



Upgrading Between Cisco UCS 2.0 Releases

First Published: March 15, 2012

Last Modified: April 06, 2014

Americas Headquarters

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

Text Part Number: OL-26682-04

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

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

© 2012-2014 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface

Preface vii

Audience vii

Organization vii

Conventions viii

Related Documentation ix

Documentation Feedback ix

Obtaining Documentation and Submitting a Service Request ix

PART I

Firmware Upgrades 1

CHAPTER 1

Overview of Upgrading to Release 2.0 3

Overview of Firmware 3

Firmware Image Management 4

Firmware Versions 5

Firmware Upgrade to Cisco UCS, Release 2.0 6

Cautions, Guidelines, and Limitations for Firmware Upgrades 6

Configuration Changes and Settings that Can Impact Upgrades 7

Hardware-Related Guidelines and Limitations for Firmware Upgrades 9

Firmware- and Software-Related Guidelines and Limitations for Upgrades 10

Outage Impacts of Direct Firmware Upgrades 11

Summary of Steps for Upgrading from Release 2.0 12

CHAPTER 2

Completing the Prerequisites for Upgrading the Firmware 15

Prerequisites for Upgrading and Downgrading Firmware 15

Creating an All Configuration Backup File 16

Verifying the Overall Status of the Fabric Interconnects 18

Verifying the High Availability Status and Roles of a Cluster Configuration 18

Verifying the Status of I/O Modules	19
Verifying the Status of Servers	20
Verifying the Status of Adapters on Servers in a Chassis	21
Obtaining Cisco UCS PowerTool and Running the Duplicate IQN Script	21

CHAPTER 3**Downloading the Release 2.0 Firmware 25**

Obtaining Software Bundles from Cisco	25
Downloading Firmware Packages to the Fabric Interconnect	26
Determining the Contents of a Firmware Package	28
Canceling an Image Download	28
Verifying Local Storage Space on a Fabric Interconnect	29
Checking the Available Space on a Fabric Interconnect	29
Deleting Firmware Images from a Fabric Interconnect	29

CHAPTER 4**Upgrading the Firmware to Release 2.0 31**

Summary of Steps for Upgrading from Release 2.0	31
Disabling Call Home	33
Updating the Firmware on the Adapters, BMCs, and IOMs	33
Activating the Firmware on the Adapters and BMCs	34
Activating the Board Controller Firmware on a Server	35
Activating the Cisco UCS Manager Software to Release 2.0	36
Activating the Firmware on the IOMs	37
Activating the Fabric Interconnect Firmware for a Cluster Configuration	38
Activating the Firmware on a Subordinate Fabric Interconnect	38
Forcing a Fabric Interconnect Failover	39
Verifying that the Data Path is Ready	40
Verifying that Dynamic vNICs Are Up and Running	40
Verifying the Ethernet Data Path	40
Verifying the Data Path for Fibre Channel End-Host Mode	41
Verifying the Data Path for Fibre Channel Switch Mode	42
Activating the Firmware on a Primary Fabric Interconnect	42
Activating the Firmware on a Standalone Fabric Interconnect	43
Updating Host and Management Firmware Packages	44
Effect of Updates to Firmware Packages in Service Profiles	44
Updating a Management Firmware Package	46

Updating a Host Firmware Package	47
Enabling Call Home	49

PART II**Hardware Upgrades 51**

CHAPTER 5**Upgrading Cisco UCS Hardware 53**

Upgrading Fabric Interconnects	53
Fabric Interconnect Upgrade Considerations	53
Port Mapping for Upgrades	54
Fabric Interconnect Port Connection Record	59
Upgrading a Fabric Interconnect Cluster	61
Upgrading I/O Modules	63
I/O Module Upgrade Considerations	63
I/O Module Port Connection Record	65
Upgrading an I/O Module	66
Upgrading Adapter Cards	66
Adapter Card Upgrade Considerations	66
Upgrading an Adapter Card	67
Upgrading Integrated Rack-Mount Servers	68
Required Order of Steps for Integrating Cisco UCS Rack-Mount Servers	68
Upgrades of Integrated Rack-Mount Servers	68



Preface

This preface includes the following sections:

- [Audience, page vii](#)
- [Organization, page vii](#)
- [Conventions, page viii](#)
- [Related Documentation, page ix](#)
- [Documentation Feedback, page ix](#)
- [Obtaining Documentation and Submitting a Service Request, page ix](#)

Audience

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

Organization

This document includes the following chapters:

Chapter	Title	Description
Part 1	Firmware Upgrades	Contains the information, prerequisites, required order of steps, and procedures that you must follow to successfully upgrade a Cisco UCS domain to the specified release with Cisco UCS Manager.
Part 2	Hardware Upgrades	Contains the information, prerequisites, and procedures that you must follow to successfully upgrade hardware in a Cisco UCS domain.

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 <i>this font</i> .
TUI elements	In a Text-based User Interface, text the system displays appears in <i>this font</i> .
System output	Terminal sessions and information that the system displays appear in <i>this font</i> .
CLI commands	CLI command keywords appear in this font . Variables in a CLI command appear in <i>this font</i> .
[]	Elements in square brackets are optional.
{x y z}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x y z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
<>	Nonprinting characters such as passwords are in angle brackets.
[]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.



Note

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



Tip

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

**Caution**

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

**Timesaver**

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

**Warning****IMPORTANT SAFETY INSTRUCTIONS**

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

SAVE THESE INSTRUCTIONS

Related Documentation

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

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

Documentation Feedback

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

Obtaining Documentation and Submitting a Service Request

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

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

Follow [Cisco UCS Docs on Twitter](#) to receive document update notifications.



PART **I**

Firmware Upgrades

- [Overview of Upgrading to Release 2.0, page 3](#)
- [Completing the Prerequisites for Upgrading the Firmware, page 15](#)
- [Downloading the Release 2.0 Firmware , page 25](#)
- [Upgrading the Firmware to Release 2.0, page 31](#)



CHAPTER 1

Overview of Upgrading to Release 2.0

This chapter includes the following sections:

- [Overview of Firmware, page 3](#)
- [Firmware Image Management, page 4](#)
- [Firmware Versions, page 5](#)
- [Firmware Upgrade to Cisco UCS, Release 2.0, page 6](#)

Overview of Firmware

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

- Cisco UCS Manager
- I/O modules
- Fabric interconnects
- Endpoints physically located on adapters, including NIC and HBA firmware, and Option ROM (where applicable) that can be upgraded through firmware packages included in a service profile
- Endpoints physically located on servers, such as the BIOS, storage controller (RAID controller), and Cisco Integrated Management Controller (CIMC) that can be upgraded through firmware packages included in a service profile

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



Note

Beginning with Cisco UCS, Release 1.4(1), Cisco is releasing firmware upgrades in multiple bundles, rather than one large firmware package. For more information see [Firmware Image Management, on page 4](#).

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

This document uses the following definitions for managing firmware:

Upgrade

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

Update

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

Activate

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

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

Firmware Image Management

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

Cisco UCS Infrastructure Software Bundle

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

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

Cisco UCS B-Series Blade Server Software Bundle

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

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

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

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

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



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

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

Firmware Versions

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

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

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

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

Running Version

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

Startup Version

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

Backup Version

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

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

Firmware Versions in the Fabric Interconnect and Cisco UCS Manager

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

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

Firmware Upgrade to Cisco UCS, Release 2.0

The firmware upgrade to Cisco UCS, Release 2.0 needs to be planned with scheduled maintenance windows for standalone fabric interconnects. With this firmware upgrade, you should expect the following data traffic interruptions:

- With a cluster configuration, no data traffic disruption if the correct sequence of steps is followed. Failover between the fabric interconnects prevents the longer disruption required for the fabric interconnects and I/O modules to reboot.
- With a standalone fabric interconnect, data traffic disruption of up to one minute for the servers to reboot and approximately ten minutes for the fabric interconnect and I/O module to reboot.

This firmware upgrade requires a combination of the following methods:

- Direct upgrade at the endpoints. For a cluster configuration with two fabric interconnects, a direct upgrade can be minimally disruptive to data traffic. However, it requires that the Cisco UCS domain does not include firmware policies for those endpoints that you upgrade directly. You cannot avoid disruption to traffic in a Cisco UCS domain with only one fabric interconnect.



Note

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

- Upgrades to server endpoints through service profiles that include a host firmware package, a management firmware package, or both. This method can be disruptive to data traffic and should be performed during a maintenance window.

Cautions, Guidelines, and Limitations for Firmware Upgrades

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

**Note**

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

Configuration Changes and Settings that Can Impact Upgrades

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

Impact of Upgrade to Cisco UCS, Release 2.1(2) and Higher on Initiator IQNs Defined at the Service Profile Level

If there are two iSCSI vNICs and both use the same initiator IQN (which is supported in Cisco UCS Release 2.0(1)), upgrading creates a single service profile level initiator IQN and resets the initiator IQNs on the iSCSI vNICs to have no value.

If the same initiator IQNs are used in iSCSI vNICs across service profiles in Cisco UCS Release 2.0(1), the upgrade creates duplicate initiator IQNs at the service profile level. This configuration generates faults for each iSCSI vNIC that has a duplicate initiator IQN defined at the service profile level. Changing the duplicate initiator IQNs at the service profile level clears these faults. You must clear these faults before you perform any service profile related operations, such as updating a host firmware package.

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 Ack, 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 on the overlapped VLANs. Therefore, we recommend that you ensure there are no overlapping Ethernet and FCoE VLAN IDs before you upgrade to Cisco UCS Release 2.2.

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.

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

For a new installation of Cisco UCS Release 2.2, the default VLAN IDs are as follows:

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

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

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



Note

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

VSANs with IDs in the Reserved Range are not Operational

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

IQN Names Must Be Unique for Each iSCSI vNIC

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

Cisco provides a script for Cisco UCS PowerTool that identifies duplicate IQN names within a Cisco UCS domain. For more information, see [Obtaining Cisco UCS Power Tool and Running the Duplicate IQN Script](#).

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

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

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

Unassociated Servers

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



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

Associated Servers

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

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

Hardware-Related Guidelines and Limitations for Firmware Upgrades

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

No Server or Chassis Maintenance



Caution

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

Avoid Replacing RAID-Configured Hard Disks 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 Cisco UCS Gen-2 Adapters through a Host Firmware Package

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

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

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

Number of Fabric Interconnects

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

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

Firmware- and Software-Related Guidelines and Limitations for Upgrades

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

Determine the Appropriate Type of Firmware Upgrade for Each Endpoint

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

Upgrades of a CIMC through a management firmware package or an adapter through a firmware package in the service profile associated with the server take precedence over direct firmware upgrades. You cannot

directly upgrade an endpoint if the service profile associated with the server includes a firmware package. To perform a direct upgrade, you must remove the firmware package from the service profile.

