



Cisco Host Upgrade Utility User Guide - For S3260 Storage Servers

First Published: 2017-04-24

Last Modified: 2021-03-16

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 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.

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.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. 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. (1721R)

© 2017–2021 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	2
Understanding the HUU User Interface	2

CHAPTER 2

Requirements and Support	5
Requirements	5
Support	5

CHAPTER 3

Updating the Firmware on Cisco UCS C-Series Servers	7
Upgrading the Firmware on a Cisco UCS C-Series Server Using the HUU	7

CHAPTER 4

Troubleshooting	11
Troubleshooting	11



Preface

This preface includes the following sections:

- [Audience, on page v](#)
- [Conventions, on page v](#)
- [Related Cisco UCS Documentation, on 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 <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> .

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.



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



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



Warning IMPORTANT SAFETY INSTRUCTIONS

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

SAVE THESE INSTRUCTIONS

Related Cisco UCS Documentation

Documentation Roadmaps

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

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

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, on page 1](#)
- [License Agreement, on page 2](#)
- [Understanding the HUU User Interface, on page 2](#)

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:

- Baseboard Management Controller (BMC)
- BIOS
- Chassis Management Controller (CMC)
- SAS Expander
- UCSC-C3260-SIOC
- LSI
 - UCS S3260 12G SAS Pass through Controller
 - Cisco RAID controller for UCS C3X60 Storage Servers
 - UCS S3260 Double Rock Pass through Controller

