco UCS Infrastructure Software Bundle for Cisco UCS Fabric Interconnects 9108 100G, Cisco UCS 6500 Series Fabric Interconnect, Cisco UCS 6400 Series Fabric Interconnect, 6300 Series Fabric Interconnects—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 for Cisco UCS Fabric Interconnects 9108 100G, Cisco UCS 6500 Series Fabric Interconnect, Cisco UCS 6400 Series Fabric Interconnect, 6300 Series Fabric Interconnects, and 6324 Fabric Interconnects	Click **UCS Infrastructure and UCS Manager Software** > **Unified Computing System (UCS) Infrastructure Software Bundle**.
Cisco UCS B-Series Blade Server Software Bundle	Click **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 **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 release 4.0 software bundle.

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

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

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

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

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

What to do next

Download the software bundles to the fabric interconnect.

Downloading Firmware Images to the Fabric Interconnect from a Remote Location

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

	Command or Action	Purpose
		• **usbA:**/ *path* • **usbB:**/ *path* **Note** USB A and USB B are applicable only for Cisco UCS 6324 (UCS Mini) and Cisco UCS 6300 Series fabric interconnects. For Cisco UCS 6300 Series fabric interconnects, only the first of the two ports is detected. **Note** 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.	

Example

The following example uses SCP to download the firmware package.

```
UCS-A# scope firmware
UCS-A /firmware # download image scp://user1@111.100.10.10/images/ucs-k9-bundle.4.0.1.988.bin
OR
download image usbB:/username/ucs-k9-bundle-b-series.4.0.1a.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.
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.

Example

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-6400-k9-bundle-infra.4.0.1a.A.bin  Scp        100.100.100.10    user1       Downloading

UCS-A /firmware # show download-task

Download task:
File Name                             Protocol   Server            Userid      State
---------                             --------   ---------------   ---------   -----
ucs-6400-k9-bundle-infra.4.0.1a.A.bin  Scp        100.100.100.10    user1       Downloading

UCS-A /firmware # show download-task

Download task:
File Name                             Protocol   Server            Userid      State
---------                             --------   ---------------   ---------   -----
ucs-6400-k9-bundle-infra.4.0.1a.A.bin  Scp        100.100.100.10    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.

Example

The following example cancels an image download:

```
UCS-A# scope firmware
UCS-A /firmware # delete download-task ucs-k9-bundle-b-series.4.0.1a.B.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.

Example

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

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

```
Name                                               Type                  Version
-------------------------------------------------- --------------------- -------
ucs-2200.3.2.2cS2.gbin                             Chassis Adaptor       3.2(2cS2)
ucs-2200.4.0.0.46.gbin                             Chassis Adaptor       4.0(0.46)
ucs-3260.3.0.4d.gbin                               Chassis Management Controller
                                                                         3.0(4d)
ucs-3260.4.0.0.149.gbin                            Chassis Management Controller
                                                                         4.0(0.149)
ucs-3260.4.0.0.155.gbin                            Chassis Management Controller
                                                                         4.0(0.155)
ucs-6100-k9-kickstart.5.0.3.N2.3.22cS2.gbin        Fabric Interconnect Kernel
                                                                         5.0(3)N2(3.22cS2)
ucs-6100-k9-kickstart.5.0.3.N2.4.00.46.gbin        Fabric Interconnect Kernel
                                                                         5.0(3)N2(4.00.46)
ucs-6100-k9-system.5.0.3.N2.3.22cS2.gbin           Fabric Interconnect System
                                                                         5.0(3)N2(3.22cS2)
ucs-6100-k9-system.5.0.3.N2.4.00.46.gbin           Fabric Interconnect System
                                                                         5.0(3)N2(4.00.46)
ucs-adaptor-pcie-ucsc-pcie-x710ta4.800031CA-1.812.1.gbin
                                                   Adapter               800031CA-1.812.1
ucs-adaptor-pcie-ucsc-pcie-xxx710da2.8000364C-1.812.1.gbin
                                                   Adapter               8000364C-1.812.1
ucs-bmc-brdprog-S3260M5.2.0.gbin                   Board Controller      2.0


...
```

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. **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.

Example

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

```
UCS-A# scope firmware
UCS-A /firmware # show package
Name                                       Version
------------------------------------------ -------
ucs-c125-bios.C125.4.0.0.15.0504180159.gbin
ucs-c125-bios.C125.4.0.0.17.0518180446.gbin
ucs-c125-k9-cimc.4.0.0.130.gbin
ucs-c125-k9-cimc.4.0.0.149.gbin
ucs-k9-bundle-c-series.3.1.3h.C.gbin       3.1(3h)C
ucs-k9-bundle-c-series.4.0.0.112.C.gbin    4.0(0.112)C
ucs-k9-bundle-c-series.4.0.0.115.C.gbin    4.0(0.115)C
ucs-k9-bundle-infra.3.2.2eS9.A.gbin        3.2(2eS9)A
ucs-k9-bundle-infra.4.0.0.57.A.gbin        4.0(0.57)A
ucs-manager-k9.4.0.0.8769.gbin
ucs-manager-k9.4.0.0.8777.gbin
ucs-manager-k9.4.0.0.8911.gbin
```

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.

Example

The following example displays the contents of a firmware package:

```
UCS-A# scope firmware
UCS-A /firmware # show package ucs-k9-bundle-infra.4.0.0.57.A.gbin expand
Package ucs-k9-bundle-infra.4.0.0.57.A.gbin:
    Images:
        ucs-2200.4.0.0.46.gbin
        ucs-6100-k9-kickstart.5.0.3.N2.4.00.46.gbin
        ucs-6100-k9-system.5.0.3.N2.4.00.46.gbin
        ucs-manager-k9.4.0.0.56b.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.

Example

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        16342            81
    opt              3873             3
    spare            5759             2
    usbdrive         Nothing          Empty
    var_sysmgr       2000             24
    var_tmp          600              2
    volatile         240              Empty
    workspace        3848             6
UCS-A /fabric-interconnect #
```

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 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. Firmware Image Management, on page 61, provides details about the available infrastructure software bundles in Cisco UCS Manager Release 4.0. Recommended Process for Upgrading Infrastructure Firmware Through Auto Install, on page 78, details the process that Cisco recommends for automatically installing infrastructure firmware.
- Install Chassis Firmware—Uses the Cisco UCS C-Series Rack-Mount UCS-Managed Server Software Bundle to upgrade the chassis components.

- Install Server Firmware—Uses the Cisco UCS B-Series Blade Server Software Bundle to upgrade all blade servers in the Cisco UCS domain; the Cisco UCS C-Series Rack-Mount UCS-Managed Server Software Bundle to upgrade all rack servers.

These 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 upgrade the chassis 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, and Guidelines for Upgrading with Auto Install, on page 37.

In Cisco UCS Manager Releases 3.1(1l), 3.1(2b), 3.1(2c), and 3.1(2e), activating the Cisco UCS Manager software through Auto Install fails if the power policy is configured with **Redundancy** set to **Grid** and **Power Capping** set to **No Cap**. In Cisco UCS Manager releases earlier than Cisco UCS Manager Release 3.1(2b) and later than 3.1(2e), activating the Cisco UCS Manager software through Auto Install no longer fails based on the configured power policy.

If you upgrade or downgrade a fabric interconnect in the following modes, the Cisco UCS Manager requests you to acknowledge for an fabric interconnect reboot:

- Cluster mode with two fabric interconnects
- Standalone mode with a single fabric interconnect

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 and the Service Pack, on page 84, provides detailed steps for clearing the startup version.

Automatic Internal Backup

Note Beginning with release 4.2(3d), Cisco UCS Manager introduces **Password Encryption Key** to enhance security for backup configuration files.

If you do not set **Password Encryption Key**, then **Automatic Internal Backup** also fails. For more information on how to set **Password Encryption Key**, see *Setting Password Encryption Key for Locally Authenticated Users* section in Cisco UCS Manager Administration Management Guide for your release.

While the Infrastructure firmware is being upgraded, an automatic full state backup file is created. Cisco UCS Manager includes backup stages that are visible in the FSM status. Cisco UCS Manager Release 2.2(4) introduced 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/
```

Prepare for Firmware Install

You can use Auto Install to upgrade a Cisco UCS domain to the firmware versions contained in a single package. Auto Install provides the ability to install firmware in three independent phases—Install Infrastructure Firmware, Install Chassis Firmware, and Install Server Firmware. During Auto Install, the firmware for some endpoints such as the IOMs, adapters, BIOS and CIMC are first updated and then activated.

Updating the firmware on an endpoint involves staging the firmware image to the backup partition on an endpoint. The update phase does not require or cause reboot of the endpoint. During activation, you set the firmware in the backup partition as the active firmware version on the endpoint. Activation can require or cause the reboot of an endpoint. Therefore, the time taken to complete the Auto Install process includes the time required to do the following:

- Update or stage firmware to the backup partition of all endpoints

Note This process takes most of the time spent to complete Auto Install.

- Activate firmware on all the endpoints
- Reboot all applicable endpoints

Cisco UCS Manager Release 3.2(3) introduces the ability to update or stage the firmware of infrastructure, server components, and S3260 chassis simultaneously, and keep it independent of the activation process. Because staging firmware does not involve rebooting any endpoints, this ability allows you to stage the firmware on all endpoints without waiting for a maintenance window. Consequently, the time taken to complete the Auto Install process no longer includes the time taken to stage firmware to the backup partition of all endpoints. You can, thus, significantly reduce the downtime required for maintenance.

If you stage the firmware using this feature before performing Auto Install, you can skip backup updates and proceed with firmware activation and endpoint reboots. If you do not stage the firmware on the endpoints through this feature, you can continue to use Auto Install to update and activate the components. The ability to stage firmware to the backup partition of endpoints does not change the legacy ability of Auto Install to update and activate the firmware of components.

Preparing the Infrastructure Firmware Pack for Install

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 # **scope fw-backup-version infra**	Enters the backup firmware mode for infrastructure.
Step 4	UCS-A /org/fw-infra-pack/fw-backup-version # **set bundle-vers** *firmware_version*	Sets the specified firmware version as the backup infrastructure firmware version.
Step 5	UCS-A /org/fw-infra-pack/fw-backup-version* # **commit-buffer**	Commits the transaction.

Example

This example shows how to set the backup infrastructure firmware version.