Do Not Activate All Endpoints Simultaneously in Cisco UCS Manager GUI

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

Impact of Activation for Adapters and I/O Modules

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

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

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

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

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

Outage Impacts of Direct Firmware Upgrades

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

Outage Impact of a Fabric Interconnect Firmware Upgrade

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

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

Outage Impact of a Cisco UCS Manager Firmware Upgrade

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

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

Outage Impact of an I/O Module Firmware Upgrade

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

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

Outage Impact of a CIMC Firmware Upgrade

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

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

Outage Impact of an Adapter Firmware Upgrade

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

- The server reboots.
- Server traffic is disrupted.

Summary of Steps for Upgrading from Release 2.0



Note

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

The order of steps in this document and the recommended options minimize the disruption to data traffic. Therefore, when you upgrade from any version of Release 2.0, upgrade the components in the following order.

- 1 Complete all prerequisite steps, as described in [Prerequisites for Upgrading and Downgrading Firmware, on page 15](#).
- 2 Obtain the following firmware images from Cisco.com and download them to the fabric interconnect. For more information, see [Downloading the Cisco UCS, Release 2.1 Firmware](#).
 - Cisco UCS Infrastructure Software Bundle—Required for all Cisco UCS domains.
 - Cisco UCS B-Series Blade Server Software Bundle—Required for all Cisco UCS domains that include blade servers.
 - Cisco UCS C-Series Rack-Mount UCS-Managed Server Software Bundle—Only required for Cisco UCS domains that include integrated rack-mount servers. This bundle contains firmware to enable Cisco UCS Manager to manage those servers and is not applicable to standalone C-Series rack-mount servers.
- 3 (Optional) Disable Call Home—If the Cisco UCS domain includes Call Home or Smart Call Home, disable Call Home to ensure you do not receive unnecessary alerts when Cisco UCS Manager restarts components.
- 4 Update adapters, CIMC, and IOMs—If you prefer, you can upgrade the CIMC and the adapters in a host firmware package as part of the last upgrade step. Certain adapters must be upgraded in a host firmware package.
- 5 Activate adapters—Choose **Ignore Compatibility Check** and **Set Startup Version Only** when performing this step.
- 6 Activate CIMC—Choose **Ignore Compatibility Check** when performing this step.
- 7 Activate Cisco UCS Manager—Choose **Ignore Compatibility Check** when performing this step.
- 8 Activate the I/O modules—Choose **Ignore Compatibility Check** and **Set Startup Version Only** when performing this step.
- 9 Activate the subordinate fabric interconnect—Choose **Ignore Compatibility Check** when performing this step.
- 10 To avoid control plane disruption, manually failover the primary fabric interconnect to the fabric interconnect that has already been upgraded.
- 11 Verify that the data path has been restored.
- 12 Activate the primary fabric interconnect—Choose **Ignore Compatibility Check** when performing this step.
- 13 Update management firmware package(s) for servers—You do not need to perform this step if you updated and activated the CIMC on the servers directly.
- 14 Update host firmware package(s) for servers—Must be the last firmware upgraded. We recommend that you upgrade the board controller firmware during this step to avoid an additional reboot of servers with that firmware. While some of these components can be upgraded directly at the endpoint, such as the BIOS on M3 servers, we recommend that you upgrade the following firmware in a host firmware package:
 - BIOS
 - Storage controller
 - Certain adapters

For information on how to upgrade these endpoints directly, see the [Cisco UCS Manager Configuration Guides](#).

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



CHAPTER 2

Completing the Prerequisites for Upgrading the Firmware

This chapter includes the following sections:

- [Prerequisites for Upgrading and Downgrading Firmware, page 15](#)
- [Creating an All Configuration Backup File, page 16](#)
- [Verifying the Overall Status of the Fabric Interconnects, page 18](#)
- [Verifying the High Availability Status and Roles of a Cluster Configuration, page 18](#)
- [Verifying the Status of I/O Modules, page 19](#)
- [Verifying the Status of Servers, page 20](#)
- [Verifying the Status of Adapters on Servers in a Chassis, page 21](#)
- [Obtaining Cisco UCS PowerTool and Running the Duplicate IQN Script, page 21](#)

Prerequisites for Upgrading and Downgrading Firmware

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

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



Note

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

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

- Review the Release Notes.
- Review the relevant [Hardware and Software Interoperability Matrix](#) to ensure the operating systems on all servers have the right driver levels for the release of Cisco UCS to which you plan to upgrade.
- Back up the configuration into an All Configuration backup file.
- For a cluster configuration, verify that the high availability status of the fabric interconnects shows that both are up and running.
- For a standalone configuration, verify that the Overall Status of the fabric interconnect is Operable.
- Verify that the data path is up and running. For more information, see [Verifying that the Data Path is Ready](#), on page 40.
- 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 2.0(2) or higher:
 - Ensure that all iSCSI vNICs used within a single service profile or across multiple service profiles have unique initiator names.
 - If any iSCSI vNICs have the same initiator name, reconfigure the IQNs with unique initiator names.
 - Make the corresponding IQN initiator name changes on any network storage devices to ensure that the boot LUNs are visible to the new IQN.

Creating an All Configuration Backup File

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

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

Before You Begin

Obtain the backup server IP address and authentication credentials.

Procedure

- Step 1** In the **Navigation** pane, click the **Admin** tab.
- Step 2** Click the **All** node.
- Step 3** In the **Work** pane, click the **General** tab.
- Step 4** In the **Actions** area, click **Backup**.
- Step 5** In the **Backup Configuration** dialog box, click **Create Backup Operation**.
- Step 6** In the **Create Backup Operation** dialog box, do the following:
- Complete the following fields:
 - Admin State** field—Click the **Enabled** radio button to run the backup operation as soon as you click **OK**.
 - Type** field—Click the **All Configuration** radio button to create an XML backup file that includes all system and logical configuration information.
 - Preserve Identities** check box—If the Cisco UCS domain includes any identities derived from pools that you need to preserve, check this check box.

Identities such as MAC addresses, WWNNs, WWPNs, or UUIDS are assigned at runtime. If you do not want these identities to change after you import the backup file, you must check this check box. If you do not, these identities may be changed after the import and operations such as a PXE boot or a SAN boot may no longer function.
 - Protocol** field—Click the one of the following radio buttons to indicate the protocol you want to use to transfer the file to the backup server:
 - FTP**
 - TFTP**
 - SCP**
 - SFTP**
 - Hostname** field—Enter the IP address or hostname of the location where the backup file is to be stored. This can be a server, storage array, local drive, or any read/write media that the fabric interconnect can access through the network. If you use a hostname, you must configure Cisco UCS Manager to use a DNS server.
 - Remote File** field—Enter the full path to the backup configuration file. This field can contain the filename as well as the path. If you omit the filename, the backup procedure assigns a name to the file.
 - User** field—Enter the username that Cisco UCS Manager should use to log in to the backup location. You do not need to complete this field if you selected TFTP for the protocol.
 - Password** field—Enter the password associated with the username. You do not need to complete this field if you selected TFTP for the protocol.
 - Click **OK**.
- Step 7** If Cisco UCS Manager displays a confirmation dialog box, click **OK**.

If you set the **Admin State** field to enabled, Cisco UCS Manager takes a snapshot of the configuration type that you selected and exports the file to the network location. The backup operation displays in the **Backup Operations** table in the **Backup Configuration** dialog box.

- Step 8** (Optional) To view the progress of the backup operation, do the following:
- If the operation does not display in the **Properties** area, click the operation in the **Backup Operations** table.
 - In the **Properties** area, click the down arrows on the **FSM Details** bar. The **FSM Details** area expands and displays the operation status.
- Step 9** Click **OK** to close the **Backup Configuration** dialog box. The backup operation continues to run until it is completed. To view the progress, re-open the **Backup Configuration** dialog box.
-

Verifying the Overall Status of the Fabric Interconnects

Procedure

- Step 1** In the **Navigation** pane, click the **Equipment** tab.
- Step 2** On the **Equipment** tab, expand **Equipment > Fabric Interconnects**.
- Step 3** Click the node for the fabric interconnect that you want to verify.
- Step 4** In the **Work** pane, click the **General** tab.
- Step 5** In the **Status** area, verify that the **Overall Status** is **operable**. If the status is not **operable**, create and download a Tech Support file, and contact Cisco Technical Support. Do not proceed with the firmware upgrade. For more information about Tech Support files, see the *Cisco UCS Manager B-Series Troubleshooting Guide*.
-

Verifying the High Availability Status and Roles of a Cluster Configuration

The high availability status is the same for both fabric interconnects in a cluster configuration.

Procedure

- Step 1** In the **Navigation** pane, click the **Equipment** tab.
- Step 2** On the **Equipment** tab, expand **Equipment > Fabric Interconnects**.
- Step 3** Click the node for one of the fabric interconnects in the cluster.
- Step 4** In the **Work** pane, click the **General** tab.
- Step 5** If the fields in the **High Availability Details** area are not displayed, click the **Expand** icon to the right of the heading.
- Step 6** Verify that the following fields display the following values:

Field Name	Required Value
Ready field	Yes
State field	Up

If the values are different, create and download a Tech Support file, and contact Cisco Technical Support. Do not proceed with the firmware upgrade. For more information about Tech Support files, see the *Cisco UCS Manager B-Series Troubleshooting Guide*.

- Step 7** Note the value in the **Leadership** field to determine whether the fabric interconnect is the primary or subordinate.
You need to know this information to upgrade the firmware on the fabric interconnects.

Verifying the Status of I/O Modules

Procedure

- Step 1** In the **Navigation** pane, click the **Equipment** tab.
- Step 2** On the **Equipment** tab, expand **Equipment > Chassis**.
- Step 3** Click on the chassis for which you want to verify the status of the I/O modules.
- Step 4** In the **Work** pane, click the **IO Modules** tab.
- Step 5** For each I/O module, verify that the following columns display the following values:

Field Name	Desired Value
Overall Status column	ok
Operability column	operable

If the values are different, create and download a Tech Support file, and contact Cisco Technical Support. Do not proceed with the firmware upgrade. For more information about Tech Support files, see the *Cisco UCS Manager B-Series Troubleshooting Guide*.

Step 6 Repeat Steps 3 through 5 to verify the status of the I/O modules in each chassis.

Verifying the Status of Servers

If a server is inoperable, you can proceed with the upgrade for other servers in the Cisco UCS domain. However, you cannot upgrade the inoperable server.

Procedure

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

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

Step 3 In the **Work** pane, click the **Servers** tab to display a list of all servers in all chassis.

