Cisco Host Upgrade Utility 2.0(6) User Guide

First Published: 2015-06-06

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

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

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

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

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

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

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

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)

© 2015 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface

Preface v

Audience v

Conventions v

Related Cisco UCS Documentation vii

CHAPTER 1

Overview of Cisco Host Upgrade Utility 1

About the Cisco Host Upgrade Utility 1

License Agreement 5

Understanding the HUU User Interface 5

CHAPTER 2

Requirements and Support 7

Requirements 7

Support 8

CHAPTER 3

Updating the Firmware on Cisco UCS C-Series Servers 9

Upgrading the Firmware on a Cisco UCS C-Series Server Using the HUU 9

CHAPTER 4

Troubleshooting 13

Troubleshooting 13

Preface

- Audience, page v
- Conventions, page v
- Related Cisco UCS Documentation, page vii

Audience

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

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

Conventions

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

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

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

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

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

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

Warning IMPORTANT SAFETY INSTRUCTIONS

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

SAVE THESE INSTRUCTIONS

Related Cisco UCS Documentation

Documentation Roadmaps

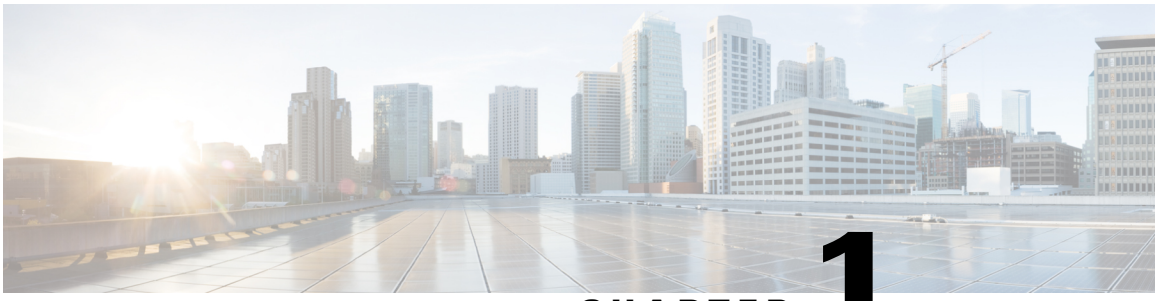
For a complete list of all B-Series documentation, see the *Cisco UCS B-Series Servers Documentation Roadmap* available at the following URL: http://www.cisco.com/go/unifiedcomputing/b-series-doc.

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

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

Other Documentation Resources

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



CHAPTER 1

Overview of Cisco Host Upgrade Utility

This chapter contains the following topics:

- About the Cisco Host Upgrade Utility, page 1
- License Agreement, page 5
- Understanding the HUU User Interface, page 5

About the Cisco Host Upgrade Utility

The Cisco Host Upgrade Utility (hereafter referred to as HUU) is a tool that you can use to upgrade the firmware on a Cisco UCS C-Series server. HUU includes an option that enables you to download a container for a selected platform on a Windows operating system. You can download the container from the HUU ISO by burning the ISO on a physical media. When you insert the physical media into the server, auto-run launches an Index.html page in your browser. This index.html page provides access to the location from where you can download the container. You also can download the container from the ISO using the standard ISO extraction utilities.

HUU provides a user interface where you can choose the firmware components that need an upgrade. In the previous releases (1.4(x)), HUU provided a text menu from which you could choose the components and initiate the upgrade. From version 1.5(x) onwards, HUU provides a graphical user interface to perform an upgrade.

You can upgrade the firmware on the following components using HUU:

- Cisco Integrated Management Controller (Cisco IMC)
- System BIOS
- Chassis Management Controller (CMC)
- LAN on motherboard (LOM)
  - Intel Ethernet i350 PCI Server Adapter
  - Intel X540 dual port LOM
  - Intel I350 mLOM
- Cisco VIC Network Controller Adapters

- Cisco Adapter UCS VIC 1225
- Cisco Adapter UCS VIC 1225T
- Cisco Adapter UCS VIC 1285
- Cisco Adapter UCS VIC 1227
- Cisco Adapter UCS VIC 1227T
- Cisco Adapter UCS VIC 1385