```
UCS-A# scope org
UCS-A /org # scope fw-infra-pack default
UCS-A /org/fw-infra-pack # scope fw-backup-version infra
UCS-A /org/fw-infra-pack/fw-backup-version # set bundle-vers 4.0(1a)A
UCS-A /org/fw-infra-pack/fw-backup-version* # commit-buffer
```

Preparing the Chassis Firmware Pack for Install

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*.

	Command or Action	Purpose
Step 2	UCS-A /org # **scope fw-chassis-pack** *name*	Enters the organization chassis firmware policy mode.
Step 3	UCS-A /org/fw-chassis-pack # **scope fw-backup-version chassis**	Enters the backup firmware mode for chassis.
Step 4	UCS-A /org/fw-chassis-pack/fw-backup-version # **set bundle-vers** *firmware_version*	Sets the specified firmware version as the backup chassis firmware version.
Step 5	UCS-A /org/fw-chassis-pack/fw-backup-version* # **commit-buffer**	Commits the transaction.

Example

This example shows how to set the backup chassis firmware version.

```
UCS-A# scope org
UCS-A /org # scope fw-chassis-pack default
UCS-A /org/fw-chassis-pack # scope fw-backup-version chassis
UCS-A /org/fw-chassis-pack/fw-backup-version # set bundle-vers 4.0(1a)C
UCS-A /org/fw-chassis-pack/fw-backup-version* # commit-buffer
```

Preparing the Blade Host Firmware Pack for Install

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-host-pack** *name*	Enters the organization host firmware policy mode.
Step 3	UCS-A /org/fw-host-pack # **scope fw-backup-version blade**	Enters the backup firmware mode for blade servers.
Step 4	UCS-A /org/fw-host-pack/fw-backup-version # **set bundle-vers** *firmware_version*	Sets the specified firmware version as the backup host firmware version for blade servers.
Step 5	UCS-A /org/fw-host-pack/fw-backup-version* # **commit-buffer**	Commits the transaction.

Example

This example shows how to set the backup host firmware version for blade servers.

```
UCS-A# scope org
UCS-A /org # scope fw-host-pack default
UCS-A /org/fw-host-pack # scope fw-backup-version blade
UCS-A /org/fw-host-pack/fw-backup-version # set bundle-vers 4.0(1a)B
UCS-A /org/fw-host-pack/fw-backup-version* # commit-buffer
```

Preparing the Rack Host Firmware Pack for Install

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-host-pack** *name*	Enters the organization host firmware policy mode.
Step 3	UCS-A /org/fw-host-pack # **scope fw-backup-version rack**	Enters the backup firmware mode for rack-mount servers.
Step 4	UCS-A /org/fw-host-pack/fw-backup-version # **set bundle-vers** *firmware_version*	Sets the specified firmware version as the backup host firmware version for rack-mount servers.
Step 5	UCS-A /org/fw-host-pack/fw-backup-version* # **commit-buffer**	Commits the transaction.

Example

This example shows how to set the backup host firmware version for rack-mount servers.

```
UCS-A# scope org
UCS-A /org # scope fw-host-pack default
UCS-A /org/fw-host-pack # scope fw-backup-version rack
UCS-A /org/fw-host-pack/fw-backup-version # set bundle-vers 4.0(1a)C
UCS-A /org/fw-host-pack/fw-backup-version* # commit-buffer
```

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.

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.

Recommended Process for Upgrading Infrastructure Firmware Through Auto Install

Cisco recommends the following process for upgrading infrastructure firmware through Auto Install:

1. Stage the software and prepare for upgrade:
   a. Create All Configuration and Full-State backup files. Creating an All Configuration Backup File, on page 42 and Configuring the Full State Backup Policy, on page 42 provide detailed information.
   b. Download firmware packages. Downloading Firmware Images to the Fabric Interconnect from a Remote Location, on page 65 provides detailed information.
   c. Stage the Infrastructure firmware if using Cisco UCS Manager Release 3.2(3) or later releases. Preparing the Infrastructure Firmware Pack for Install, on page 74, provides detailed information about staging the infrastructure firmware.

Note Although this step is optional, it is also recommended.

   d. Disable Smart Call Home. Disabling Smart Call Home, on page 45 provides detailed information about disabling Smart Call Home.

2. Prepare for fabric upgrade:
   a. Verify Cisco UCS Manager faults and resolve the service -impacting faults.
   b. Verify High Availability status and identify the secondary fabric interconnect. Verifying the High Availability Status and Roles of a Cluster Configuration, on page 49 provides detailed information.
   c. Configure the default maintenance policy. Configuring the Default Maintenance Policy, on page 50 provides detailed information about maintenance policies and configuring the default maintenance policy to **User Ack**.
   d. Verify that VLAN and FCOE IDs do not overlap.
   e. Disable the management interface. Disabling the Management Interface, on page 52 provides detailed information about disabling the management interface for the secondary fabric interconnect.
   f. Verify that all paths are working. Verification that the Data Path is Ready, on page 55 provides detailed information.

3. Upgrade the Infrastructure Firmware with Auto Install, on page 79
4. Verify High Availability status in cluster.
5. Verify that all paths are working.
6. Verify new faults. Viewing Faults Generated During the Upgrade of a Fabric Interconnect, on page 47 provides detailed information.
7. Acknowledge activation of the primary fabric. Acknowledging the Reboot of the Primary Fabric Interconnect, on page 82 provides detailed information.
8. Verify new faults.

Upgrade the Infrastructure Firmware with Auto Install

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 Manager 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, and Guidelines for Upgrading with Auto Install, on page 37 and the appropriate Cisco UCS upgrade guide.

Beginning with Cisco UCS Manager Release 3.1(3), you can use Auto Install to install a service pack on Cisco UCS Manager and both fabric interconnects. You can apply a service pack on a base infrastructure pack, but you cannot install the service pack independently.

You can install a compatible service pack through Auto Install without upgrading the infrastructure pack. This will trigger service pack installation on both fabric interconnects. Certain service pack installations may require the fabric interconnects to be reloaded.

Auto Install of infrastructure firmware using a service pack is supported only when all the infrastructure components are at Cisco UCS Manager Release 3.1(3) or later releases.

Before you begin

- Complete all prerequisites listed in Prerequisites for Upgrading and Downgrading Firmware, on page 40
- Stage the Infrastructure firmware if using Cisco UCS Manager Release 3.2(3) or later releases. Preparing the Infrastructure Firmware Pack for Install, on page 74, provides detailed information about staging the infrastructure firmware.

Note Although this step is optional, it is also recommended.

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* **servicepack-vers** *servicepack-bundle-version*	Updates and activates the infrastructure firmware and the service pack bundle.

	Command or Action	Purpose
	[**starttime** *mon dd yyyy hh min sec*] [**force**] [**evacuate**] [**skipvalidation**]	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. Use the **evacuate** keyword to enable fabric evacuation on each fabric interconnect that is being upgraded through Auto Install. Both fabric interconnects are evacuated, but not at the same time. **Note** If you enable fabric evacuation during Auto Install, and fabric evacuation was enabled manually on any of the fabric interconnects before Auto Install, fabric evacuation is disabled after Auto Install is complete.

	Command or Action	Purpose
Step 4	(Optional) UCS-A /firmware/auto-install # **install infra servicepack-vers** *servicepack-bundle-version* [**force**]	Updates and activates the service pack bundle over the existing base infrastructure pack.

Example

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 4.0(1a)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
(6) Check if any hardware (fabric interconnects, io-modules, servers or adapters) is
unsupported in the target release
Do you want to proceed? (yes/no): yes

Triggering Install-Infra with:
   Infrastructure Pack Version: 4.0(1a)A
UCS-A /firmware/auto-install #
```

This example shows how to upgrade the infrastructure to the firmware in the Cisco UCS Infrastructure Software Bundle with the **evacuate** option enabled:

```
UCS-A# scope firmware
UCS-A /firmware # scope auto-install
UCS-A /firmware/auto-install # install infra infra-vers 4.0(1a)A evacuate
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
(6) Check if any hardware (fabric interconnects, io-modules, servers or adapters) is
unsupported in the target release
Do you want to proceed? (yes/no): yes

Evacuate option: true
Warning: Please note that if fabric evacuation was configured ON manually on any of the
FIs, it will be turned OFF in the process of Auto Install.

Triggering Install-Infra with:
   Infrastructure Pack Version: 4.0(1a)A
UCS-A /firmware/auto-install #
```

This example shows how to upgrade the infrastructure to a service pack version:

```
UCS-A# scope firmware
UCS-A /firmware # scope auto-install
UCS-A /firmware/auto-install # install infra infra-vers 4.0(1a)A servicepack-vers 4.0(1)SP1
 force
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
(6) Check if any hardware (fabric interconnects, io-modules, servers or adapters) is
unsupported in the target release
Do you want to proceed? (yes/no):
```

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.