Step 4 For each server, verify that the following columns display the following values:

Field Name	Desired Value
Overall Status column	<p>ok, unassociated, or any value that does not indicate a failure.</p> <p>If the value indicates a failure, such as discovery-failed, the endpoints on that server cannot be upgraded.</p>
Operability column	operable

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

- a) Right-click the server for which you want to verify the discovery status and choose **Show Navigator**.
 - b) In the **Status Details** area of the **General** tab, verify that the **Discovery State** field displays a value of **complete**.
If the fields in the **Status Details** area are not displayed, click the **Expand** icon to the right of the heading.
-

Verifying the Status of Adapters on Servers in a Chassis

Procedure

- Step 1** In the **Navigation** pane, click the **Equipment** tab.
- Step 2** On the **Equipment** tab, expand **Equipment > Chassis > Chassis Number > Servers**.
- Step 3** Click the server for which you want to verify the status of the adapters.
- Step 4** In the **Work** pane, click the **Inventory** tab.
- Step 5** In the **Inventory** tab, click the **Adapters** subtab.
- Step 6** For each adapter, verify that the following columns display the following values:

Field Name	Desired Value
Overall Status column	ok
Operability column	operable

If the fields show a different value and the adapter is inoperable, you can proceed with the upgrade for other adapters on the servers in the Cisco UCS domain. However, you cannot upgrade the inoperable adapter.

Obtaining Cisco UCS PowerTool and Running the Duplicate IQN Script

If a Cisco UCS domain is configured for iSCSI boot, before you upgrade from Cisco UCS, Release 2.0(1) to Cisco UCS, Release 2.0(2) or higher, you must ensure that all iSCSI vNICs used across multiple service profile have unique initiator names.

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

Procedure

- Step 1** To download Cisco UCS PowerTool, do the following:
- In your web browser, navigate to the following website: <http://developer.cisco.com/web/unifiedcomputing/microsoft>
 - Scroll down to the **Cisco UCS PowerTool (PowerShell Toolkit) Beta Download** area.
 - Download the `CiscoUcs-PowerTool-0.9.6.0.zip` file.
 - Unzip the file and follow the prompts to install Cisco UCS PowerTool.
You can install Cisco UCS PowerTool on any Windows computer. You do not need to install it on a computer used to access Cisco UCS Manager.
- Step 2** To launch Cisco UCS PowerTool, enter the following at a command line:

```
C:\Program Files (x86)\Cisco\Cisco UCS PowerTool>C:\Windows\System32\windowspowershell\v1.0\powershell.exe -NoExit -ExecutionPolicy RemoteSigned -File .\StartUcsPS.ps1
```

Example:

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

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

Step 3 In Cisco UCS PowerTool, do the following:

- a) Connect to Cisco UCS Manager, as follows:

```
PS C:\> Connect-Ucs IP_address
```

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

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

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

```
Cookie           : 1331303969/2af0afde-6627-415c-b85f-a7cae6233de3
Domains          :
LastUpdateTime   : 3/9/2012 6:20:42 AM
Name             : 209.165.201.15
NoSsl            : False
NumPendingConfigs : 0
NumWatchers      : 0
Port             : 443
Priv             : {admin, read-only}
RefreshPeriod    : 600
SessionId        : web_49846_A
TransactionInProgress : False
Ucs              : ucs-4
Uri              : https://209.165.201.15
UserName         : admin
VirtualIpv4Address : 209.165.201.15
Version          : 2.0 (2i)
WatchThreadStatus : None
```

Step 4 In the Cisco UCS PowerTool, run the following script to validate your iSCSI boot configuration and check for duplicate IQNs :

```
PS C:\> Get-UcsServiceProfile -type instance | Get-UcsVnicIScsi | ? { $_.InitiatorName -ne "" } | select
Dn,InitiatorName | group InitiatorName | ? { $_.Count -gt 1 } | % { $obj = New-Object PSObject ; $obj
| Add-Member NoteProperty Count $_.Count; $obj | Add-Member NoteProperty InitiatorName $_.Name;
$obj | Add-Member NoteProperty Dn ($_ | select -exp Group | % { $_.Dn } ); $obj }
```

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

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



```

4 iqn.2012-01.cisco.com:s... {org-root/ls-SP_2_7/is...
2 iqn.2012-01.cisco.com:s... {org-root/org-sub1/ls-...
2 iqn.2012-01.cisco.com:s... {org-root/org-sub2/ls-...

```

Step 5 (Optional) If you have .NET Framework 3.5 Service Pack 1 installed, you can use the following script to view the output in the GUI:

```

PS C:\> Get-UcsServiceProfile -type instance | Get-UcsVnicIscsi | ? { $_.InitiatorName -ne "" } | select
Dn,InitiatorName | group InitiatorName | ? { $_.Count -gt 1 } | % { $obj = New-Object PSObject ; $obj
| Add-Member NoteProperty Count $_.Count; $obj | Add-Member NoteProperty InitiatorName $_.Name;
$obj | Add-Member NoteProperty Dn ($_ | select -exp Group | % { $_.Dn } ); $obj } | ogv

```

Step 6 Disconnect from Cisco UCS Manager, as follows:

```

PS C:\> Disconnect-Ucs

```

What to Do Next

If duplicate IQNs exist across multiple service profiles in the Cisco UCS domain, reconfigure the iSCSI vNICs with unique IQNs in Cisco UCS Manager before you upgrade to Cisco UCS, Release 2.1 or greater.

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



Downloading the Release 2.0 Firmware

This chapter includes the following sections:

- [Obtaining Software Bundles from Cisco](#), page 25
- [Downloading Firmware Packages to the Fabric Interconnect](#), page 26
- [Determining the Contents of a Firmware Package](#), page 28
- [Canceling an Image Download](#), page 28
- [Verifying Local Storage Space on a Fabric Interconnect](#), page 29

Obtaining Software Bundles from Cisco

Before You Begin

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

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

Procedure

- Step 1** In a web browser, navigate to Cisco.com.
- Step 2** Under **Support**, click **All Downloads**.
- Step 3** In the center pane, click **Servers - Unified Computing**.
- Step 4** If prompted, enter your Cisco.com username and password to log in.
- Step 5** In the right pane, click the link for the software bundles you require, as follows:

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

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

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

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

- a) Click the link for the latest release 2.0 software bundle.
The release number is followed by a number and a letter in parentheses. The number identifies the maintenance release level, and the letter differentiates between patches of that maintenance release. For more information about what is in each maintenance release and patch, see the latest version of the Release Notes.
- b) Click one of the following buttons and follow the instructions provided:
 - **Download Now**—Allows you to download the software bundle immediately.
 - **Add to Cart**—Adds the software bundle to your cart to be downloaded at a later time.
- c) Follow the prompts to complete your download of the software bundle(s).

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

What to Do Next

Download the software bundles to the fabric interconnect.

Downloading Firmware Packages to the Fabric Interconnect

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



Note

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

Before You Begin

Obtain the required firmware bundles from Cisco.

Procedure

- Step 1** In the **Navigation** pane, click the **Equipment** tab.
- Step 2** Click the **Equipment** node.
- Step 3** In the **Work** pane, click the **Firmware Management** tab.
- Step 4** Click the **Installed Firmware** tab.
- Step 5** Click **Download Firmware**.
- Step 6** In the **Download Firmware** dialog box, complete the following fields:

Name	Description
Protocol field	The protocol to use when communicating with the remote server. This can be one of the following: <ul style="list-style-type: none"> • FTP • TFTP • SCP • SFTP <p>Note TFTP has a file size limitation of 32 MB. Because firmware bundles can be much larger than that, we recommend that you do not choose TFTP for firmware downloads.</p>
Server field	If the file came from a remote server, this is the IP address or hostname of the remote server on which the files resides. If the file came from a local source, this field displays "local". <p>Note If you use a hostname rather than an IP address, you must configure a DNS server in Cisco UCS Manager.</p>
Filename field	The name of the firmware file.
Path field	The absolute path to the file on the remote server. <p>If you use SCP, the absolute path is always required. If you use any other protocol, you may not need to specify a remote path if the file resides in the default download folder. For details about how your file server is configured, contact your system administrator.</p>
User field	The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP.
Password field	The password for the remote server username. This field does not apply if the protocol is TFTP.

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

Step 7 Click **OK**.

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

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

What to Do Next

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

Determining the Contents of a Firmware Package

Procedure

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

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

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

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

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

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

Canceling an Image Download

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

Procedure

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

Step 2 Expand the **Equipment** node.

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

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

Verifying Local Storage Space on a Fabric Interconnect

Checking the Available Space on a Fabric Interconnect

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

Procedure

- Step 1** In the **Navigation** pane, click the **Equipment** tab.
 - Step 2** On the **Equipment** tab, expand **Equipment > Fabric Interconnects**.
 - Step 3** Click the fabric interconnect on which you want to check the available space.
 - Step 4** In the **Work** pane, click the **General** tab.
 - Step 5** Expand the **Local Storage Information** area.
When you download a firmware image bundle, a fabric interconnect needs at least twice as much available space as the size of the firmware image bundle. If the bootflash does not have sufficient space, delete the obsolete firmware, core files, and other unneeded objects from the fabric interconnect.
-

Deleting Firmware Images from a Fabric Interconnect

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

Procedure

- Step 1** In the **Navigation** pane, click the **Equipment** tab.
 - Step 2** On the **Equipment** tab, click the **Equipment** node.
 - Step 3** In the **Work** pane, click the **Firmware Management** tab.
 - Step 4** On the **Firmware Management** tab, click the **Images** tab.
 - Step 5** In the table, click the image that you want to delete.
You can use the Shift key or Ctrl key to select multiple entries.
 - Step 6** Right-click the highlighted image or images and choose **Delete**.
 - Step 7** If the Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.
-



Upgrading the Firmware to Release 2.0

This chapter includes the following sections:

- [Summary of Steps for Upgrading from Release 2.0](#), page 31
- [Disabling Call Home](#), page 33
- [Updating the Firmware on the Adapters, BMCs, and IOMs](#), page 33
- [Activating the Firmware on the Adapters and BMCs](#), page 34
- [Activating the Board Controller Firmware on a Server](#), page 35
- [Activating the Cisco UCS Manager Software to Release 2.0](#), page 36
- [Activating the Firmware on the IOMs](#), page 37
- [Activating the Fabric Interconnect Firmware for a Cluster Configuration](#), page 38
- [Activating the Firmware on a Standalone Fabric Interconnect](#), page 43
- [Updating Host and Management Firmware Packages](#), page 44
- [Enabling Call Home](#), page 49

Summary of Steps for Upgrading from Release 2.0



Note

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

The order of steps in this document and the recommended options minimize the disruption to data traffic. Therefore, when you upgrade from any version of Release 2.0, upgrade the components in the following order.

- 1 Complete all prerequisite steps, as described in [Prerequisites for Upgrading and Downgrading Firmware](#), on page 15.
- 2 Obtain the following firmware images from Cisco.com and download them to the fabric interconnect. For more information, see [Downloading the Cisco UCS, Release 2.1 Firmware](#).
 - Cisco UCS Infrastructure Software Bundle—Required for all Cisco UCS domains.