- Broadcom PCI adapters:
  - 5709 Dual and Quad port adapters
  - 57712 Dual port adapter SFP+
  - 57712 Dual port adapter 10GBaseT
  - 57810 Dual port

- Intel PCI adapters:
  - i350 Quad port adapter
  - X520 Dual port adapter
  - X540 Dual port adapter

- QLogic PCI adapters:
  - 2462 dual port adapter
  - 2562 dual port adapter
  - 2672 dual port adapter
  - 8242 dual port 10 Gbps adapter
  - 8362 dual port adapter

- Emulex PCI adapters:
  - LightPulse LPe11002 adapter
  - LightPulse LPe12002 adapter
  - LightPulse LPe16002 adapter
  - OneConnect® OCe11102 dual-port adapter
  - OneConnect® OCe14102 dual-port adapter

- LSI
  - Cisco UCSC RAID SAS 12G SAS Modular Raid Controller
  - Cisco UCSC RAID SAS 12G SAS Modular Raid Controller for C460 M4
  - UCS C3X60 12G SAS Pass through Controller

- Cisco RAID controller for UCS C3X60 Storage Servers
- Cisco UCSC RAID SAS 2008M-8i
- LSI MegaRAID SAS 9220-4i
- LSI MegaRAID SAS 9220-8i
- LSI MegaRAID SAS 9240-8i
- LSI MegaRAID SAS 9265CV-8i
- LSI MegaRAID SAS 9270CV-8i
- LSI MegaRAID SAS 9286CV-8e
- LSI MegaRAID SAS 8110-4i
- LSI MegaRAID SAS 9266-8i
- LSI MegaRAID SAS 9271CV-8i
- LSI MegaRAID SAS 9285CV-8e
- LSI MegaRAID SAS 9361-8i
- LSI MegaRAID SAS 9300-8i
- LSI MegaRAID SAS 9300-8E

- Hard Disk Drives
  - ST9146853SS
  - ST9300653SS
  - ST300MM0006
  - ST600MM0006
  - ST900MM0006
  - ST9500620SS
  - ST91000640SS
  - MZ6ER200HAGM
  - MZ6ER400HAGL
  - MZ6ER800HAGL
  - ST1000NM0001
  - ST2000NM0001
  - ST500NM0011
  - AL13SEB300
  - AL13SEB600
  - AL13SEB900
  - ST9300605SS

- ST9600205SS
- ST9900805SS
- MK1001TRKB
- MK2001TRKB
- ST33000650SS
- ST3600057SS
- ST9146803SS
- ST9300603SS
- ST9500530NS
- MTFDDAK100MAR
- MTFDDAK400MAR

- Fusion-io
  - Fusion-io ioDrive2 1205G
  - Fusion-io ioDrive2 3000G
  - Fusion-io ioDrive2 365G
  - Fusion-io ioDrive2 785G
  - Fusion-io ioDrive3 1000G
  - Fusion-io ioDrive3 1300G
  - Fusion-io ioDrive3 2600G
  - Fusion-io ioDrive3 3200G
  - Fusion-io ioDrive3 5200G
  - Fusion-io ioDrive3 6400G

- Nvidia
  - Nvidia GRID K1
  - Nvidia TESLA K10
  - Nvidia GRID K2
  - Nvidia TESLA K20m
  - Nvidia TESLA K20xm
  - Nvidia GRID K40m

Note

- This is the list of all the components supported by various servers. While upgrading firmware for a particular server, HUU discovers and displays only the components supported by that server.

For updated information on the components supported by various servers, see the Release Notes for Cisco UCS C-Series Software.

For information about upgrading the firmware on C-Series servers using non-interactive HUU, see the *Cisco UCS Rack-Mount Servers Cisco IMC XML API Programmer Guide*.