Certain service pack installations may require the fabric interconnects to be reloaded. In such scenarios, you must acknowledge the reboot of the primary fabric interconnect to complete the service pack installation.

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 Verification that the Data Path is Ready, on page 55.

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.

	Command or Action	Purpose
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.

Example

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.

Example

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 and the Service Pack

You must clear the startup version of the default infrastructure pack and service 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 ""**	Clears the startup version of the default infrastructure pack and the service pack.
Step 4	(Optional) UCS-A /org/fw-infra-pack # **set servicepack-vers ""**	Clears the startup version of the service pack.
Step 5	UCS-A /org/fw-infra-pack* # **commit-buffer**	Commits the transaction.

Example

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

Example

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: Success
        Completion Time: 2017-02-03T18:02:13.699
        Progress (%): 100

        FSM Stage:

        Order  Stage Name                                Status       Try
        ------ ------------------------------------------ ------------ ---
        1      DeployWaitForDeploy                        Success      0
        2      DeployResolveDistributableNames            Skip         0
        3      DeployResolveDistributable                 Skip         0
        4      DeployResolveImages                        Skip         0
        5      DeployDownloadImages                       Skip         0
        6      DeployCopyAllImagesToPeer                  Skip         0
        7      DeployInternalBackup                       Skip         0
        8      DeployPollInternalBackup                   Success      0
        9      DeployActivateUCSM                         Skip         0
        10     DeployPollActivateOfUCSM                   Success      0
        11     DeployUpdateIOM                            Success      0
        12     DeployPollUpdateOfIOM                      Success      0
        13     DeployActivateIOM                          Success      0
        14     DeployPollActivateOfIOM                    Success      0
        15     DeployFabEvacOnRemoteFI                    Skip         0
        16     DeployPollFabEvacOnRemoteFI                Skip         0
        17     DeployActivateRemoteFI                     Success      0
        18     DeployPollActivateOfRemoteFI               Success      0
        19     DeployFabEvacOffRemoteFI                   Skip         0
        20     DeployPollFabEvacOffRemoteFI               Skip         0
        21     DeployWaitForUserAck                       Skip         0
        22     DeployPollWaitForUserAck                   Success      0
        23     DeployFailOverToRemoteFI                   Skip         0
        24     DeployPollFailOverToRemoteFI               Skip         0
        25     DeployActivateLocalFI                      Success      0
        26     DeployPollActivateOfLocalFI                Success      0
        27     DeployActivateUCSMServicePack              Skip         0
```

```
28      DeployPollActivateOfUCSMServicePack      Success      0
```

Firmware Upgrades through Firmware Packages in Service Profiles

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

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

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**
- **BIOS**
- **CIMC**

Note For rack mount servers, if you exclude CIMC from the host firmware pack, and upgrade or downgrade the board controller, the upgrade or downgrade may fail. This is because the CIMC firmware version and board controller firmware version may be incompatible.

- **Board Controller**
- **Flex Flash Controller**
- **GPUs**
- **FC Adapters**
- **HBA Option ROM**
- **Host NIC**
- **Host NIC Option ROM**
- **Local Disk**

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

In Cisco UCS Manager Release 3.1(1), 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. Starting with Cisco UCS Manager Release 3.1(2), the firmware for local disk and other common endpoints is available in both the blade and rack packages.

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

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 BIOS firmware through the host firmware package, you can exclude BIOS firmware from the list of firmware package components.

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.

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 that 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. This 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.

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. Disassociate 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 to 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 user acknowledgment with **On Next Boot** option	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. To reboot and to apply the new firmware, do one of the following: • Click the flashing **Pending Activities** button to select the servers you want to reboot and apply the new firmware. • Manually reboot the servers. 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 causes Cisco UCS to apply the firmware package. This is enabled by the **On Next Boot** option.

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 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 to 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	(Optional) UCS-A /org/fw-host-pack # **set descr** *description*	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** | **host-hba-optionrom** | **host-nic** | **local-disk** | **raid-controller** | **server-bios**} "*version-num*"	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 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** | **unspecified**}	Excludes the specified component from the host firmware package. **Note** By default, all components are included in the host firmware package.

	Command or Action	Purpose
Step 6	Required: UCS-A org/fw-host-pack # **delete 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** | **unspecified**}	Includes the specified component from the host firmware package.
Step 7	(Optional) UCS-A org/fw-host-pack/pack-image # **set blade-vers** *blade-version-num*	Specifies the B-Series server package image version number. Changing this number triggers firmware updates on all B-Series server components using the firmware through a service profile. Use this step only when updating a host firmware package, not when creating a package. The host firmware package can contain multiple package images. Repeat steps 4 and 5 to create additional package images for other components.
Step 8	(Optional) UCS-A org/fw-host-pack/pack-image # **set rack-vers** *rack-version-num*	Specifies the C-Series server package image version number. Changing this number triggers firmware updates on all C-Series server components using the firmware through a service profile. Use this step only when updating a host firmware package, not when creating a package. The host firmware package can contain multiple package images. Repeat steps 4 and 5 to create additional package images for other components.
Step 9	(Optional) UCS-A org/fw-host-pack/pack-image # **set servicepack-vers** *servicepack-version-num*	Specifies the service pack version number. You cannot directly upgrade to a service pack without selecting a base server pack. To remove the service pack from the host firmware package, use **""** as the service pack version number. The images from the service pack will take precedence over the images from Blade Package or Rack Package.
Step 10	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

	Command or Action	Purpose
		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.

Example

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 #
```

The following example adds a service pack to the app1 host firmware package, and commits the transaction:

```
UCS-A# scope org
UCS-A /org # scope fw-host-pack app1
UCS-A /org/fw-host-pack # set servicepack-vers 4.0(1)SP1
UCS-A /org/fw-host-pack* # commit-buffer
UCS-A /org/fw-host-pack #
```

The following example removes a service pack from the app1 host firmware package, and commits the transaction:

```
UCS-A# scope org
UCS-A /org # scope fw-host-pack app1
UCS-A /org/fw-host-pack # set servicepack-vers ""
UCS-A /org/fw-host-pack* # commit-buffer
UCS-A /org/fw-host-pack #
```

What to do next

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

Firmware Automatic Synchronization

You can use the **Firmware Auto Sync Server policy** in Cisco UCS Manager to determine whether firmware versions on recently discovered servers must be upgraded or not. 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**.

Note You cannot use the **Firmware Auto Sync Server policy** in the server that is part of a server pool.

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

- **No Action**—No firmware upgrade is initiated on the server.

  This value is selected by default.

- **User Acknowledge**—Firmware on the server is not synchronized until the administrator acknowledges the upgrade in the **Pending Activities** dialog box.

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 **User Ack** and you change it to **No Action**.

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 auto-sync**{*user-acknowledge* | *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. This value is selected by default.
Step 4	UCS-A /org/fw-autosync-policy # **commit-buffer**	Commits the transaction to the system configuration.

Example

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

```
UCS-A # scope org
UCS-A /org # scope fw-autosync-policy
UCS-A /org/fw-autosync-policy # set auto-sync user-acknowledge
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

	Command or Action	Purpose
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.

Example

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 #
```

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. Recommended Process for Directly Upgrading Infrastructure Firmware at Endpoints, on page 101, details the process that Cisco recommends for upgrading infrastructure firmware on endpoints.

You can directly upgrade the firmware on the following components:

Infrastructure	Cisco UCS X9508 Chassis	UCS 5108 Chassis	UCS Rack Server	Cisco UCS S3260 Chassis

• Cisco UCS Manager
• Fabric Interconnects
 	
Ensure that you upgrade Cisco UCS Manager first and then the fabric interconnects.
	• I/O modules, FI-IO Module, and Intelligent Fabric Module (IFM)
	• X-Fabric module (XFM)
	• Power supply unit
	• Server
	  • Adapter
	  • CIMC
	  • BIOS
	  • Storage controller
	  • Board controller
		• I/O modules
		• Power supply unit
		• Server:
		  • Adapter
		  • CIMC
		  • BIOS
		  • Storage controller
		  • Board controller
			• Adapter
			• CIMC
			• BIOS
			• Storage controller
			• Board controller
				• CMC
				• Chassis adapter
				• SAS expander
				• Chassis board controller
				• Server:
				  • CIMC
				  • BIOS
				  • Board controller
				  • Storage controller

For the Cisco UCS S3260 chassis, you can upgrade the CMC, chassis adapter, chassis board controller, SAS expander, and local disk firmware through the chassis firmware package in the chassis profile. *Cisco UCS S3260 Server Integration with Cisco UCS Manager, Release 4.0* provides detailed information about chassis profiles and chassis firmware packages.

You can upgrade the adapter, board controller, CIMC, and BIOS firmware 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.

Important All server components must be kept at the same release level. These components are tested together for each release and a version mismatch may cause unpredictable system operation.