- Cisco UCS B-Series Blade Server Software Bundle—Required for all Cisco UCS domains that include blade servers.
 - Cisco UCS C-Series Rack-Mount UCS-Managed Server Software Bundle—Only required for Cisco UCS domains that include integrated rack-mount servers. This bundle contains firmware to enable Cisco UCS Manager to manage those servers and is not applicable to standalone C-Series rack-mount servers.
- 3 (Optional) Disable Call Home—If the Cisco UCS domain includes Call Home or Smart Call Home, disable Call Home to ensure you do not receive unnecessary alerts when Cisco UCS Manager restarts components.
 - 4 Update adapters, CIMC, and IOMs—If you prefer, you can upgrade the CIMC and the adapters in a host firmware package as part of the last upgrade step. Certain adapters must be upgraded in a host firmware package.
 - 5 Activate adapters—Choose **Ignore Compatibility Check** and **Set Startup Version Only** when performing this step.
 - 6 Activate CIMC—Choose **Ignore Compatibility Check** when performing this step.
 - 7 Activate Cisco UCS Manager—Choose **Ignore Compatibility Check** when performing this step.
 - 8 Activate the I/O modules—Choose **Ignore Compatibility Check** and **Set Startup Version Only** when performing this step.
 - 9 Activate the subordinate fabric interconnect—Choose **Ignore Compatibility Check** when performing this step.
 - 10 To avoid control plane disruption, manually failover the primary fabric interconnect to the fabric interconnect that has already been upgraded.
 - 11 Verify that the data path has been restored.
 - 12 Activate the primary fabric interconnect—Choose **Ignore Compatibility Check** when performing this step.
 - 13 Update management firmware package(s) for servers—You do not need to perform this step if you updated and activated the CIMC on the servers directly.
 - 14 Update host firmware package(s) for servers—Must be the last firmware upgraded. We recommend that you upgrade the board controller firmware during this step to avoid an additional reboot of servers with that firmware. While some of these components can be upgraded directly at the endpoint, such as the BIOS on M3 servers, we recommend that you upgrade the following firmware in a host firmware package:
 - BIOS
 - Storage controller
 - Certain adapters

For information on how to upgrade these endpoints directly, see the [Cisco UCS Manager Configuration Guides](#).

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

Disabling Call Home

This step is optional.

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

Procedure

-
- Step 1** In the **Navigation** pane, click the **Admin** tab.
 - Step 2** On the **Admin** tab, expand **All > Communication Management > Call Home**.
 - Step 3** In the **Work** pane, click the **General** tab.
 - Step 4** In the **Admin** area, click **off** in the **State** field.
Note If this field is set to **off**, Cisco UCS Manager hides the rest of the fields on this tab.
 - Step 5** Click **Save Changes**.
-

Updating the Firmware on the Adapters, BMCs, and IOMs



Caution

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

Procedure

-
- Step 1** In the **Navigation** pane, click the **Equipment** tab.
 - Step 2** On the **Equipment** tab, click the **Equipment** node.
 - Step 3** In the **Work** pane, click the **Firmware Management** tab.
 - Step 4** On the **Installed Firmware** tab, click **Update Firmware**.
 Cisco UCS Manager GUI opens the **Update Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS domain. This step may take a few minutes, depending upon the number of chassis and servers.
 - Step 5** In the **Update Firmware** dialog box, do the following:
 - a) From the **Filter** drop-down list on the menu bar, choose **ALL**.
 If you would prefer to update one type of endpoint at a time, choose that endpoint from the **Filter** drop-down list.
 - b) From the **Set Version** drop-down list on the menu bar, choose the version for the current 2.0 release.

c) Click **OK**.

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

Cisco UCS Manager copies the selected firmware image to the backup memory partition and verifies that the image is not corrupt. The image remains as the backup version until you explicitly activate it. Cisco UCS Manager begins all updates at the same time. However, some updates may complete at different times.

The update is complete when the **Update Firmware** dialog box displays **ready** in the **Update Status** column for all updated endpoints.

Step 6 (Optional) To monitor the progress of the update to a specific endpoint, right-click the endpoint and choose **Show Navigator**.

Cisco UCS Manager displays the progress in the **Update Status** area on the **General** tab. If the navigator has an **FSM** tab, you can also monitor the progress there. An entry in the **Retry #** field may not indicate that the update has failed. The retry count also includes retries that occur when Cisco UCS Manager retrieves the update status.

What to Do Next

Activate the firmware.

Activating the Firmware on the Adapters and BMCs

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



Caution

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

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

Procedure

Step 1 In the **Installed Firmware** tab, choose **Activate Firmware**.

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

- Step 2** If the adapter firmware is not updated through a host firmware package in a service profile, do the following in the **Activate Firmware** dialog box to activate the adapter firmware:
- From the **Filter** drop-down list, choose **Interface Cards**.
 - From the **Set Version** drop-down list, choose the version for the current 2.0 release.
 - Check the **Ignore Compatibility Check** check box.
The firmware for this release is not compatible with previous releases. Therefore, you must check the **Ignore Compatibility Check** check box to ensure that the activation succeeds.
 - Check the **Set Startup Version Only** check box.
Note During a direct upgrade, you should configure **Set Startup Version Only** for an adapter. With this setting, the activated firmware moves into the pending-next-boot state, and the server is not immediately rebooted. The activated firmware does not become the running version of firmware on the adapter until the server is rebooted. You cannot configure **Set Startup Version Only** for an adapter in the host firmware package.
 - Click **Apply**.
When the **Activate Status** column for all adapters displays **pending-next-boot** or **ready**, continue with Step 3.

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 3** If the BMC firmware is not updated through a management firmware package in a service profile, do the following in the **Activate Firmware** dialog box to activate the BMC firmware:
- From the **Filter** drop-down list, choose **BMC**.
 - From the **Set Version** drop-down list, choose the version for the current 2.0 release.
If one or more of the selected endpoints are not configured with the desired version as the backup version, Cisco UCS Manager GUI does not display that version in the **Set Version** drop-down list. You must select the version from the **Startup Version** column for each individual endpoint.
 - Check the **Ignore Compatibility Check** check box.
 - Click **Apply**.
The activation of firmware for a BMC does not disrupt data traffic. However, it will interrupt all KVM sessions, disconnect any vMedia attached to the server, and interrupt all monitoring and IPMI polling.

When the **Activate Status** column for all BMC components displays **ready** continue with Step 4.
- Step 4** Click **OK**.

Activating the Board Controller Firmware on a Server

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

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

**Note**

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

Procedure

-
- Step 1** On the **Installed Firmware** tab, click **Activate Firmware**.
Cisco UCS Manager GUI opens the **Activate Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS domain. This step may take a few minutes, depending upon the number of chassis and servers.
 - Step 2** From the **Filter** drop-down list on the menu bar of the **Activate Firmware** dialog box, select **Board Controller**.
Cisco UCS Manager GUI displays all servers that have board controllers in the **Activate Firmware** dialog box.
 - Step 3** From the **Set Version** drop-down list on the menu bar of the **Activate Firmware** dialog box, choose the version for the current 2.0 release.
 - Step 4** Check the **Ignore Compatibility Check** check box.
 - Step 5** Click **OK**.
-

Activating the Cisco UCS Manager Software to Release 2.0

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

Procedure

-
- Step 1** On the **Installed Firmware** tab, click **Activate Firmware**.
Cisco UCS Manager GUI opens the **Activate Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS domain. This step may take a few minutes, depending upon the number of chassis and servers.
 - Step 2** From the **Filter** drop-down list, choose **UCS Manager**.
 - Step 3** On the **UCS Manager** row of the **Activate Firmware** dialog box, do the following:
 - a) From the drop-down list in the **Startup Version** column, choose the version for the current 2.0 release.
 - b) Check the **Ignore Compatibility Check** check box.
 - Step 4** Click **OK**.
Cisco UCS Manager disconnects all active sessions, logs out all users, and activates the software. When the upgrade is complete, you are prompted to log back in. If you are prompted to re-login immediately after being disconnected, the login will fail. You must wait until the activation of Cisco UCS Manager is completed, which takes a few minutes.

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

Activating the Firmware on the IOMs

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



Caution

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

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

Procedure

- Step 1** In the **Installed Firmware** tab, choose **Activate Firmware**.
If one or more of the selected endpoints are not configured with the desired version as the backup version, Cisco UCS Manager GUI does not display that version in the **Set Version** drop-down list. You must select the version from the **Startup Version** column for each individual endpoint.
- Step 2** To activate the IOM firmware, do the following in the **Activate Firmware** dialog box:
- a) From the **Filter** drop-down list, choose **IO Modules**.
 - b) From the **Set Version** drop-down list, choose the version for the current 2.0 release.
 - c) Check the **Ignore Compatibility Check** check box.
 - d) Check the **Set Startup Version Only** check box.

Important When you configure **Set Startup Version Only** for an I/O module, the I/O module is rebooted when the fabric interconnect in its data path is rebooted. If you do not configure **Set Startup Version Only** for an I/O module, the I/O module reboots and disrupts traffic. In addition, if Cisco UCS Manager detects a protocol and firmware version mismatch between the fabric interconnect and the I/O module, Cisco UCS Manager automatically updates the I/O module with the firmware version that matches the firmware in the fabric interconnect and then activates the firmware and reboots the I/O module again.
 - e) Click **Apply**.
When the **Activate Status** column for all IOMs displays **pending-next-boot**, continue with Step 3.
- Step 3** Click **OK**.

Activating the Fabric Interconnect Firmware for a Cluster Configuration

To minimize the disruption to data traffic, always upgrade the subordinate fabric interconnect and ensure it is up and running before you upgrade the primary fabric interconnect.

Activating the Firmware on a Subordinate Fabric Interconnect

Before You Begin

Determine which fabric interconnect in the cluster is the subordinate fabric interconnect. For more information, see [Verifying the High Availability Status and Roles of a Cluster Configuration](#), on page 18.

Procedure

-
- Step 1** In the **Navigation** pane, click the **Equipment** tab.
- Step 2** On the **Equipment** tab, click the **Equipment** node.
- Step 3** In the **Work** pane, click the **Firmware Management** tab.
- Step 4** On the **Installed Firmware** tab, click **Activate Firmware**.
Cisco UCS Manager GUI opens the **Activate Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS domain. This step may take a few minutes, depending upon the number of chassis and servers.
- Step 5** From the **Filter** drop-down list on the menu bar, choose **Fabric Interconnects**.
- Step 6** On the menu bar, check the **Ignore Compatibility Check** check box.
- Step 7** On the row of the **Activate Firmware** dialog box for the subordinate fabric interconnect, do the following:
- In the **Kernel** row, choose the version for the current 2.0 release from the drop-down list in the **Startup Version** column.
 - In the **System** row, choose the version for the current 2.0 release from the drop-down list in the **Startup Version** column.
- Step 8** Click **Apply**.
Cisco UCS Manager updates and activates the firmware and reboots the fabric interconnect and any I/O module in the data path to that fabric interconnect, disrupting data traffic to and from that fabric interconnect. However, assuming the Cisco UCS domain is configured to permit traffic and port failover, data traffic fails over to the primary fabric interconnect and is not disrupted.
- Step 9** Verify the high availability status of the subordinate fabric interconnect.
- Note** If the **High Availability Details** area for the fabric interconnect does not show the following values, contact Cisco Technical Support immediately. Do not continue to update the primary fabric interconnect.