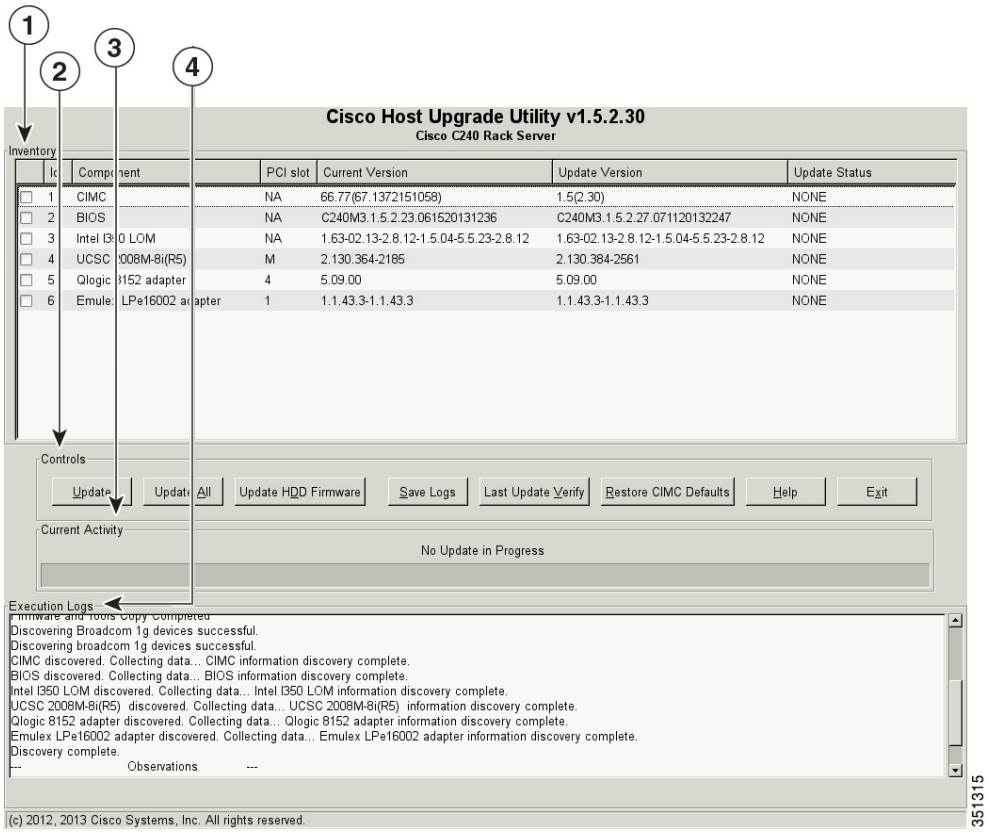
License Agreement

After the HUU boots, the first interface that appears is the End User License Agreement. Choose **I Agree** to agree to this license.

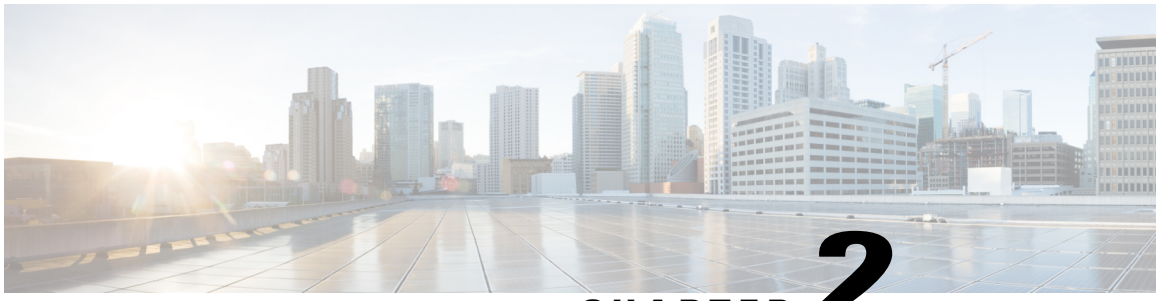
Understanding the HUU User Interface

This section provides a brief introduction to the UI elements in the various sections of the HUU user interface.