Stages of a Direct Firmware Upgrade

Cisco UCS Manager separates the direct upgrade process into two stages, ensuring 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 in a UCS 5108 chassis:

- Adapters
- CIMCs
- I/O modules

On a Cisco UCS S3260 dense storage rack server chassis, the update stage applies only to the following endpoints:

- Chassis Management Controller (CMC)
- Shared adapter
- SAS expander
- Server:
  - BIOS
  - CIMC
  - 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.

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
- On a Cisco UCS S3260 dense storage rack server chassis:
  - CMC
  - Shared adapter

- Board controllers for chassis and server
- SAS expander
- Storage controller
- BIOS
- CIMC

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 non-cluster 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 10 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.

Recommended Process for Directly Upgrading Infrastructure Firmware at Endpoints

Cisco recommends the following process for directly upgrading infrastructure firmware at endpoints:

1. Stage the software and prepare for upgrade:
   a. Create All Configuration and Full-State backup files. Creating an All Configuration Backup File, on page 42 and Configuring the Full State Backup Policy, on page 42 provide detailed information.
   b. Download firmware packages. Downloading Firmware Images to the Fabric Interconnect from a Remote Location, on page 65 provides detailed information.
   c. Disable Smart Call Home. Disabling Smart Call Home, on page 45 provides detailed information.
2. Activating the Cisco UCS Manager Software, on page 103
3. Update IOM firmware. Updating and Activating the Firmware on an IOM, on page 106 provides detailed information.
4. Prepare for fabric upgrade:
   a. Verify UCS Manager faults and resolve the service -impacting faults.
   b. Verify High Availability status and identify the secondary fabric interconnect. Verifying the High Availability Status and Roles of a Cluster Configuration, on page 49 provides detailed information.

c. Configure the default maintenance policy. Configuring the Default Maintenance Policy, on page 50 provides detailed information.

d. Verify that VLAN and FCOE IDs do not overlap.

e. Disable the management interface. Disabling the Management Interface, on page 52 provides detailed information.

f. Activate IOM firmware. Updating and Activating the Firmware on an IOM, on page 106 provides detailed information.

5. Activate the subordinate fabric interconnect

a. Evacuate subordinate fabric interconnect traffic. Stopping Traffic on a Fabric Interconnect, on page 32 provides detailed information.

b. Activate the subordinate fabric interconnect (FI-B) and monitor FSM. Activating the Firmware on a Fabric Interconnect, on page 109 provides detailed information.

c. Verify that all paths are working. Verification that the Data Path is Ready, on page 55 provides detailed information.

d. Disable subordinate fabric interconnect traffic evacuation. Restarting Traffic on a Fabric Interconnect, on page 32 provides detailed information.

e. Verify new faults. Viewing Faults Generated During the Upgrade of a Fabric Interconnect, on page 47 provides detailed information.

6. Activate the primary fabric interconnect (FI-A)

a. Migrate management services from the primary fabric interconnect to the secondary fabric interconnect, and change the cluster lead to the secondary fabric interconnect. Switching Over Fabric Interconnect Cluster Lead, on page 110 provides detailed information.

b. Evacuate primary fabric interconnect traffic.

c. Activate the primary fabric interconnect (FI-A) and monitor FSM. Acknowledging the Reboot of the Primary Fabric Interconnect, on page 82 provides detailed information.

d. Verify that all paths are working.

e. Disable primary fabric interconnect traffic evacuation. Restarting Traffic on a Fabric Interconnect, on page 32 provides detailed information.

f. Verify new faults.

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 and then use the **Force** option to continue with the upgrade.

For example, because M1 and M2 blade servers are not supported on Release 3.1(1), if you have M1 or M2 blade servers in the configuration when upgrading from Release 2.2(x) to Release 3.1(1), these will be reported as validation faults in the **Upgrade Validation** tab, and the upgrade will fail.

If you do not want Cisco UCS Manager to validate the upgrade or downgrade process, check the **Skip Validation** check box.

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.
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.

Example

The following example upgrades Cisco UCS Manager and commits the transaction:

```
UCS-A# scope system
```

```
UCS-A# /system # show image
Name                                        Type                Version
------------------------------------------- ------------------- -------
ucs-manager-k9.4.0.1.0.bin                  System              4.0(1a)

UCS-A# /system # activate firmware 4.0(1a)
UCS-A# /system* # commit-buffer
UCS-A# /system #
```

Activating a Service Pack for the Cisco UCS Manager Software

You can use the steps detailed here to activate a service pack for the Cisco UCS Manager software. This process will not involve upgrading or rebooting the fabric interconnects.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope firmware**	
Step 2	UCS-A /firmware # **show image type** mgmt-service-pack	Displays the available software images for Cisco UCS Manager (system).
Step 3	UCS-A /firmware # **exit**	
Step 4	UCS-A# **scope system**	Enters system mode.
Step 5	UCS-A /system # **activate service-pack** *version-num* **module security**	Activates the selected service -pack version on the system. Cisco UCS Manager disconnects all active sessions, logs out all users, and activates the software. When the upgrade is complete, you are prompted to log back in. If you are prompted to re-login immediately after being disconnected, the login will fail. You must wait until the activation of Cisco UCS Manager is completed, which takes a few minutes.
Step 6	UCS-A /system # **commit-buffer**	Commits the transaction.
Step 7	(Optional) UCS-A /system # **show version**	Shows a summary of the firmware versions, including the service pack version, on the system.

Example

The following example upgrades Cisco UCS Manager to version 3.1(3)SP2 and commits the transaction:

```
UCS-A# scope firmware
UCS-A# /firmware # show image type mgmt-service-pack
Name                                        Type                Version
```

```
------------------------------------------- -------------------- -------
ucs-manager-k9.service-pack.3.1.3.SP1.gbin    Mgmt Service Pack    3.1(3)SP1
ucs-manager-k9.service-pack.3.1.3.SP2.gbin    Mgmt Service Pack    3.1(3)SP2
ucs-manager-k9.service-pack.3.1.4.SP1.gbin    Mgmt Service Pack    3.1(4)SP1
UCS-A# /firmware # exit
UCS-A# scope system
UCS-A# /system # activate service-pack 3.1(3)SP2 module security
As part of activation, all cli sessions will be terminated.
Continue with activation? (yes/no) yes
UCS-A# /system* # commit-buffer
UCS-A# /system # show version
UCSM:
    Running-Vers: 3.1(2.172a)
    Package-Vers: 3.1(2.173)A
    Activate-Status: Ready

UCSM Service Pack:
    Running-Vers: 3.1(3)SP2
    Running-Modules: security
    Package-Vers:
    Activate-Status: Ready


UCS-A# /system #
```

Removing a Service Pack from the Cisco UCS Manager Software

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope system**	Enters system mode.
Step 2	UCS-A /system # **remove service-pack**	Removes the activated service pack from the system. All CLI sessions are terminated while removing the service pack from the system.
Step 3	UCS-A /system # **commit-buffer**	Commits the transaction.

Example

The following example removes the service pack from Cisco UCS Manager and commits the transaction:

```
UCS-A# scope system
UCS-A# /system # remove service-pack
As part of activation, all cli sessions will be terminated.
Continue with activation? (yes/no)yes
UCS-A# /system* # commit-buffer
```

IOM and IFM (IOM for Cisco UCS X-Series Servers) Firmware

Beginning with release 4.3(2a), Cisco UCS Manager supports Cisco UCS X9508 server chassis with Cisco UCS X-Series servers. Cisco UCS X-Series servers support Intelligent Fabric Modules (IFM), which function

similarly to the Input/Output Module (IOM) in Cisco UCS B-Series servers. This guide uses the term IOM to refer both IOM and IFM.

Cisco UCS I/O modules (IOMs) bring the unified fabric into the blade server enclosure, thus providing multiple 10 Gigabit Ethernet connections between blade servers and the fabric interconnect, simplifying diagnostics, cabling, and management. IOMs extend the I/O fabric between the fabric interconnects and blade server chassis, and enable a lossless and deterministic Fibre Channel over Ethernet (FCoE) fabric to connect all blades and chassis together.

Because the IOM is similar to a distributed line card, it does not perform any switching, and is managed as an extension of the fabric interconnects. This approach removes switching from the chassis, reducing overall infrastructure complexity, and enables Cisco UCS to scale to many chassis without multiplying the number of switches needed. It allows all chassis to be managed as a single, highly available management domain.

The IOM also manages the chassis environment, which includes the power supply, fans, and blades, along with the fabric interconnect. Therefore, separate chassis management modules are not required. It fits into the back of the blade server chassis. Each blade chassis can support up to two IOMs, thus allowing increased capacity and redundancy.

Guidelines for Updating and Activating IOM Firmware

Consider the following guidelines and best practices while updating and activating firmware on IOMs:

- Each IOM stores two images—a running image and a backup image.
- The update operation replaces the backup image of an IOM with the new firmware version.
- The activate operation demotes the current startup image to a backup image. A new startup image is put in its place, and the system is configured to boot from this backup image.
- Check the **Set Startup Version Only** checkbox to set only the active image; a reset does not occur. This process can be used to upgrade multiple IOMs and then simultaneously reset them. If the fabric interconnect is updated and then activated, the fabric interconnect reboots the corresponding IOM and reduces the downtime.
- The IOM and fabric interconnect must be compatible with each other.
- If the software that runs on the fabric interconnect detects an IOM that runs an incompatible version, it performs an automatic update of the IOM to bring it to the same version as the fabric interconnect system software.