Field Name	Required Value
Ready field	Yes
State field	Up

What to Do Next

Force a fabric interconnect switchover to make this into the primary fabric interconnect. Then log into the new subordinate fabric interconnect (formerly the primary fabric interconnect) and verify that the data path is ready and has returned to normal operation. If the data path is not ready and the servers have not failed back over to the subordinate fabric interconnect, data traffic may be disrupted when you activate the primary fabric interconnect.

If the high availability status of the subordinate fabric interconnect contains the required values and the data path has returned to normal operation, activate the former primary fabric interconnect.

Forcing a Fabric Interconnect Failover

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

You must force the failover from the primary fabric interconnect.

Procedure

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

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

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

A: UP, PRIMARY
B: UP, SUBORDINATE

HA READY
UCS-A# connect local-mgmt
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2011, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
```

the GNU General Public License (GPL) version 2.0 or the GNU Lesser General Public License (LGPL) Version 2.1. A copy of each such license is available at <http://www.opensource.org/licenses/gpl-2.0.php> and <http://www.opensource.org/licenses/lgpl-2.1.php>

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

Verifying that the Data Path is Ready

This chapter includes the following sections:

Verifying that Dynamic vNICs Are Up and Running

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

Perform this step in the Cisco UCS Manager GUI.

Procedure

-
- Step 1** In the **Navigation** pane, click the **VM** tab.
 - Step 2** On the **VM** tab, expand **All > VMware > Virtual Machines**.
 - Step 3** Expand the virtual machine for which you want to verify the dynamic vNICs and choose a dynamic vNIC.
 - Step 4** In the **Work** pane, click the **VIF** tab.
 - Step 5** On the **VIF** tab, verify that the **Status** column for each VIF is **Online**.
 - Step 6** Repeat Steps 3 through 5 until you have verified that the VIFs for all dynamic vNICs on all virtual machines have a status of **Online**.
-

Verifying the Ethernet Data Path

Procedure

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

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

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

Verifying the Data Path for Fibre Channel 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.

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
INTERFACE VSAN FCID                PORT NAME                NODE NAME                EXTERNAL
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 -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.

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

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

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

Activating the Firmware on a Primary Fabric Interconnect

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



Note

If you have followed the entire procedure to activate the fabric interconnects in a cluster configuration, the former primary fabric interconnect is now the subordinate fabric interconnect.

Before You Begin

Activate the subordinate fabric interconnect, force a fabric interconnect switchover, and verify that the data path is up and running.

Procedure

- Step 1** On the **Installed Firmware** tab, click **Activate Firmware**.
Cisco UCS Manager GUI opens the **Activate Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS domain. This step may take a few minutes, depending upon the number of chassis and servers.
- Step 2** From the **Filter** drop-down list on the menu bar, choose **Fabric Interconnects**.
- Step 3** On the menu bar, check the **Ignore Compatibility Check** check box.
- Step 4** On the row of the **Activate Firmware** dialog box for the (former) primary fabric interconnect, do the following:
- In the **Kernel** row, choose the version for the current 2.0 release from the drop-down list in the **Startup Version** column.
 - In the **System** row, choose the version for the current 2.0 release from the drop-down list in the **Startup Version** column.
- Step 5** Click **Apply**.
Cisco UCS Manager updates and activates the firmware and reboots the fabric interconnect and any I/O module in the data path to that fabric interconnect, disrupting data traffic to and from that fabric interconnect. However, assuming the Cisco UCS domain is configured to permit traffic and port failover, data traffic fails over to the other fabric interconnect, which becomes the primary. When it comes back up, this fabric interconnect is the subordinate fabric interconnect.
- Step 6** Verify the high availability status of the fabric interconnect.
- Note** If the **High Availability Details** area for the fabric interconnect does not show the following values, contact Cisco Technical Support immediately.

Field Name	Required Value
Ready field	Yes
State field	Up

Activating the Firmware on a Standalone Fabric Interconnect

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

Procedure

- Step 1** In the **Navigation** pane, click the **Equipment** tab.
- Step 2** On the **Equipment** tab, click the **Equipment** node.
- Step 3** In the **Work** pane, click the **Firmware Management** tab.
- Step 4** On the **Installed Firmware** tab, click **Activate Firmware**.
Cisco UCS Manager GUI opens the **Activate Firmware** dialog box and verifies the firmware versions for all endpoints in the Cisco UCS domain. This step may take a few minutes, depending upon the number of chassis and servers.
- Step 5** From the **Filter** drop-down list, choose **Fabric Interconnects**.
- Step 6** On the menu bar, check the **Ignore Compatibility Check** check box.
- Step 7** On the row of the **Activate Firmware** dialog box for the fabric interconnect, do the following:
- a) In the **Kernel** row, choose the version for the current 2.0 release from the drop-down list in the **Startup Version** column.
 - b) In the **System** row, choose the version for the current 2.0 release from the drop-down list in the **Startup Version** column.
- Step 8** Click **OK**.
-

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

Updating Host and Management Firmware Packages

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
<p>Firmware package is not included in a service profile or an updating service profile template.</p> <p>OR</p> <p>You want to upgrade the firmware without making any changes to the existing service profile or updating service profile template.</p>	<p>No maintenance policy</p>	<p>After you update the firmware package, do one of the following:</p> <ul style="list-style-type: none"> • 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: <ol style="list-style-type: none"> 1 Create a new service profile and include the firmware package in that service profile. 2 Dissociate the server from its service profile. 3 Associate the server with the new service profile. 4 After the server has been rebooted and the firmware upgraded, disassociate the server from the new service profile and associate it with its original service profile. <p>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.</p>
<p>The firmware package is included in one or more service profiles, and the service profiles are associated with one or more servers.</p> <p>OR</p> <p>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.</p>	<p>No maintenance policy</p> <p>OR</p> <p>A maintenance policy configured for immediate updates.</p>	<p>The following occurs when you update the firmware package:</p> <ol style="list-style-type: none"> 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. <p>All servers associated with service profiles that include the firmware package are rebooted at the same time.</p>

Service Profile	Maintenance Policy	Upgrade Actions
<p>The firmware package is included in one or more service profiles, and the service profiles are associated with one or more servers.</p> <p>OR</p> <p>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.</p>	<p>Configured for user acknowledgment</p>	<p>The following occurs when you update the firmware package:</p> <ol style="list-style-type: none"> 1 Cisco UCS asks you to confirm your change and advises that a user-acknowledged reboot of the servers is required. 2 Click the flashing Pending Activities button to select the servers you want to reboot and apply the new firmware. 3 Cisco UCS verifies the model numbers and vendor against all servers associated with service profiles that include this policy. If the model numbers and vendor match a firmware version in the policy, Cisco UCS reboots the server and updates the firmware. <p>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.</p>
<p>The firmware package is included in one or more service profiles, and the service profiles are associated with one or more servers.</p> <p>OR</p> <p>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.</p>	<p>Configured for changes to take effect during a specific maintenance window.</p>	<p>The following occurs when you update the firmware package:</p> <ol style="list-style-type: none"> 1 Cisco UCS asks you to confirm your change and advises that a user-acknowledged reboot of the servers is required. 2 Click the flashing Pending Activities button to select the servers you want to reboot and apply the new firmware. 3 Cisco UCS verifies the model numbers and vendor against all servers associated with service profiles that include this policy. If the model numbers and vendor match a firmware version in the policy, Cisco UCS reboots the server and updates the firmware. <p>A manual reboot of the servers does not cause Cisco UCS to apply the firmware package, nor does it cancel the scheduled maintenance activities.</p>

Updating a Management Firmware Package

If the policy is included in one or more service profiles associated with a server and those service profiles do not include maintenance policies, Cisco UCS Manager updates and activates the management firmware in