- Cisco UCS C3000 RAID controller for M4 Servers

**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 XML API Programmer Guide*.

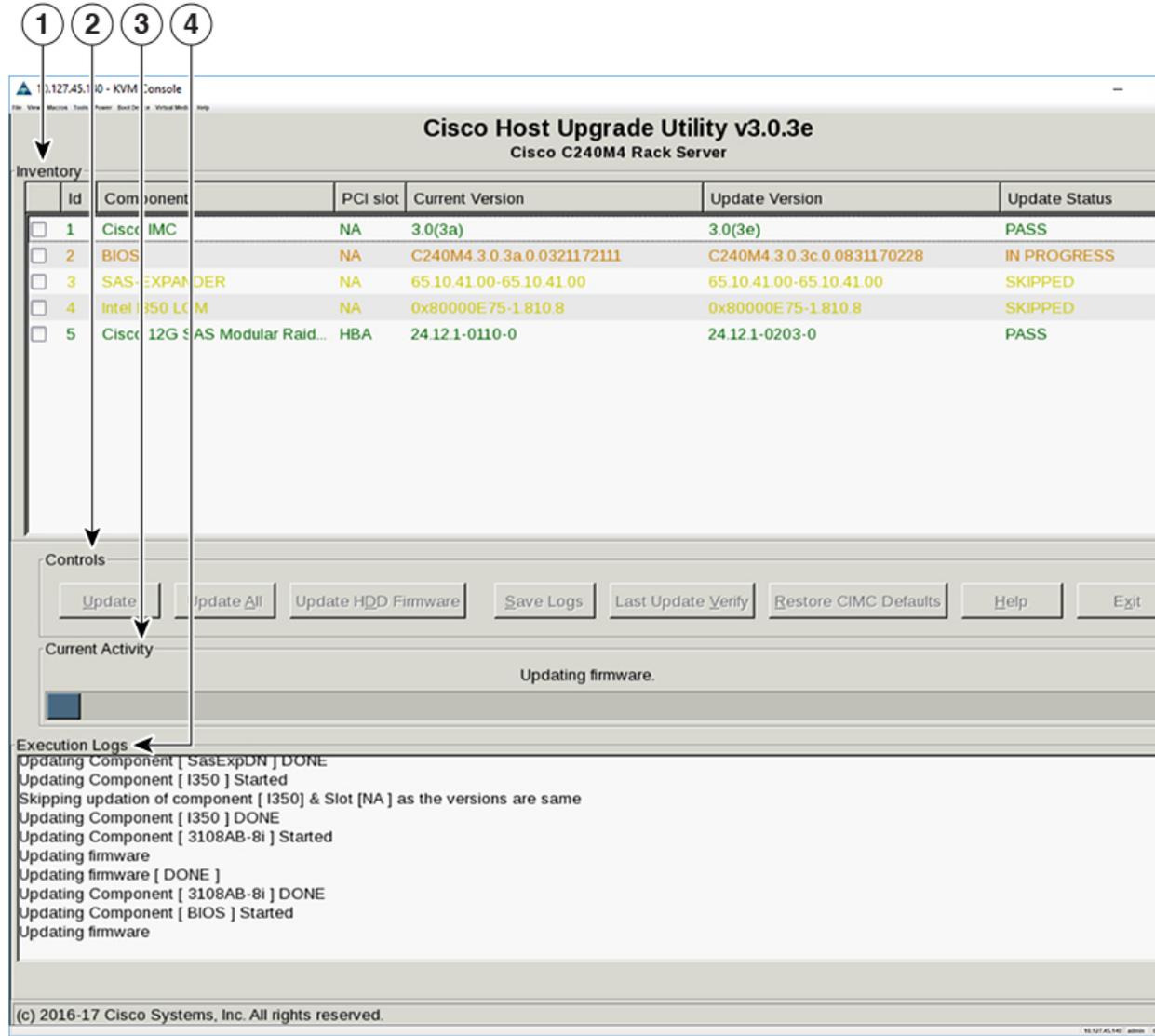
License Agreement

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.

UI element	Description
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 Chassis Defaults	This button is used to restore the CMC settings for the S3260 servers to factory defaults. Note This option is available only for S3260 servers.
Restore Cisco IMC Defaults	This button is used to restore the Cisco IMC settings to factory defaults. Note This option is available only for non S3260 servers.
Exit	This button is used to exit from the HUU. If you have updated the BMC or CMC when you click Exit , BMC or CMC gets activated.
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, on page 5](#)
- [Support, on page 5](#)

Requirements



Important

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

We recommend the minimum version required for an upgrade is N-2. Where N is the release that you want to upgrade to. However, upgrading to higher versions maybe possible. For detailed information about the firmware versions of the servers and associated components for all releases, see [Cisco UCS C-Series Integrated Management Controller Firmware Files](#)

Support

The Cisco Host Upgrade Utility checks for and then updates the firmware for LSI controller devices on Cisco UCS C-series servers. For a complete list of supported 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, on page 7](#)

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:



Important While downgrading from 3.0(3) to a previous version, if the single server Dual SIOC option is enabled, you must disable it before downgrading.

Step 1

Download the HUU ISO file:

- Navigate to the following URL: [Software Download](#)
- Search for **Servers – Unified Computing**.
- In the right-hand column, click **Cisco UCS S-Series Rack-Mount Standalone Server Software**.
- Choose the name of your model of server in the right column.
- Click **Unified Computing System (UCS) Server Firmware**.
- Choose the release number.
- Click **Download Now** to download the `ucs-server platform-huu-version_number.iso` file.
- Verify the information on the next page, and click **Proceed With Download**.
- 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**.

- Burn the ISO image onto a writable disk (CD).
- 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 software on the server that you are upgrading.
- b) In the address field of the browser, enter the 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**.

Note Select the server node on which you want to boot the HUU.

- 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**.

Enabling CMC Secure Boot confirmation dialog box appears.

Important Do not choose secure boot while upgrading to 2.0(13e) from a previous release. Upgrade CMC to 2.0(13e) version first and then upgrade it to enable secure boot.

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 CMC 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.

Enabling CMC Secure Boot confirmation dialog box appears.

Note Do not choose secure boot while upgrading to 2.0(13e) from a previous release. Upgrade CMC to 2.0(13e) version first and then upgrade it to enable secure boot.

Step 10 Click **Update**.

Note

- We recommend you to 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: BMC, BIOS, or CMC, we recommend that you also update the firmware of the other two components.
- If you update the BMC firmware, click **Exit** and then **Ok** to activate the BMC firmware.
- If you choose to update BMC 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.

Important When you click **Update** or **Update all** to update the chassis components of CMC1 and CMC2 simultaneously, the update on the second triggering server component is skipped, and the subsequent component is updated.

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 BMC and not the BIOS, when you click **Exit**, BMC gets activated and you lose connectivity to the BMC 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**.

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, on page 11](#)

Troubleshooting

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

Issue	Suggested Solution
Connection to BMC 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 BMC and reestablish your KVM session.
<p>The following error message is observed:</p> <pre>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.</pre>	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.
When you update the chassis components simultaneously using either Update or Update All option, the update on the second triggering chassis component is skipped, and the subsequent component is updated.	Update the server nodes 1 and 2 sequentially.