  Cisco UCS Manager raises a fault to indicate this situation. Additionally, the discovery state of IOM displays **Auto updating** while the automatic update is in progress.
- Cisco UCS Manager enables you to view the IOM firmware at the chassis level on the **Installed Firmware** tab.

Updating and Activating the Firmware on an IOM

If your system is running in a high availability cluster configuration, you must update and activate both I/O modules.

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

Procedure

	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 /chassis/iom # **show image**	Displays the available software images for the I/O module.
Step 4	UCS-A /chassis/iom # **update firmware** *version-num*	Updates the selected firmware version on the I/O module.
Step 5	(Optional) UCS-A /chassis/iom # **commit-buffer**	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	(Optional) UCS-A /chassis/iom # **show firmware**	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.

	Command or Action	Purpose
Step 7	UCS-A /chassis/iom # **activate firmware** *version-num* [**set-startup-only**]	Activates the selected firmware version on the I/O module. Use the **set-startup-only** keyword if you want to reboot the I/O module only when the fabric interconnect in its data path reboots. If you do not use the **set-startup-only** keyword, the I/O module reboots and disrupts traffic. In addition, if Cisco UCS Manager detects a protocol and firmware version mismatch between it and the I/O module, it updates the I/O module with the firmware version that matches its own and then activates the firmware and reboots the I/O module again.
Step 8	UCS-A /chassis/iom # **commit-buffer**	Commits the transaction.
Step 9	(Optional) UCS-A /chassis/iom # **show firmware**	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.

Example

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

```
UCS-A# scope chassis 1
UCS-A# /chassis # scope iom 1
UCS-A# /chassis/iom # show image
Name                                       Type                 Version
------------------------------------------ -------------------- -------
ucs-2200.4.0.0.332.bin                     IOM                  4.0(1a)

UCS-A# /chassis/iom # update firmware 4.0(1a)
UCS-A# /chassis/iom* # activate firmware 4.0(1a) set-startup-only
UCS-A# /chassis/iom* # commit-buffer
UCS-A# /chassis/iom #
```

The following example updates the I/O module firmware, verifies that the firmware update completed successfully before starting the firmware activation, activates the I/O module firmware, and verifies that the firmware activation completed successfully:

```
UCS-A# scope chassis 1
UCS-A# /chassis # scope iom 1
UCS-A# /chassis/iom # show image
Name                                       Type                 Version
```

```
-------------------------------------------- -------------------- -------
ucs-2200.4.0.0.332.bin                       IOM                  4.0(1)

UCS-A# /chassis/iom # update firmware 4.0(1)
UCS-A# /chassis/iom* # commit-buffer
UCS-A# /chassis/iom # show firmware
IOM      Fabric ID Running-Vers    Update-Status   Activate-Status
-------- --------- --------------- --------------- ---------------
       1 A         4.0(1)          Updating        Ready

UCS-A# /chassis/iom # show firmware
IOM      Fabric ID Running-Vers    Update-Status   Activate-Status
-------- --------- --------------- --------------- ---------------
       1 A         4.0(1)          Ready           Ready

UCS-A# /chassis/iom # activate firmware 4.0(1) ignorecompcheck
UCS-A# /chassis/iom* # commit-buffer
UCS-A# /chassis/iom # show firmware
IOM      Fabric ID Running-Vers    Update-Status   Activate-Status
-------- --------- --------------- --------------- ---------------
       1 A         4.0(1)          Ready           Activating

UCS-A# /chassis/iom # show firmware
IOM      Fabric ID Running-Vers    Update-Status   Activate-Status
-------- --------- --------------- --------------- ---------------
       1 A         4.0(1)          Ready           Ready
```

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 49.

For a non-cluster 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.

	Command or Action	Purpose
Step 2	UCS-A /fabric-interconnect # **show image**	Displays the available software images for the fabric interconnect.
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. **Note** The kernel-version and system-version must be the same.
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.

Example

The following example upgrades the fabric interconnect to version 5.0(3)N2(3.10.123) and commits the transaction:

```
UCS-A# scope fabric-interconnect a
UCS-A /fabric-interconnect # show image
Name                                       Type                 Version
------------------------------------------ -------------------- -------
ucs-6300-k9-kickstart.5.0.3.N2.3.10.123.bin   Fabric Interconnect Kernel
                                                                  5.0(3)N2(3.10.123)
ucs-6300-k9-system.5.0.3.N2.3.10.123.bin      Fabric Interconnect System
                                                                  5.0(3)N2(3.10.123)

UCS-A /fabric-interconnect # activate firmware kernel-version 5.0(3)N2(3.10.123)
system-version 5.0(3)N2(3.10.123)
UCS-A /fabric-interconnect* # commit-buffer
UCS-A /fabric-interconnect #
```

Switching Over Fabric Interconnect Cluster Lead

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

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	(Optional) 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: **force** Forces local fabric interconnect to become the primary. **lead** Makes the specified subordinate fabric interconnect the primary.

Example

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)#
```

Activating a Service Pack on a Fabric Interconnect

Procedure

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

	Command or Action	Purpose
Step 2	UCS-A /firmware # **show image type** fabric-interconnect-service-pack	Displays the available service packs for the fabric interconnects.
Step 3	UCS-A /firmware # **exit**	
Step 4	UCS-A# **scope fabric-interconnect** {**a** | **b**}	Enters fabric-interconnect mode.
Step 5	UCS-A /fabric-interconnect # **activate service-pack** *version-num* [**security**]	Activates the selected service -pack version on the system. **Note** Cisco UCS Manager activates the firmware. In some cases, Cisco UCS Manager reboots the fabric interconnect, disrupting data traffic to and from that fabric interconnect.
Step 6	UCS-A /fabric-interconnect # **commit-buffer**	Commits the transaction.
Step 7	(Optional) UCS-A /fabric-interconnect # **show version**	Shows a summary of the firmware versions, including the service pack version, on the fabric interconnect.

Example

The following example upgrades fabric interconnect a and commits the transaction:

```
UCS-A# scope firmware
UCS-A# /firmware # show image type fabric-interconnect-service-pack
Name                                       Type                  Version
------------------------------------------ --------------------- -------
ucs-6400-servicepack.4.0.1.SP1.gbin        Fabric Interconnect Service Pack
                                                                  4.0(1)SP1
ucs-6400-servicepack.4.0.1.SP2.gbin        Fabric Interconnect Service Pack
                                                                  4.0(1)SP2
ucs-6300-servicepack.4.0.1.SP1.gbin        Fabric Interconnect Service Pack
                                                                  4.0(1)SP1
ucs-6300-servicepack.4.0.1.SP2.gbin        Fabric Interconnect Service Pack
                                                                  4.0(1)SP2
ucs-mini-servicepack.4.0.1.SP1.gbin        Fabric Interconnect Service Pack
                                                                  4.0(1)SP1
ucs-mini-servicepack.4.0.1.SP2.gbin        Fabric Interconnect Service Pack
                                                                  4.0(1)SP2

UCS-A# /firmware # exit
UCS-A# scope fabric-interconnect a
UCS-A# /fabric-interconnect # activate service-pack 4.0(1)SP0 security
UCS-A# /fabric-interconnect* # commit-buffer
UCS-A# /fabric-interconnect # show version
 Fabric Interconnect A:
    Running-Kern-Vers: 7.0(3)N2(4.00.226)
    Running-Sys-Vers: 7.0(3)N2(4.00.226)
    Running-Service-Pack-Vers: 4.0(1)SP0(Default)
    Package-Vers: 4.0(0.147)A
    Package-Service-Pack-Vers:
    Startup-Kern-Vers: 7.0(3)N2(4.00.226)
```

```
Startup-Sys-Vers: 7.0(3)N2(4.00.226)
Startup-Service-Pack-Vers: 4.0(1)SP0(Default)
Act-Kern-Status: Ready
Act-Sys-Status: Ready
Act-Service-Pack-Status: Ready
Bootloader-Vers: v05.28(01/18/2018)
```

Removing a Service Pack from a Fabric Interconnect

In some specific scenarios, such as Open SLL, removal of the service pack will lead to FI rebooting.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope fabric-interconnect** {**a** | **b**}	Enters fabric-interconnect mode.
Step 2	UCS-A /fabric-interconnect # **remove service-pack security**	Removes the activated service pack from the fabric interconnect.
Step 3	UCS-A /fabric-interconnect # **commit-buffer**	Commits the transaction.

Example

The following example removes the service pack from fabric interconnect a and commits the transaction:

```
UCS-A# scope fabric-interconnect a
UCS-A# /fabric-interconnect # remove service-pack security
UCS-A# /fabric-interconnect* # commit-buffer
```

Adapter Firmware

The Cisco Unified Computing System supports a broad set of converged network adapters (CNAs). CNAs eliminate the need for multiple network interface cards (NICs) and host bus adapters (HBAs) by converging LAN and SAN traffic in a single interface.

All Cisco UCS network adapters:

- Allow for the reduction of the number of required network interface cards and host bus adapters
- Are managed using Cisco UCS Manager software
- Can be used in a redundant configuration with two fabric extenders and two fabric interconnects
- Enable a "wire-once" architecture that allows cabling to be configured once, with features enabled and configured using software
- Support fibre channel multipathing

The Cisco Virtual Interface Card (VIC) delivers 256 virtual interfaces and supports Cisco VM-FEX technology. The Cisco VIC provides I/O policy coherency and visibility to enable true workload mobility in virtualized environments. The Cisco VIC is available in form factors for B-Series blade servers, and C-Series rack servers.

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	(Optional) UCS-A /chassis/server/adapter # **commit-buffer**	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 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	(Optional) UCS-A /chassis/server/adapter # **show firmware**	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.

	Command or Action	Purpose
		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	(Optional) UCS-A /chassis/server/adapter # **show firmware**	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.

Example

The following example updates and activates the adapter firmware to version 4.1(0.123) 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
------------------------------------------ ------------------- -------
ucs-m82-8p-vic.4.1.0.123.bin               Adapter             4.1(0.123)

UCS-A# /chassis/server/adapter # update firmware 4.1(0.123)
UCS-A# /chassis/server/adapter* # activate firmware 4.1(0.123) set-startup-only
UCS-A# /chassis/server/adapter* # commit-buffer
UCS-A# /chassis/server/adapter #
```

The following example updates the adapter firmware to version 4.1(0.123), 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
------------------------------------------ ------------------- -------
ucs-m82-8p-vic.4.1.0.123.bin               Adapter             4.2(1.13)

UCS-A# /chassis/server/adapter # update firmware 4.2(3.13)
UCS-A# /chassis/server/adapter* # commit-buffer
UCS-A# /chassis/server/adapter # show firmware
Adapter 1:
    Running-Vers: 4.2(3.13)
    Package-Vers: 4.0(0.128)B
    Update-Status: Updating
    Activate-Status: Ready

UCS-A# /chassis/server/adapter # show firmware
Adapter 1:
    Running-Vers: 4.2(3.13)
    Package-Vers: 4.0(0.128)B
    Update-Status: Ready
    Activate-Status: Ready

UCS-A# /chassis/server/adapter # activate firmware 4.2(3.13)
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: 4.2(3.13)
    Package-Vers: 4.0(0.128)B
    Update-Status: Ready
    Activate-Status: Activating

UCS-A# /chassis/server/adapter # show firmware
Adapter 1:
    Running-Vers: 4.2(3.13)
    Package-Vers: 4.0(0.128)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: 4.2(3.13)
    Package-Vers: 4.0(0.128)B
    Update-Status: Ready
    Activate-Status: Ready
UCS-A# /chassis/server/adapter #
```

BIOS Firmware

The Basic Input Output System (BIOS) tests and initializes the hardware components of a system and boots the operating system from a storage device. In Cisco UCS, there are several BIOS settings that control the system's behavior. You can update the BIOS firmware directly from Cisco UCS Manager.

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 and and higher 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	(Optional) UCS-A /chassis/server/bios # **commit-buffer**	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.

	Command or Action	Purpose
Step 6	(Optional) UCS-A /chassis/server/bios # **show firmware**	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/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	(Optional) UCS-A /chassis/bios # **show firmware**	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.

Example

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-b200-m2-bios.S5500.2.1.3c.0.081120151437.bin
                                            Server BIOS          S5500.2.1.3c.0.081120151437
ucs-b200-m3-bios.B200M3.2.2.6c.0.110420151250.bin
                                            Server BIOS
B200M3.2.2.6c.0.110420151250
ucs-b200-m4-bios.B200M4.3.1.0.4.113020151739.bin
                                            Server BIOS          B200M4.3.1.0.4.113020151739

UCS-A# /chassis/server/bios # update firmware B200M4.3.1.0.4.113020151739
UCS-A# /chassis/server/bios* # activate firmware B200M4.3.1.0.4.113020151739
UCS-A# /chassis/server/bios* # commit-buffer
UCS-A# /chassis/server/bios #
```

CIMC Firmware

Cisco Integrated Management Controller (CIMC) is used for the management and monitoring of servers in Cisco UCS. CIMC provides options such as GUI, CLI, and IPMI for management and monitoring tasks. On the C-Series servers, CIMC runs on a separate chip. Thus, it is able to provide services in case of any major hardware failure or system crash. CIMC is also useful for initial configuration of the server and troubleshooting any problems in server operation. You can update the CIMC firmware directly from Cisco UCS Manager.

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	(Optional) UCS-A /chassis/server/cimc # **commit-buffer**	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.

	Command or Action	Purpose
Step 6	(Optional) UCS-A /chassis/server/cimc # **show firmware**	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.
Step 9	(Optional) UCS-A /chassis/server/cimc # **show firmware**	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.

Example

The following example updates and activates the CIMC firmware 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-m3-k9-cimc.4.0.1.bin               CIMC                4.0(1)
ucs-b200-m3-k9-cimc.4.0.1.bin               CIMC                4.0(1)
ucs-b200-m4-k9-cimc.4.0.1.bin               CIMC                4.0(1)
ucs-b200-m5-k9-cimc.4.0.1.bin               CIMC                4.0(1)
ucs-b22-m3-k9-cimc.4.0.1.bin                CIMC                4.0(1)

...

UCS-A# /chassis/server/cimc # update firmware 4.0(1)
UCS-A# /chassis/server/cimc* # activate firmware 4.0(1) set-startup-only
UCS-A# /chassis/server/cimc* # commit-buffer
UCS-A# /chassis/server/cimc #
```

The following example updates the CIMC firmware, 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.4.0.1.bin              CIMC                  4.0(1)
ucs-b200-m1-k9-cimc.4.0.1.bin              CIMC                  4.0(1)
ucs-b200-m1-k9-cimc.4.0.1.bin              CIMC                  4.0(1)
ucs-b200-m3-k9-cimc.4.0.1.bin              CIMC                  4.0(1)
...

UCS-A# /chassis/server/cimc # update firmware 4.0(1)
UCS-A# /chassis/server/cimc* # commit-buffer
UCS-A# /chassis/server/cimc # show firmware
Running-Vers    Update-Status   Activate-Status
--------------- --------------- ---------------
4.0(1)          Updating        Ready

UCS-A# /chassis/server/cimc # show firmware
Running-Vers    Update-Status   Activate-Status
--------------- --------------- ---------------
4.0(1)          Ready           Ready

UCS-A# /chassis/server/cimc # activate firmware 4.0(1)
UCS-A# /chassis/server/cimc* # commit-buffer
UCS-A# /chassis/server/cimc # show firmware
Running-Vers    Update-Status   Activate-Status
--------------- --------------- ---------------
4.0(1)          Ready           Activating

UCS-A# /chassis/server/cimc # show firmware
Running-Vers    Update-Status   Activate-Status
--------------- --------------- ---------------
4.0(1)          Ready           Ready
```

PSU Firmware

You can update PSU firmware directly from Cisco UCS Manager.

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.

	Command or Action	Purpose
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	(Optional) UCS-A /chassis/psu # **commit-buffer**	Commits the transaction. 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.

Example

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: V01
    Part Number: 341-0571-01
    Vendor: Cisco Systems Inc
    Serial (SN): DTM190304FD
    HW Revision: 0
    Firmware Version: 05.10
    Type: DV
    Wattage (W): 2500
    Input Source: 210AC 50 380DC
    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	Required: UCS-A /chassis/psu # **commit-buffer**	Commits the transaction. **Note** Committing the transaction resets the end points.

Example

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 03.10
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. Previously, 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. 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.

You can apply the capability catalog update as follows:

1. Download 2.2(4c) Infra/Catalog or 2.2(5b) Infra/Catalog software bundle.
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 130 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 will no longer be raised.
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 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*.

- 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 Cisco UCS B-Series M3 and Higher 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.

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	(Optional) UCS-A /chassis/server/boardcontroller # **show image**	Displays the available software images for the board controller.
Step 4	(Optional) UCS-A /chassis/server/boardcontroller # **show firmware**	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.

Example

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
------------------------------------------ ------------------- -------
ucs-b200-m3-brdprog.15.0.bin               Board Controller    15.0
ucs-b22-m3-brdprog.16.0.bin                Board Controller    16.0
ucs-b420-m3-brdprog.12.0.bin               Board Controller    12.0
```

```
UCS-A# /chassis/server/boardcontroller # show firmware
BoardController:
    Running-Vers: 15.0
    Package-Vers: 3.2(1)B
    Activate-Status: Ready

UCS-A# /chassis/server/boardcontroller # activate firmware 15.0
UCS-A# /chassis/server/boardcontroller* # commit-buffer
```

Activating the Board Controller Firmware on a Cisco UCS C-Series M3 and Higher 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 higher 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	(Optional) UCS-A /server/boardcontroller # **show image**	Displays the available software images for the board controller.
Step 4	(Optional) UCS-A /server/boardcontroller # **show firmware**	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.

Example

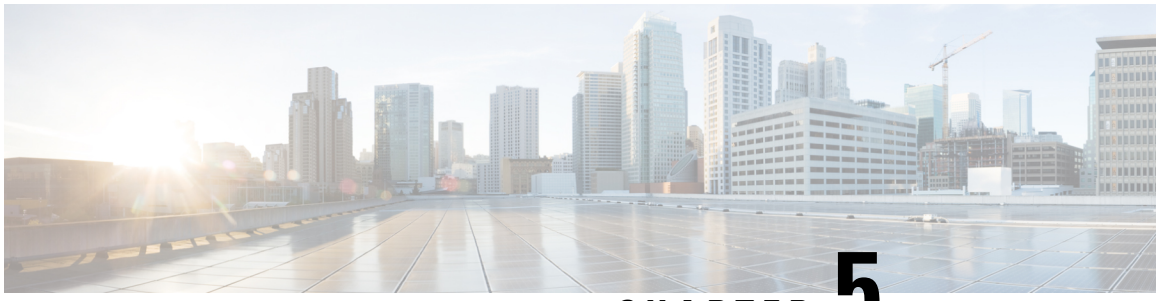
The following example activates the board controller firmware:

```
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
```



CHAPTER 5

Manage the Capability Catalog in Cisco UCS Manager

- Capability Catalog, on page 129
- Activating a Capability Catalog Update, on page 130
- Verifying that the Capability Catalog is Current, on page 131
- Viewing a Capability Catalog Provider, on page 132
- Obtaining Capability Catalog Updates from Cisco, on page 133
- Updating the Capability Catalog from a Remote Location, on page 134

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.

Note The capability catalog version is determined by the version of Cisco UCS that you are using. You can upgrade a capability catalog within the same major release version. For example, Cisco UCS 3.2(2) release can use a capability catalog with the same major release version like 3.2(1) and cannot use a capability catalog with the release version 3.0(1). However, there is an exception for Cisco UCS release 4.2(1) as it can be used only with 4.2(1) release version of capability catalog and not with later releases like 4.2(2) or previous releases like 4.0(1).

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* **force**	Activates the specified Capability Catalog version.

	Command or Action	Purpose
		You can activate the capability catalog only with the **force** option. Force option is a hidden command.
Step 4	UCS-A /system/capability # **commit-buffer**	Commits the transaction to the system configuration.

Example

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 4.x(xx)T force
UCS-A /system/capability* # commit-buffer
UCS-A /system/capability #
```

```
UCS-A# scope system
UCS-A /system # scope capability
UCS-A /system/capability # activate firmware 4.3(4.230074)T force
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 133.
Step 5	If a more recent version of the Capability Catalog is available on Cisco.com, update the Capability Catalog with that version.	

Example

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: 4.x(x)T
     Package-Vers: 4.x(x)A
    Activate-Status: Ready
UCS-A /system/capability #
```

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.

Example

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                    HW Revision
    ------------------------ ------------------------ ------------
    Cisco Systems, Inc.      N20-FAN5                 0
    Cisco Systems, Inc.      N10-FAN1                 0
    Cisco Systems, Inc.      N10-FAN2                 0
    Cisco Systems, Inc.      N5K-C5548P-FAN           0
    Cisco Systems, Inc.      N5K-C5596P-FAN           0
    Cisco Systems, Inc.      UCS-FAN-6332UP           0
    Cisco Systems, Inc.      UCS-FAN-6332UP           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 6332 Fabric Interconnect
        PID: N10-FAN1
        VID: NA
        Caption: Fan Module for UCS 6332 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 #
```

Obtaining Capability Catalog Updates from Cisco

Procedure

Step 1 In a web browser, navigate to http://www.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.

Example

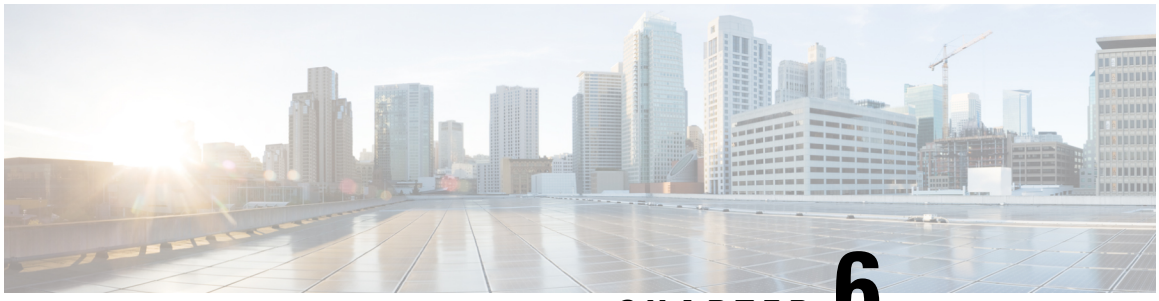
The following example uses SCP to import a Capability Catalog file:

```
UCS-A# scope system
UCS-A /system # scope capability
UCS-A /system/capability # update catalog
scp://user1@192.0.2.111/catalogs/ucs-catalog.3.1.1a.T.bin
Password:
UCS-A /system/capability # show version
Catalog:
    Update Version: 3.1(1a)T
```

```
UCS-A /system/capability # show cat-updater ucs-catalog.3.1.1a.T.bin

Catalog Updater:
    File Name                 Protocol Server          Userid          Status
    ---------                 -------- --------------- --------------- ------
    ucs-catalog.3.1.1a.T.bin  Scp      192.0.2.111     user1           Success

UCS-A /system/capability #
```



CHAPTER 6

Troubleshoot Firmware

- Recovering Fabric Interconnect During Upgrade, on page 137
- Recovering IO Modules During Firmware Upgrade, on page 144

Recovering Fabric Interconnect During Upgrade

If one or both fabric interconnects fail during failover or firmware upgrade, you can recover them by using one of the following approaches:

- Recover a fabric interconnect when you do not have a working image on the fabric interconnect
- Recover a fabric interconnect when you have a working image on the fabric interconnect
- Recover an unresponsive fabric interconnect during upgrade or failover
- Recover fabric interconnects from a failed FSM during upgrade with Auto Install

Recovering Fabric Interconnects When You Do Not Have Working Images on the Fabric Interconnect or the Bootflash

You can perform these steps when both or any fabric interconnect goes down during firmware upgrade, gets rebooted, and is stuck at the loader prompt, and you do not have working images on the fabric interconnect.

Procedure

Step 1 Reboot the switch, and in the console, press **Ctrl+L** as it boots to get the loader prompt.

Note
You may need to press the selected key combination multiple times before your screen displays the loader prompt.

Example:

```
loader>
```

Step 2 Required: Configure the interface to receive the kickstart image through TFTP.

a) Enter the local IP address and subnet mask for the system at the loader> prompt, and press **Enter**.

Example:

```
loader> set ip 10.104.105.136 255.255.255.0
```

b) Specify the IP address of the default gateway.

Example:

```
loader> set gw 10.104.105.1
```

c) Boot the kickstart image file from the required server.

Example:

```
loader> boot
tftp://10.104.105.22/tftpboot/Images.3.0.2/ucs-6300-k9-kickstart.5.0.2.N1.3.02d56.bin
switch(boot)#
```

Note
You do not need to do this step if you already have a kickstart image in the bootflash.

Step 3 Enter the **init system** command at the switch(boot)# prompt.

This will reformat the fabric interconnect.

Example:

```
switch(boot)# init system
```

Step 4 Configure the management interface.

a) Change to configuration mode and configure the IP address of the mgmt0 interface.

Example:

```
switch(boot)# config t
switch(boot)(config)# interface mgmt0
```

b) Enter the **ip address** command to configure the local IP address and the subnet mask for the system.

Example:

```
switch(boot)(config-if)# ip address 10.104.105.136 255.255.255.0
```

c) Enter the **no shutdown** command to enable the mgmt0 interface on the system.

Example:

```
switch(boot)(config-if)# no shutdown
```

d) Enter the **ip default-gateway** command to configure the IP address of the default gateway.

Example:

```
switch(boot)(config-if)# exit
switch(boot)(config)# ip default-gateway 10.104.105.1
```

e) Enter **exit** to exit to EXEC mode.

Example:

```
switch(boot)(config)# exit
```

Step 5 Copy the kickstart, system, and Cisco UCS Manager management images from the TFTP server to the bootflash.

Example:

```
switch(boot)# copy
scp://<username>@10.104.105.22/tftpboot/Images.3.0.2/ucs-6300-k9-kickstart.5.0.2.N1.3.02d56.bin
 bootflash://
switch(boot)# copy
scp://<username>@10.104.105.22/tftpboot/Images.3.0.2/ucs-6300-k9-system.5.0.2.N1.3.02d56.bin
 bootflash://
switch(boot)# copy
scp://<username>@10.104.105.22/tftpboot/Images.3.0.2/ucs-manager-k9.3.0.2d56.bin bootflash://
```

Step 6 Create separate directories for installables and installables/switch in the bootflash.

Example:

```
switch(boot)# mkdir bootflash:installables
switch(boot)# mkdir bootflash:installables/switch
```

Step 7 Copy the kickstart, system, and Cisco UCS Manager images to the installables/switch directory.

Example:

```
switch(boot)# copy ucs-6300-k9-kickstart.5.0.2.N1.3.02d56.bin bootflash:installables/switch/
switch(boot)# copy ucs-6300-k9-system.5.0.2.N1.3.02d56.bin bootflash:installables/switch/
switch(boot)# copy ucs-manager-k9.3.02d56.bin bootflash:installables/switch/
```

Step 8 Ensure that the management image is linked to nuova-sim-mgmt-nsg.0.1.0.001.bin.

nuova-sim-mgmt-nsg.0.1.0.001.bin is the name that the reserved system image uses, and it makes the management image Cisco UCS Manager-compliant.

Example:

```
switch(boot)# copy bootflash:installables/switch/ucs-manager-k9.3.02d56.bin
nuova-sim-mgmt-nsg.0.1.0.001.bin
```

Step 9 Reload the switch.

Example:

```
switch(boot)# reload
This command will reboot this supervisor module. (y/n) ? y
```

Step 10 Boot from the kickstart image.

Example:

```
loader> dir
nuova-sim-mgmt-nsg.0.1.0.001.bin
ucs-6300-k9-kickstart.5.0.2.N1.3.02d56.bin
ucs-6300-k9-system.5.0.2.N1.3.02d56.bin
ucs-manager-k9.3.02d56.bin
loader> boot ucs-6300-k9-kickstart.5.0.2.N1.3.02d56.bin
switch(boot)#
```

Step 11 Load the system image.

The **Basic System Configuration Dialog** wizard appears after the system image is completely loaded. Use this wizard to configure the fabric interconnect.

Example:

```
switch(boot)# load ucs-6300-k9-system.5.0.2.N1.3.02d56.bin
Uncompressing system image: bootflash:/ucs-6300-k9-system.5.0.2.N1.3.02d56.bin

...