the server with the new versions and reboots the server as soon as you save the management firmware package policy unless you have configured and scheduled a maintenance window.

Before You Begin

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

Procedure

-
- Step 1** In the **Navigation** pane, click the **Servers** tab.
- Step 2** On the **Servers** tab, expand **Servers > Policies**.
- Step 3** Expand the node for the organization that includes the policy you want to update. If the system does not include multitenancy, expand the **root** node.
- Step 4** Expand **Management Firmware Packages** and choose the policy you want to update.
- Step 5** In the **Work** pane, click the **General** tab.
- Step 6** In the table on the right, do the following to delete the existing entry for the firmware you want to update:
- Select the line in the table for the firmware version that you want to change.
 - Right-click and select **Delete**.
 - Click **Yes** to confirm that you want to delete that entry.
- Step 7** In the **BMC Firmware Packages** section on the left:
- Click the down arrows to expand the section.
By default, the entries in a section are sorted by vendor name. To sort the entries, click on a column heading.
 - Select the line in the table which lists the firmware version for the release that you want to add to the firmware package.
The firmware version must match the model numbers (PID) on the servers that are associated with the firmware package . If you select a firmware version with the wrong model number, Cisco UCS Manager cannot install the firmware update.
 - Drag the line to the table on the right.
 - Click **Yes** to confirm that you selected the correct version.
- Step 8** If you need to include BMC firmware for servers with different model numbers (PIDs) in this management firmware package, repeat Step 6.
- Step 9** Click **Save Changes**.
Cisco UCS Manager verifies the model numbers and vendor against all servers associated with service profiles that include this policy. If the model numbers and vendor match a firmware version in the policy, Cisco UCS Manager updates the firmware according to the settings in the maintenance policies included in the service profiles.
-

Updating a Host Firmware Package

You must upgrade the BIOS and storage controller firmware through the host firmware package when you upgrade to Release 2.0. If you do not upgrade those packages, the servers may experience communication issues with Cisco UCS Manager and the BMC.

**Caution**

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

This procedure assumes that the host firmware package already exists. For information on how to create a host firmware package, see *Cisco UCS Manager GUI Configuration Guide* or *Cisco UCS Manager CLI Configuration Guide*.

Before You Begin

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

- Upgrade Cisco UCS Manager and the fabric interconnects
- Determine an appropriate maintenance window to reduce the impact of the disruption of data traffic when the server reboots
- Ensure you know the 2.0 firmware version and model number (PID) for the servers or servers

Procedure

-
- Step 1** In the **Navigation** pane, click the **Servers** tab.
- Step 2** On the **Servers** tab, expand **Servers > Policies**.
- Step 3** Expand the node for the organization that includes the policy you want to update. If the system does not include multitenancy, expand the **root** node.
- Step 4** Expand **Host Firmware Packages** and select the policy you want to update.
- Step 5** In the **Work** pane, click the **General** tab.
- Step 6** In the table on the right, do the following to delete the existing entry for the firmware you want to update:
- a) Select the line in the table for the firmware version that you want to change.
 - b) Right-click and select **Delete**.
 - c) Click **Yes** to confirm that you want to delete that entry.
- Step 7** On the **General** tab, click the down arrows to expand one or more of the following sections on the left:
- **Adapter Firmware Packages**
 - **Storage Controller Firmware Packages**
 - **Fibre Channel Adapters Firmware Packages**
 - **BIOS Firmware Packages**
 - **HBA Option ROM Packages**
- Step 8** In each section for the endpoint to which you want to include firmware in the package:
- a) Select the line in the table for the firmware version that you want to add to the pack. By default, the entries are sorted by vendor name. To sort the entries, click on a column heading.
 - b) Drag the line to the table on the right.

The model and model number (PID) must match the servers that are associated with this firmware package. If you select the wrong model or model number, Cisco UCS Manager cannot install the firmware update.

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

Step 9 If you need to include firmware updates for servers with different model numbers (PIDs) in this management firmware package, repeat Steps 6 and 7.

Step 10 Click **Save Changes**.

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

What to Do Next

Verify that the firmware on the endpoints included in the host firmware package has been updated to release 2.0. If the firmware has not been updated, check the model numbers and vendors in the host firmware package against those on the endpoints that were not updated.

Enabling Call Home

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

Procedure

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

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

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

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

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

Step 5 Click **Save Changes**.

What to Do Next

Ensure that Call Home is fully configured.



PART **II**

Hardware Upgrades

- [Upgrading Cisco UCS Hardware, page 53](#)



Upgrading Cisco UCS Hardware

This chapter includes the following sections:

- [Upgrading Fabric Interconnects, page 53](#)
- [Upgrading I/O Modules, page 63](#)
- [Upgrading Adapter Cards, page 66](#)
- [Upgrading Integrated Rack-Mount Servers, page 68](#)

Upgrading Fabric Interconnects

Fabric Interconnect Upgrade Considerations

Be sure the following prerequisites are met before beginning any procedures in this section:

**Caution**

All software and firmware on all components must be upgraded to the latest software release and build available before attempting an upgrade. Cisco UCS software version 2.0 is the bare minimum version for the Cisco UCS 6248 UP. The new Cisco UCS 6200 series fabric interconnects must be loaded with the same build version that is on the Cisco UCS 6100 series fabric interconnect it will replace.

**Caution**

If you intend to implement the fabric port channel feature after you upgrade the hardware, you may need to rearrange the cabling between the FEX and the fabric interconnect before you configure this feature. A fabric port channel requires that all physical links from a given FEX physically connect to a contiguous block of ports (1 to 8 or 9 to 16, and so on), and that a Cisco UCS 2200 Series FEX is connected to a Cisco UCS 6200 Series fabric interconnect.

- Licenses from Cisco UCS 6100 series fabric interconnects are not transferable to Cisco UCS 6200 series fabric interconnects. You must obtain licenses for the Cisco UCS 6200 series fabric interconnects before you upgrade.
- Upgrading the fabric interconnect should be done before upgrading to a new FEX or virtual interface card.

- Do not attempt to implement new software features from the new Cisco UCS software version until all required hardware is installed.
- Changes to the topology, such as the number of servers or uplink connections, should be performed after the fabric interconnect upgrade is complete.
- Make a detailed record of the cabling between FEXes and fabric interconnects using the provided table. You must preserve the physical port mapping to maintain the server pinning already configured and minimize down time. See [Table 1: Fabric Interconnect Port Connection Record](#), on page 59.
- For a cluster configuration, both fabric interconnects must have symmetrical connection topologies between fabric interconnect and FEXes.
- Standalone installations should expect down time. Upgrading a fabric interconnect is inherently traffic disruptive.
- A best practice would be to perform a full configuration and software backup before performing this hardware upgrade.

Port Mapping for Upgrades

The upgrade described here is primarily for upgrading a Cisco UCS 6120 fabric interconnect to a Cisco UCS 6248. If you have a Cisco UCS 6140 fabric interconnect that has 48 or less physical ports connected, you will also be able to utilize these steps, the same principles will apply though you will have to manually map any ports connected to slot 3 on a UCS 6140 as the UCS 6248 has no slot 3. The same considerations will also apply when upgrading a Cisco UCS 6140 fabric interconnect to a Cisco UCS 6296, though as the 6296 has enough slots that no manual re-mapping will be necessary.

Fixed Ports

On the UCS 6120 fabric interconnect, the fixed ports on slot 1 are all ethernet ports, which might be further configured as Server ports or uplink Ethernet ports. On the UCS 6248 fabric interconnect, you can separate the 32 physical ports in slot one into two contiguous pools, low numbered ports being Ethernet ports and high numbered ports being Fibre Channel ports. When upgrading to a UCS 6248, the UCS 6120 port mappings can be directly carried over on fixed ports with no reconfiguration required. When upgrading a UCS 6140 to a UCS 6296, the port mappings can be directly carried over on fixed ports with no reconfiguration required.



Note

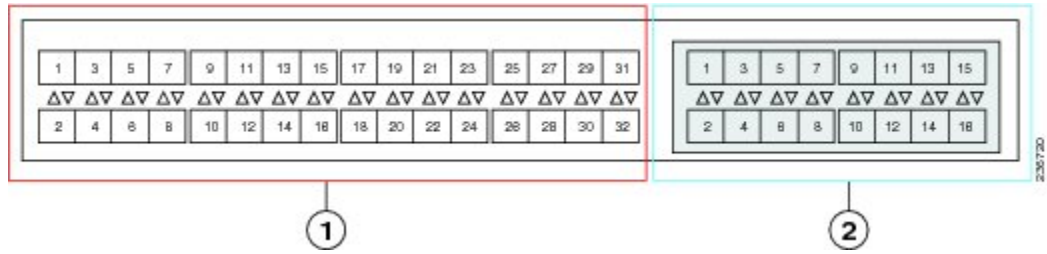
Since a UCS 6140 has 40 ports on slot 1 and a UCS 6248 has 32 ports, any ports currently configured on ports 1/33 to 1/40 of the UCS 6140 will have to be moved during the upgrade process.



Caution