Figure 1: HUU User Interface



UI element	Description
1. Inventory section	
Id	Displays the serial number of the rows of the components.
Component	Displays the list of components of a server.
PCI Slot	Display the PCI slot information for the PCI adapter components.
Current Version	Displays the current version of the firmware for each of the listed components.
Update Version	Displays the version of the firmware that is available for upgrade.
Update Status	Displays the status of the update for each element in the list while an update is in progress.
2. Controls section	
Update	This button is used to initiate the firmware update for the selected components.
Update All	This button is used to initiate the firmware update of all the available components for a server.
Update HDD Firmware	This button is used to initiate firmware update on specific hard drives that support new firmware.
Save Logs	This button is used to save the log files that contain a detailed status of the update to an external USB device connected to the server physically or through the KVM vMedia. When an error occurs during an update, you are prompted to save the logs. The Save Logs feature is useful for troubleshooting.
Last Update Verify	This button is used to compare the previously updated firmware version for each component that was updated using the HUU with the current version of the firmware on the components.
Restore CIMC Defaults	This button is used to restore the CIMC settings to factory defaults.
3. Current Activity section	This section indicates the status of an update.
4. Execution Logs section	This section provides a detailed log of the various activities and their status while an update is in progress.



CHAPTER 2

Requirements and Support

This chapter contains the following topics:

- Requirements, page 7
- Support, page 8

Requirements

Important Separate ISO containers are released for each server platform. Be sure to download the correct ISO container for the server.

Note If you are downgrading from 2.0(x) to a version before 1.5.4, you need to downgrade to 1.5.4 first and then downgrade to a version that you want to downgrade to.

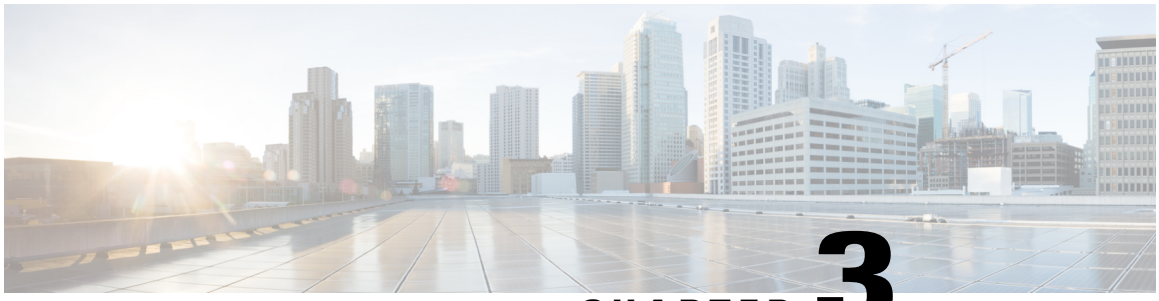
Server	Container	Minimum Cisco IMC and BIOS Version Requirements
C22	2.0.3i	Cisco IMC version: 2.0(3i) BIOS version: 2.0.3.0
C24	2.0.3i	Cisco IMC version: 2.0(3i) BIOS version: 2.0.3.0

Server	Container	Minimum Cisco IMC and BIOS Version Requirements
C220	2.0.3i	For CPUs with Intel Xeon(C) 26XX series or Intel Xeon(C) 24XX series processors Cisco IMC version: 2.0(3i) BIOS version: 2.0.3.0 For CPUs with Intel Xeon(C) 26XX V2 series processors Cisco IMC version: 2.0(3i) BIOS version: 2.0.3.0
C240	2.0.3i	For CPUs with Intel Xeon(C) 26XX series or Intel Xeon(C) 24XX series processors Cisco IMC version: 2.0(3i) BIOS version: 2.0.3.0 For CPUs with Intel Xeon(C) 26XX V2 series processors Cisco IMC version: 2.0(3i) BIOS version: 2.0.3.0
C3160	2.0.2e	Cisco IMC version: 2.0(2e) BIOS version: 2.0.2a.0 Chassis Management Controller (CMC) version: 2.0(2d)
C220 M4	2.0.3j	Cisco IMC version: 2.0(3j) BIOS version: 2.0.3d.0
C240 M4	2.0.3j	Cisco IMC version: 2.0(3j) BIOS version: 2.0.3d.0
C460 M4	2.0.3j	Cisco IMC version:2.0(3j) BIOS version: 2.0.3c.0