---- Basic System Configuration Dialog ----

  This setup utility will guide you through the basic configuration of
  the system. Only minimal configuration including IP connectivity to
  the Fabric interconnect and its clustering mode is performed through these steps.

...

Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
Applying configuration. Please wait.

Configuration file - Ok
```

Step 12 Log in to Cisco UCS Manager and download the firmware.

Example:

```
UCS-A# scope firmware
UCS-A /firmware # download image scp://<username>@<server ip>//<downloaded image
location>/<infra bundle name>
Password:
UCS-A /firmware # download image scp://<username>@<server ip>//<downloaded image
location>/<b-series bundle name>
Password:
UCS-A /firmware # download image scp://<username>@<server ip>//<downloaded image
location>/<c-series bundle name>
Password:
UCS-A /firmware # show download-task
Download task:
    File Name Protocol Server          Userid          State
    --------- -------- --------------- --------------- -----
    ucs-k9-bundle-b-series.3.0.2.B.bin
              Scp      10.104.105.22   abcdefgh        Downloading
    ucs-k9-bundle-c-series.3.0.2.C.bin
              Scp      10.104.105.22   abcdefgh        Downloading
    ucs-k9-bundle-infra.3.0.2.A.bin
              Scp      10.104.105.22   abcdefgh        Downloading
UCS-A /firmware #
```

Step 13 After the firmware download is complete, activate the fabric interconnect firmware and Cisco UCS Manager firmware.

This step updates Cisco UCS Manager and the fabric interconnects to the version you want, and then reboots them.

Example:

```
UCS-A# scope fabric-interconnect a
UCS-A /fabric-interconnect* # activate firmware kernel-version 5.0(2)N1(3.02d56)
ignorecompcheck
Warning: When committed this command will reset the end-point
```

```
UCS-A /fabric-interconnect* # activate firmware system-version 5.0(2)N1(3.02d56)
ignorecompcheck
Warning: When committed this command will reset the end-point
UCS-A /fabric-interconnect* # commit-buffer
UCS-A /fabric-interconnect # exit

UCS-A# scope system
UCS-A /system # show image

Name                                        Type                Version
------------------------------------------- ------------------- -------
ucs-manager-k9.3.02d56.bin                  System              3.0(2d)
UCS-A /system # activate firmware 3.0(2d) ignorecompcheck
The version specified is the same as the running version
UCS-A /system # activate firmware 3.0(2d) ignorecompcheck
The version specified is the same as the running version
UCS-A /system #
```

Recovering Fabric Interconnect During Upgrade When You have Working Images on the Bootflash

You can perform these steps when both or any fabric interconnect goes down during firmware upgrade, gets rebooted, and is stuck at the loader prompt.

Before you begin

You must have working images on the bootflash to perform these steps.

Procedure

Step 1 Reboot the switch, and in the console, press Ctrl+L as it boots to get the loader prompt.

Note
You may need to press the selected key combination multiple times before your screen displays the loader prompt.

Example:

```
loader>
```

Step 2 Run the **dir** command.

The list of available kernel, system, and Cisco UCS Manager images in the bootflash appears.

Example:

```
loader> dir
nuova-sim-mgmt-nsg.0.1.0.001.bin
ucs-6400-k9-kickstart.5.0.2.N1.3.02d56.bin
ucs-6400-k9-system.5.0.2.N1.3.02d56.bin
ucs-manager-k9.3.02d56.bin
```

Step 3 Boot the kernel firmware version from the bootflash.

Note
Any kernel image available here will be a working image from which you can boot.

Example:

```
loader> boot ucs-6400-k9-kickstart.5.0.2.N1.3.02d56.bin
```

Step 4 Ensure that the management image is linked to nuova-sim-mgmt-nsg.0.1.0.001.bin.

nuova-sim-mgmt-nsg.0.1.0.001.bin is the name that the reserved system image uses, and it makes the management image Cisco UCS Manager-compliant.

Example:

```
switch(boot)# copy ucs-manager-k9.1.4.1k.bin nuova-sim-mgmt-nsg.0.1.0.001.bin
```

Step 5 Load the system image.

Example:

```
switch(boot)# load ucs-6400-k9-system.5.0.2.N1.3.02d56.bin
```

Step 6 Log in to Cisco UCS Manager and update your fabric interconnect and Cisco UCS Manager software to the version that you want.

Recovering Unresponsive Fabric Interconnects During Upgrade or Failover

During upgrade or failover, avoid performing the following tasks because they introduce additional risk:

- Pmon stop/start
- FI reboots – power cycle or CLI
- HA failover

Procedure

Step 1 If the **httpd_cimc.sh** process is lost, as documented in CSCup70756, you lose access to the KVM. Continue with the failover or contact Cisco Technical Assistance.

Step 2 If you lose access to the KVM on the primary side, continue with the failover to resolve the issue.

Step 3 If KVM is needed or is down on the subordinate side, start only that service using the debug plugin. Contact TAC to run the debug image.

Step 4 If the /dev/null issue is encountered, as documented in CSCuo50049, fix the rights to 666 with the debug-plugin at both steps if required. Contact Cisco Technical Assistance to run debug commands.

Step 5 If both CSCup70756 and CSCuo50049 are encountered, it can cause VIP loss. If the VIP is lost, do the following:

a. Access the primary physical address through the GUI and use the GUI to verify all IO Module backplane ports recovered.

b. If the GUI is down, verify IO Module backplane ports with the NXOS **show fex detail** command.

c. Perform the workaround and verify that the cluster state is UP on both fabric interconnects.

d. If the cluster state is UP on both fabric interconnects, continue the upgrade by reacknowledging the primary fabric interconnect reboot using the SSH CLI syntax:

```
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 #
```

Recovering Fabric Interconnects From a Failed FSM During Upgrade With Auto Install

You can perform these steps when all the following occur:

- You are upgrading or downgrading firmware using Auto Install between Cisco UCS Manager Release 3.1(2) and Release 3.1(3) while a service pack is installed on the fabric interconnects.
- Both or any fabric interconnect goes down because of an FSM failure or multiple retries in the DeployPollActivate stage of the FSM

Procedure

Step 1 When the FSM fails, or when multiple retries are observed in the DeployPollActivate stage of the FSM on the subordinate fabric interconnect, do the following:

a) Clear the startup version of the default infrastructure pack and the service pack.

Example:

```
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
```

b) Remove the service pack from the subordinate fabric interconnect.

Example:

```
UCS-A# scope fabric-interconnect b
UCS-A# /fabric-interconnect # remove service-pack security
UCS-A# /fabric-interconnect* # commit-buffer
```

Step 2 Upgrade the infrastructure firmware using the force option through Auto Install.

Example:

```
UCS-A# scope firmware
UCS-A /firmware # scope auto-install
UCS-A /firmware/auto-install # install infra infra-vers 3.1(3a)A force
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
(6) Check if any hardware (fabric interconnects, io-modules, servers or adapters) is
unsupported in the target release
Do you want to proceed? (yes/no): yes
Triggering Install-Infra with:
Infrastructure Pack Version: 3.1(3a)A
```

Step 3 Acknowledge the reboot of the primary fabric interconnect.

Example:

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

Step 4 When the FSM fails, or when multiple retries are observed in the DeployPollActivate stage of the FSM on the current subordinate fabric interconnect, do the following:

a) Clear the startup version of the default infrastructure pack and the service pack.

Example:

```
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
```

b) Remove the service pack from the current subordinate fabric interconnect.

Example:

```
UCS-A# scope fabric-interconnect a
UCS-A# /fabric-interconnect # remove service-pack security
UCS-A# /fabric-interconnect* # commit-buffer
```

Both fabric interconnects will now reflect Release 3.1(3) firmware and the default service pack for Running and Startup versions.

Recovering IO Modules During Firmware Upgrade

You can recover an IO Module during firmware upgrade by resetting it from a peer IO Module. After it is reset, it can derive the configuration from the fabric interconnect.

Resetting an I/O Module from a Peer I/O Module

Sometimes, I/O module upgrades can result in failures or I/O modules can become unreachable from Cisco UCS Manager due to memory leaks. You can reboot an I/O module that is unreachable through its peer I/O module.

Resetting the I/O module restores the I/O module to factory default settings, deletes all cache files and temporary files, but retains the size-limited OBFL file.

Procedure

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

Step 2 Expand **Equipment** > **Chassis** > ***Chassis Number*** > **IO Modules**.

Step 3 Choose the peer I/O module of the I/O module that you want to reset.

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

Step 5 In the Actions area, click **Reset Peer IO Module**.