If you ever need to change the pool sizes for slot 1 this will require a reboot of the fabric interconnect which can lead to a service disruption. If you ever need to change the pool sizes for slot 2 this will require a reset of the expansion module in slot 2. To minimize disruption, plan to have at least a few Ethernet uplink and Fibre Channel uplink ports configured on Slot 1. Implement this fail safe after the upgrade is complete and the system re-stabilizes.

Figure 1: Cisco UCS 6248 Port Numbering



1	Slot 1, 32 fixed universal ports	2	Slot 1, 16 expansion universal ports
---	----------------------------------	---	--------------------------------------

Expansion Ports

On the UCS 6120 fabric interconnect, the expansion slot port types depend on which of four possible expansion modules are installed. On the UCS 6248 fabric interconnect, you can separate the 16 physical ports in an expansion slot into two pools, low numbered ports being Ethernet ports and high numbered ports being Fibre Channel, see [the Cisco UCS Manager configuration guides](#). When upgrading to a UCS 6248 or UCS 6296, you may need to pre-plan and re-configure expansion module port mappings before powering up the new interconnect.



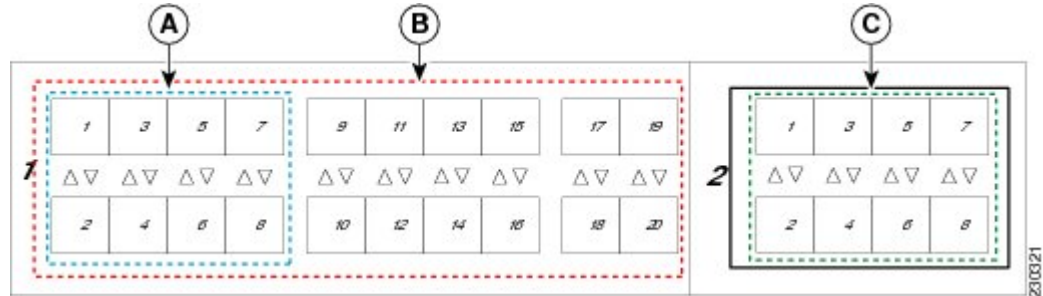
Note

Any expansion ports in slot 3 of a UCS 6140 fabric interconnect will need to have their configuration deleted and their use re-mapped to ports on slots 1 or 2 of the new UCS 6248. Upgrading a UCS 6140 to a UCS 6296 is the preferred path as this manual re-mapping will not be necessary.

- If you have an N10-E0080 or N10-E0060 Fibre channel expansion module in your UCS 6120, the existing fibre channel configurations can simply carry over to the new UCS 6248, though this may not

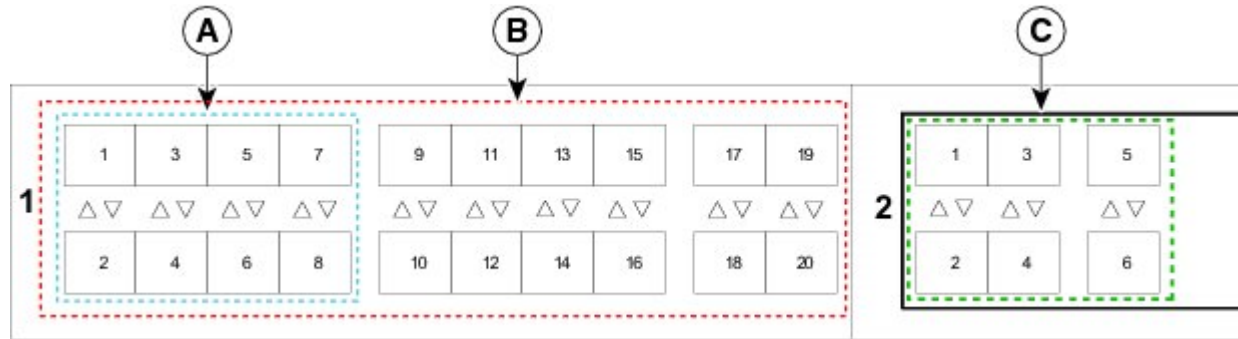
be appropriate for all situations as it will mean that all ports in slot two are fibre channel. If you want to reconfigure ports 2/1 to 2/8 to use ports 2/9 to 2/16, do so after the upgrade is completed.

Figure 2: Cisco UCS 6120 Port Numbering when Configured with the N10-E0080 Expansion Module



A	Slot 1, ports 1 through 8: 10-Gigabit or 1 Gigabit Ethernet capable ports	C	Slot 2 Fibre Channel ports 1 through 8
B	Slot 1, ports 1 through 20: 10-Gigabit Ethernet ports		

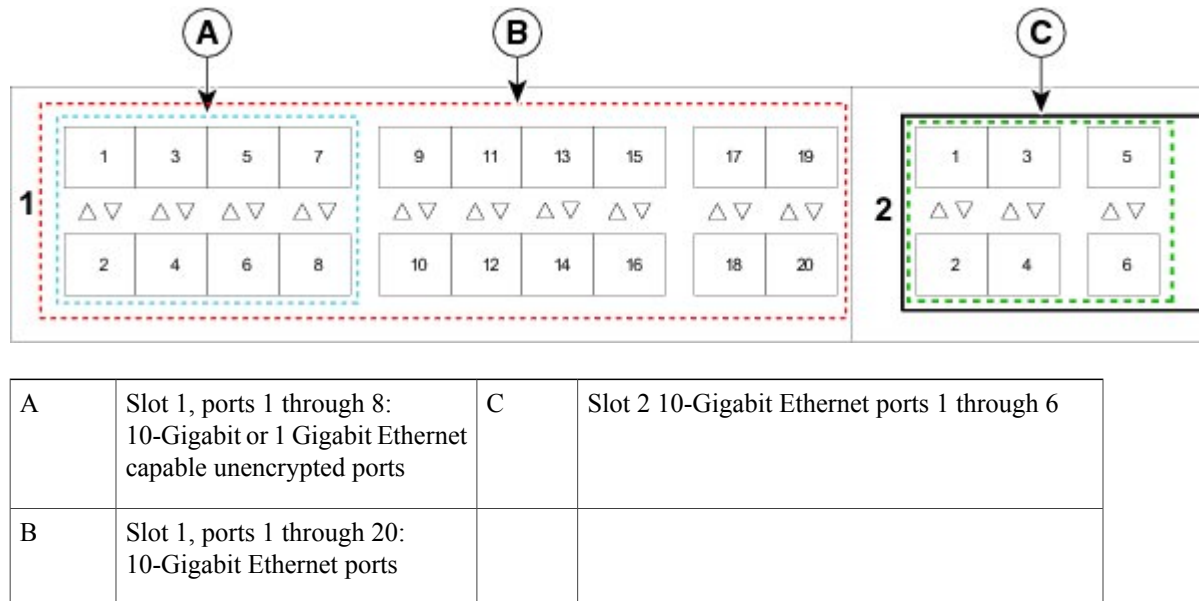
Figure 3: Cisco UCS 6120 Port Numbering when Configured with the N10-E0060 Expansion Module



A	Slot 1, ports 1 through 8: 10-Gigabit or 1 Gigabit Ethernet capable ports	C	Slot 2 Fibre Channel ports 1 through 6
B	Slot 1, ports 1 through 20: 10-Gigabit Ethernet ports		

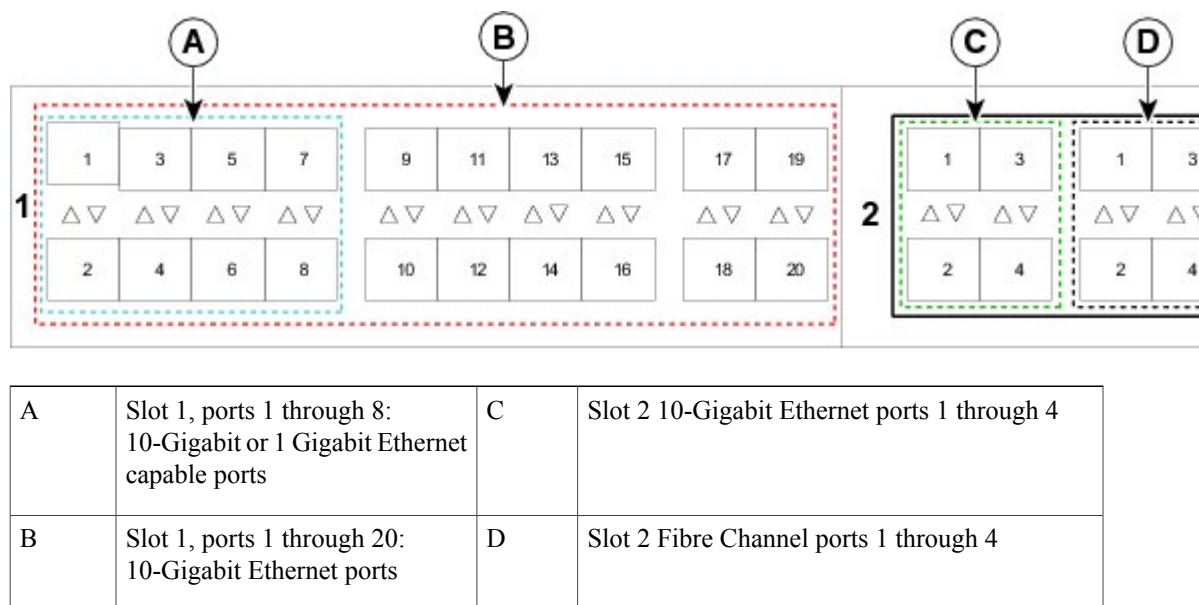
- If you have an N10-E0600 Fibre channel expansion module in your UCS 6120, the existing Ethernet configurations can simply carry over to the UCS 6248, with ports 2/7 to 2/16 potentially configurable for either Ethernet or FC.

Figure 4: Cisco UCS 6120 Port Numbering when Configured with the N10-E0600 Expansion Module



- If you have an N10-E0440 expansion module in your UCS 6120, the simplest direct mapping would be to allow Ethernet ports 2/1 to 2/4 on the UCS 6248 to carry over, then remap the fibre channel ports to new port numbers on either slot 1 or slot 2.

Figure 5: Cisco UCS 6120 Port Numbering when Configured with the N10-E0440 Expansion Module



Fabric Interconnect Port Connection Record

Table 1: Fabric Interconnect Port Connection Record

Fabric Interconnect A/B		Connected to					
Slot	Port	Chassis	IOM	Port	LAN or SAN Pin Group	Port Channel Group	Connection Notes
1	1						
	2						
	3						
	4						
	5						
	6						
	7						
	8						
	9						
	10						
	11						
	12						
	13						
	14						
	15						
	16						
	17						
	18						
	19						

Fabric Interconnect A/B		Connected to					
Slot	Port	Chassis	IOM	Port	LAN or SAN Pin Group	Port Channel Group	Connection Notes
	20						
	21						
	22						
	23						
	24						
	25						
	26						
	27						
	28						
	29						
	30						
	31						
	32						

Fabric Interconnect A/B		Connected to					
Slot	Port	Chassis	IOM	Port	LAN or SAN Pin Group	Port Channel Group	Connection Notes
2	1						
	2						
	3						
	4						
	5						
	6						
	7						
	8						
	9						
	10						
	11						
	12						
	13						
	14						
	15						
	16						

Upgrading a Fabric Interconnect Cluster



Caution

If your UCS 6120 fabric interconnect uses a N10-E0440 expansion module, or if you are migrating a UCS 6140 with an expansion module in slot 3 to a UCS 6248, pre-plan their deletion and re-mapping following the guidelines in the previous section on port maps.

Unless otherwise noted, for more information about how to perform configuration procedures in Cisco UCS Manager for a particular step, see the [Cisco UCS Manager configuration guide](#) for the appropriate release.

Procedure

-
- Step 1** Mount the replacement fabric interconnects into either the same rack or an adjacent rack. Refer to the Cisco UCS 6200 Series Installation Guide for details.
- Step 2** Using either the UCS manager CLI or GUI, verify the state (subordinate or active) of the fabric interconnects. See http://www.cisco.com/en/us/docs/unified_computing/ucs/sw/upgrading/from1.4/to2.0/b_upgradingciscoucsfrom1.4to2.0_chapter_0101.html.
- Step 3** Back up the software configuration information and the UCS Manager software.
- Step 4** Disable the server ports on the subordinate fabric interconnect.
- Step 5** Power down the subordinate fabric interconnect by unplugging it from the power source. If you are monitoring the upgrade using a KVM session, you may need to reconnect the KVM session when you power down the fabric interconnect.
- Step 6** Disconnect the cables from the chassis IO Modules or fabric extenders to the subordinate fabric interconnect ports in slot 1 on the old fabric interconnect.
- Step 7** Connect these cables into the corresponding ports on slot 1 of one of the new Cisco UCS 6248 UP fabric interconnects, using the connection records to preserve the port mapping and the configured server pinning. See [Fabric Interconnect Port Connection Record](#), on page 59. See [Fabric Interconnect Upgrade Considerations](#), on page 53.
- Step 8** Disconnect the L1/L2, M1 management, and Console cables on the old fabric interconnect. The ports for these connections are on the opposite side of the interconnect, so if your cables are just barely long enough to connect two rack-adjacent UCS 6120 interconnects you will probably need new cables.
- Step 9** Connect the M1 management, and Console cables to the new Cisco UCS 6248 UP.
- Step 10** Connect the L1/L2 cables that were disconnected onto the new Cisco UCS 6248 UP. L1 connects to L1, L2 connects to L2.
- Step 11** Disconnect the Ethernet or FC cables from slot 2 of the old fabric interconnect.
- Step 12** Connect the Ethernet or FC cables to the corresponding ports in slot 2 of the new Cisco UCS 6248 UP. Some may go to slot 1, depending on the mappings planned out earlier in the process.
- Step 13** Connect the power to the new Cisco UCS 6248 UP, it will automatically boot and run POST tests. If it reboots itself, this is a normal behavior.
- Important** [Directly connect the console port to a terminal](#) and observe the boot sequence. You should at some point see the Basic System Configuration Dialog, where you will configure the switch as a subordinate interconnect. If you do not see this dialog, you either have different builds of software on your old primary and new subordinate, or the new subordinate has previously been part of a cluster and will need to have all configuration information wiped before it can be added to a cluster as a subordinate. In either case, immediately disconnect the L1 and L2 connections and complete the bringup as a standalone fabric interconnect, then correct the issue before proceeding further.
- Step 14** (Optional) Remap UCS 6100 fabric interconnect FC ports 2/1 to 2/4 on a N10-E0440 expansion module or any slot 3 ports onto the new fabric interconnect expansion module.

- a) Use UCS Manager to delete the ports on the subordinate fabric interconnect that you will need to move within the configuration.
- b) For each port you have just deleted, create new ports on either slot 1 or slot 2. These ports must use the same port type definitions as the old ports, but will use different port numbers.
- c) For recently moved Ethernet server ports, reconfigure the associated service profile to use the new port number for the appropriate LAN pin group.
- d) For recently moved uplink Ethernet ports, reconfigure the port channel settings to use the new ports.
- e) For recently moved uplink FC ports, reconfigure the associated service profile SAN pin group to use the new ports.
- f) Re-acknowledge chassis for blade servers and fabric extender for rack servers.
This will be disruptive to traffic, but is necessary in this specific scenario.

Step 15 The new subordinate fabric interconnect will automatically synchronize the configuration and database/state information from the primary fabric interconnect.
Synchronization between primary and subordinate fabric interconnects can take several minutes. You may see an error message that will persist until the server ports are enabled.

The port configuration is copied from the subordinate switch to the new hardware.

Step 16 Verify that the data path is ready.
See http://www.cisco.com/en/us/docs/unified_computing/ucs/sw/upgrading/from1.4/to2.0/b_upgradingciscoucsfrom1.4to2.0_chapter_0100.html.

Make sure all faults are resolved before proceeding.

- a) Verify and if necessary reconfigure the SAN pin group for FC ports in the associated service profile.
- b) Verify and if necessary reconfigure the LAN pin group for Ethernet ports in the associated service profile.
- c) Verify and if necessary reconfigure the port channel for uplink Ethernet ports.

Step 17 Enable the server ports that had been disabled in Step 4.

- a) If you have changed port mappings, you may need to reacknowledge the chassis or rack server connected to the subordinate fabric interconnect.
- b) Verify and if necessary reconfigure Ethernet ports as server ports.

Step 18 Promote the subordinate fabric interconnect to active, and repeat the process on the second Cisco UCS 6248 UP.

Cable the second new fabric interconnect identically to the first, and allow the reconfiguration done to be applied to the second new fabric interconnect as well.

See http://www.cisco.com/en/us/docs/unified_computing/ucs/sw/upgrading/from1.4/to2.0/b_upgradingciscoucsfrom1.4to2.0_chapter_0100.html.