Support

The Cisco Host Upgrade Utility checks for and then updates the firmware for LOM and LSI controller devices on Cisco UCS C-series servers. For a complete list of supported LOM and LSI controller devices on the supported servers, see the *Release Notes for Cisco UCS C-Series Software* available at the following location:

http://www.cisco.com/en/US/products/ps10739/prod_release_notes_list.html



CHAPTER 3

Updating the Firmware on Cisco UCS C-Series Servers

This chapter includes the following topics:

- Upgrading the Firmware on a Cisco UCS C-Series Server Using the HUU, page 9

Upgrading the Firmware on a Cisco UCS C-Series Server Using the HUU

You can use the HUU ISO to upgrade components of the server from the host locally with a writable disk (DVD or CD), or remotely by mounting the HUU ISO as a virtual device. This following procedure explains how to upgrade the firmware using the HUU:

Step 1 Download the HUU ISO file:

a) Navigate to the following URL: http://www.cisco.com/cisco/software/navigator.html.
b) In the middle column, click **Servers – Unified Computing**.
c) In the right-hand column, click **Cisco UCS C-Series Rack-Mount Standalone Server Software**.
d) Choose the name of your model of server in the right column.
e) Click **Unified Computing System (UCS) Server Firmware**.
f) Choose the release number.
g) Click **Download Now** to download the `ucs-server platform-huu-version_number.iso` file.
h) Verify the information on the next page, and click **Proceed With Download**.
i) Continue through the subsequent screens to accept the license agreement and browse to a location where you want to save the file.

Step 2 If you want to prepare the ISO for a local upgrade, complete this step; Otherwise, go to Step 3.

a) Burn the ISO image onto a writable disk (CD).
b) Connect a VGA monitor and USB keyboard to the Cisco C-Series server.
c) Insert the disk into the USB DVD drive of the Cisco C-Series server.

d) Go to Step 4.

Step 3 Prepare the ISO for a remote upgrade using the **KVM Console**.

a) Use a browser to connect to the Cisco IMC GUI software on the server that you are upgrading.
b) in the address field of the browser, enter the Cisco IMC IP address for that server, and then enter your username and password.
c) Click **Launch KVM Console** on the toolbar to launch the **KVM Console**.
d) In the **KVM Console**, click the **Virtual Media**.
e) Click **Add Image** and click the `ucs-server-name-huu-version_number.iso` file.
f) In the **Client View** area, in the **Mapped** column, check the check box for the ISO file that you added and then wait for mapping to complete.
g) After the ISO file appears as a mapped remote device, go to Step 4.

Step 4 Boot the server and press F6 when prompted to open the **Boot Menu** screen.

Step 5 In the **Boot Menu** screen, choose the prepared ISO:

- For a local upgrade, choose the physical or externally connected CD/DVD device and then press Enter.
- For a remote upgrade, choose **Cisco vKVM-Mapped vDVD1.22,** and press Enter.

The server boots from the selected device.

Step 6 After the HUU boots, Cisco End User License Agreement (EULA) appears, read the EULA and click:

- I Agree to agree with the license agreement and proceed with the update.
- I Disagree to cancel.

After you accept the EULA, when the **Cisco Host Upgrade Utility** window appears with a list of all the components that are available for update.

Step 7 If you want to update all the listed components, click **Update all**.

Note
- If you are updating to 2.0 (x) from versions 1.5(1l) and before, or from version 1.5.3 both the active and the backup versions of Cisco IMC will be updated to 2.0(x).
- During update the KVM connection will be lost, you have to reconnect to view the progress of the updates.

Enabling Cisco IMC Secure Boot confirmation dialog box appears.

Step 8 Read the content on the confirmation box carefully and click **Yes**, if you want to go ahead and update the firmware and enable Cisco Secure Boot.

Note
- If you are updating from a version below 2.0 (x) to 2.0(x), when you click **YES** both the active and the backup versions of Cisco IMC will be updated to 2.0(x).
- During update the KVM connection will be lost, you have to reconnect to view the progress of the updates.

For more information on Cisco IMC secure boot, refer to the **Introduction to Cisco IMC Secure Boot** section in the *Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide, Release 2.0(1)*.

Step 9 If you want update specific components from the list, choose the components that you want to update.

Step 10 Click **Update**.