Upgrading I/O Modules

I/O Module Upgrade Considerations

Be sure the following prerequisites are met before beginning any procedures in this section:

All software and firmware on all components must be upgraded to the same software release available before attempting an upgrade. This release must support the hardware you will be adding. UCS software version

2.0(1) is the bare minimum version for the UCS 2208XP I/O Module. UCS software version 2.0(2) is the bare minimum version for the UCS 2204XP I/O Module.

- Do not attempt to implement new software features from the new UCS software version until all required hardware is installed.
- Make a detailed record of the cabling between I/O Modules and fabric interconnects. You will need to preserve the physical port mapping to maintain the server pinning already configured and minimize down time.
- For a cluster configuration, both fabric interconnects must have symmetrical connection topologies between fabric interconnect and I/O module.
- Standalone installations should expect down time. Upgrading an I/O module will be inherently traffic disruptive.
- When performing hardware upgrades to implement features new to UCS software version 2.0, upgrade the fabric interconnect, then the I/O module, then the adapter in the blade server.
- Cisco I/O modules only support one, two, four, and (UCS 2208 only) eight link topologies between I/O module and fabric interconnect. If there is a link failure on one of the links, UCS falls back to the next largest possible topology with regards to blade to fabric port mapping. If this ever happens, re-acknowledge the chassis, and manually re-map the fabric ports. It is recommended during the replacement of a fabric interconnect that you have all ports connected to the fabric interconnect before the configuration sync.
- A best practice would be to perform a full configuration and database/state information backup before performing this hardware upgrade.
- If you intend to implement the fabric port channel feature available in UCS software version 2.0, you may need to rearrange the cabling between I/O module and fabric interconnect before performing the feature configuration. Fabric port channel will require that all physical links from a given I/O module physically connect to a contiguous block of ports (1-8 or 9-16, and so on). This feature requires a UCS 2200 Series I/O Module connecting to a UCS 6200 Series Fabric Interconnect. See the [Cisco UCS Manager configuration guides](#).

I/O Module Port Connection Record

Table 2: I/O Module Port Connection Record

I/O Module		Connected to			
Number	Port	Fabric Interconnect A or B	Slot	Port	Connection Notes
1	1				
	2				
	3				
	4				
	5				
	6				
	7				
	8				
2	1				
	2				
	3				
	4				
	5				
	6				
	7				
	8				

Upgrading an I/O Module

Procedure

- Step 1** Connect to the cluster's fabric interconnect, and verify the state (subordinate or active) of the fabric interconnects.
- Step 2** Make a detailed record of the port mapping of the connections between the fabric interconnects and the I/O modules.
- Step 3** Disconnect the 10GbE cables connecting the chassis I/O module to the subordinate fabric interconnect on the I/O module side.
- Step 4** Loosen the captive screws on the old I/O module's levers.
- Step 5** Pull the levers outward to unseat the old I/O module.
- Step 6** Make sure that the two levers at the front of the new I/O module are pulled open.
- Step 7** Slide the new I/O module into the I/O module slot, ensuring that the new I/O module is fully seated.
- Step 8** Close the levers and tighten the captive screw on each lever.
- Step 9** Connect the 10GbE cables into the appropriate ports on the new Cisco UCS 2208UP I/O Module or Cisco UCS 2204UP I/O Module, using the connection records to preserve the port mapping and the configured server pinning.
- Step 10** If you have changed port mappings, you may need to reacknowledge the I/O Module, fabric extender, or rack server connected to the subordinate fabric interconnect. This action will only be necessary if you have changed port mappings, but it will be disruptive if it is needed. See the [Cisco UCS Manager configuration guides](#).
- Step 11** Promote the subordinate fabric interconnect to active, and repeat steps 2 to 9 on the second Cisco UCS 2208 UP or Cisco UCS 2204UP I/O Module. It may take 5-15 minutes for all error indications to clear on the GUI, and for the service profiles on the servers in the chassis to come up.
-

Upgrading Adapter Cards

Adapter Card Upgrade Considerations

Be sure the following prerequisites are met before beginning any procedures in this section.

All software and firmware on all components must be upgraded to the latest software release available before attempting an upgrade. UCS software version 2.0(1) is the bare minimum version for the Cisco UCS 6248 UP, the UCS 2208 IO Module, and the Cisco UCS Virtual Interface Card 1280. UCS software version 2.0(2) is the bare minimum version for the Cisco UCS 6296 UP and the UCS 2204 IO Module.

- Do not attempt to implement new software features from the new UCS software version until all required hardware is installed.
- You will be able to physically install a Cisco UCS Virtual Interface Card 1280 without first installing a UCS 2208 I/O Module or UCS 2204 I/O Module and additional connections to a fabric interconnect,

but to do so would not allow you to take full advantage of the additional performance the Cisco UCS Virtual Interface Card 1280 provides compared to the UCS M81KR. The preferred order is to upgrade the Fabric interconnect, then the I/O Module, and finally the Cisco UCS Virtual Interface Card 1280.

- Blade servers allowing more than one Adapter Card may mix the Cisco UCS Virtual Interface Card 1280 with the UCS M81KR, the M72KR-E, or the M72KR-Q. Dual Cisco UCS Virtual Interface Card 1280 adapters are also supported.
- A best practice would be to perform a full configuration and software backup before performing this hardware upgrade.
- If you intend to implement the fabric port channel feature available in UCS software version 2.0, you may need to rearrange the cabling between IOM and Fabric Interconnect before performing the feature configuration. Fabric port channel will require that all physical links from a given I/O module physically connect to a contiguous block of ports (1-8 or 9-16, and so on). This feature requires a UCS 2200 Series I/O Module connecting to a UCS 6200 Series Fabric Interconnect. See the [Fabric Port Channel](#) sections in the configuration guides for more details.

Upgrading an Adapter Card

Procedure

-
- Step 1** Use the locator button in the UCS Manager GUI to confirm which server you are upgrading.
- Step 2** Decommission and remove the blade server using the adapter you wish to upgrade.
- Decommission the server as described in [Decommissioning the Server](#) or by using the power button on the front panel.
 - Completely loosen the captive screws on the front of the blade.
 - Remove the blade from the chassis by pulling the ejector levers on the blade until it unseats the extended memory blade server.
 - Slide the blade part of the way out of the chassis, and place your other hand under the blade to support its weight.
 - Once removed, place the blade on an antistatic mat or antistatic foam if you are not immediately reinstalling it into another slot.
- Step 3** Remove the top cover and remove the old Adapter Card.
- Press and hold the button down.
 - (Most models) Press and hold the top cover release button down. While holding the back end of the cover, pull the cover back and then up.
 - (B230) Press and hold the top cover release button down. While holding the back end of the cover, pull the cover forward. The face plate is meant to be removed along with the top cover.
 - Loosen the three captive screws attaching the Adapter Card to the motherboard. Remove the adapter connector from the motherboard connector and pull straight up. Be careful not to damage the connectors.
 - Remove the adapter connector from the motherboard connector and pull straight up. Be careful not to damage the connectors. You may need to gently rock the card from side to side to get the connector to unseat.
- Step 4** Install the new Adapter card.
- Position the adapter board connector above the mother board connector and align the three adapter captive screws to the posts on the motherboard.

- b) Firmly press the adapter connector into the motherboard connector. If the seating is bad, it may cause the network connection LED to stay amber when the server is restarted.
- c) Tighten the three captive screws.

Step 5 Replace the top cover and reinsert the blade server in the chassis.

Step 6 Recommission the server by [reacknowledging the server slot](#).

Step 7 When upgrading a Virtual Interface Card, configurations created for the older card will carry over to the new hardware. Additional configuration is now possible, but no re-configuration is required.

Upgrading Integrated Rack-Mount Servers

Required Order of Steps for Integrating Cisco UCS Rack-Mount Servers

After you upgrade the firmware for the existing components, you can integrate one or more Cisco UCS rack-mount servers. When you integrate rack-mount servers, you must perform the steps in the following order:

- 1 If you have not already done so, configure the rack server discovery policy in Cisco UCS Manager.
- 2 Follow the instructions in the appropriate [rack-mount server installation guide](#) for installing and integrating a rack-mount server in a system managed by Cisco UCS Manager.
- 3 Wait for Cisco UCS Manager to discover the new server. If server discovery does not begin within a few minutes, acknowledge the server.

Upgrades of Integrated Rack-Mount Servers

Cisco UCS, Release 2.0(2) does not support integration with rack-mount servers through Cisco Nexus 2248 FEXes. If you upgrade a Cisco UCS domain that includes integrated rack-mount servers to Release 2.0(2) or later, you must to upgrade your setup to include Cisco Nexus 2232 FEXes.

For more information, see the appropriate [rack-mount server installation guide](#) for migrating a rack-mount server integration to Cisco UCS, Release 2.0(2).