Note
- We recommend you update the firmware on all components using the **Update all** option, unless you want to specifically update the firmware of a component.
- When you update the firmware of one of the following three components: BIOS, Cisco IMC, or CMC, we recommend that you also update the firmware of the other two components.
- If you update the Cisco IMC firmware, click **Exit** and then **Ok** to activate the Cisco IMC firmware.
- If you choose to update Cisco IMC and any other component with it and if you have not chosen BIOS, then on exit, you will be prompted to update the **Chassis Firmware**, click **Yes** in the confirmation box to update the chassis firmware.

This initiates the update and the status of the update is displayed in the **Update Status** column. You can also view a more detailed log of a series of activities and statuses that are involved while updating the firmware in the **Execution Logs** section.

Step 11 If you want to update the firmware of the hard disk of a server, click **Update HDD Firmware**. A window displays a list of hard disk drives on the server that support new firmware. Hard disk drives that do not support firmware upgrades are not listed.

Important Updating the firmware of the hard disk drive could result in data loss. Cisco recommends that you take a complete system backup prior to updating the firmware.

a) To update the firmware of all the hard disks, click **Update All**.
With this option, HDDs with the latest firmware installed are not updated.

b) To update a specific HDD, choose the HDD and click **Update**.

Step 12 Click **Exit** to exit from the HUU.

Note
- If you have updated the Cisco IMC and not the BIOS, when you click **Exit**, Cisco IMC gets activated and you lose connectivity to the Cisco IMC and KVM.
- If you have selected LOM for update and you are on shared LOM mode, when you click **Exit**, you lose connectivity to the Cisco IMC and KVM.

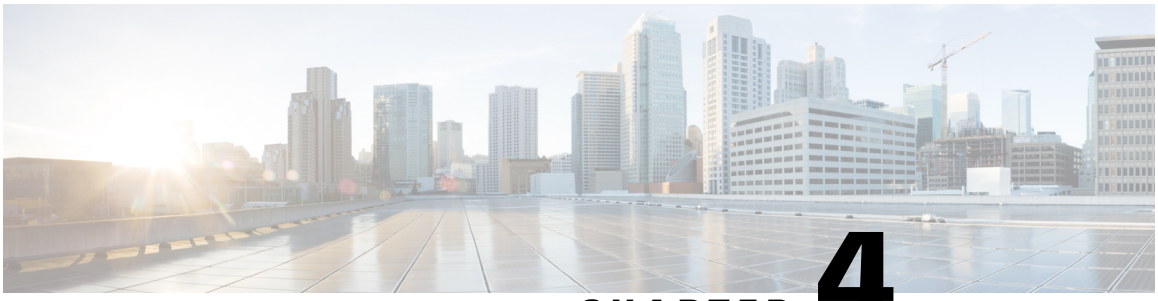
Step 13 Click **Yes** at the confirmation prompt.

Step 14 Reboot the server to apply firmware changes.

Step 15 Boot the server back into HUU ISO, and click **Last Update Verify** to verify if the update was successfully completed. This action compares the previously updated firmware version for each component that was updated using the HUU with the current version of the firmware on the components and provides the status of the update.

Step 16 If you want to save the log files of the update status for later use, click **Save Logs**.
Log files that contain a detailed status of the update are saved to an external USB device that is connected to the server physically or through the KVM vMedia.

Note If an error occurs while updating the firmware, you are prompted to save the error log. Click **Save Logs** to save the log to an externally connected USB. This log can be used for identifying the cause of the error and troubleshooting.



CHAPTER 4

Troubleshooting

This chapter contains the following topics:

- Troubleshooting, page 13

Troubleshooting

The following table describes troubleshooting suggestions for issues that you might encounter.

Issue	Suggested Solution
Connection to Cisco IMC is lost after an update and reboot and the KVM session ends.	This is expected behavior after a firmware update. Log back in to the Cisco IMC and reestablish your KVM session.
The following error message is observed: `PID, Board Part Number, Product Part Number <PID, Board Part Number, Product Part Number> is not supported by this HUU image. HUU will not boot on this machine. Press any key to reboot the server.`	This error message is displayed when the HUU ISO is not supported by the server. Use the HUU ISO that is supported by the server.

Troubleshooting