Cisco Host Upgrade Utility User Guide

First Published: 2016-12-14

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

CONTENTS

Preface

This preface includes the following sections:

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.

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

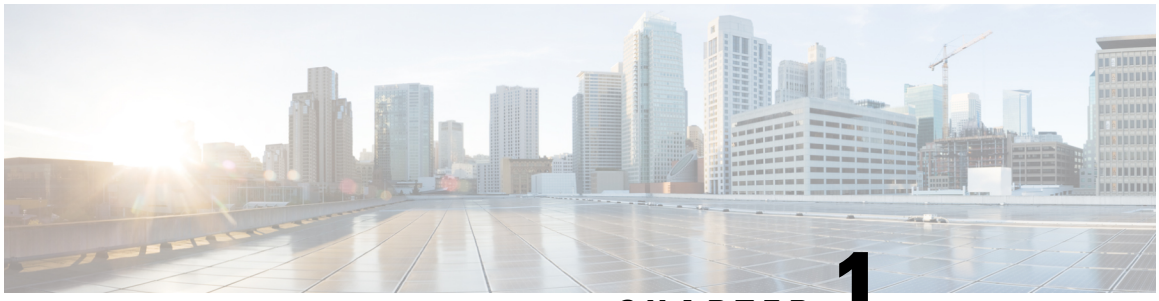
For a complete list of all B-Series documentation, see the *Cisco UCS B-Series Servers Documentation Roadmap* available at the following URL: http://www.cisco.com/go/unifiedcomputing/b-series-doc.

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

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.

For information about the components supported and their firmware versions for various servers in a release, see the Firmware Version Listing and Internal Dependencies for Cisco IMC Releases.

For information about upgrading the firmware on C-Series servers using non-interactive HUU, see the Cisco UCS C-Series XML API Programmer's Guides

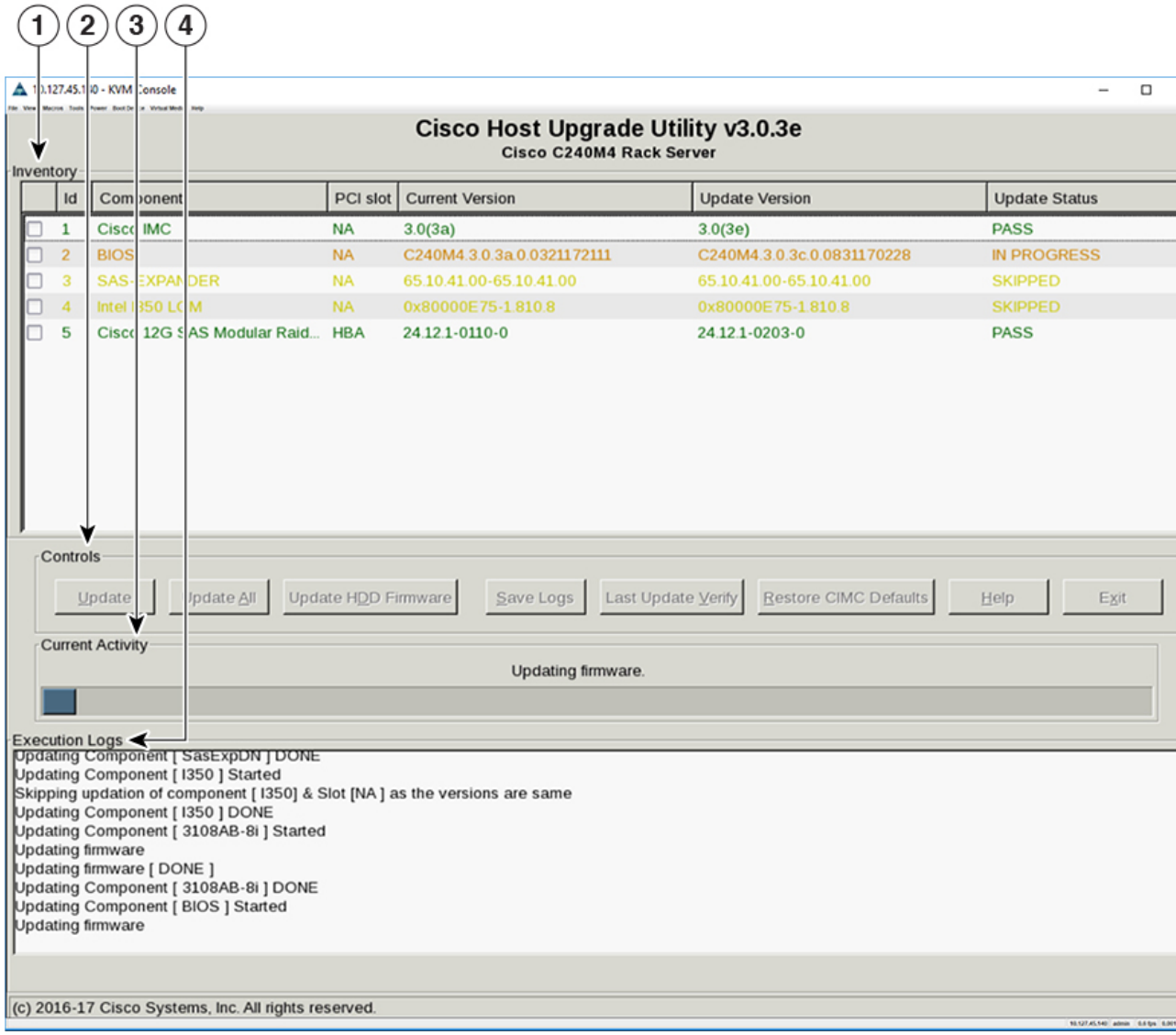
License Agreement

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

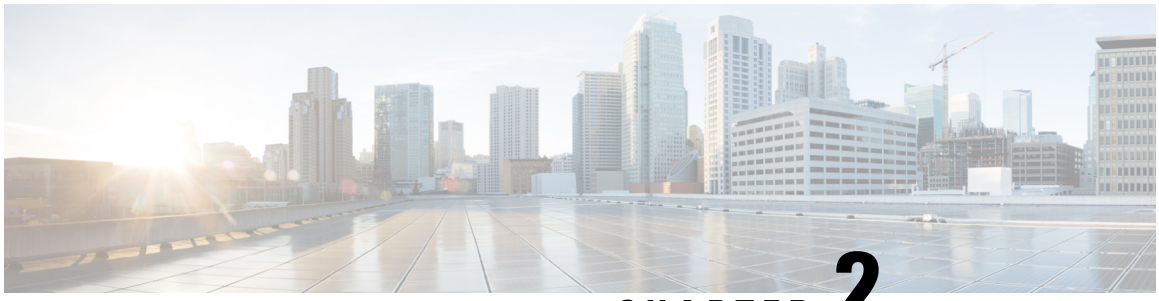
This section provides a brief introduction to the UI elements in the various sections of the HUU user interface.

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

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

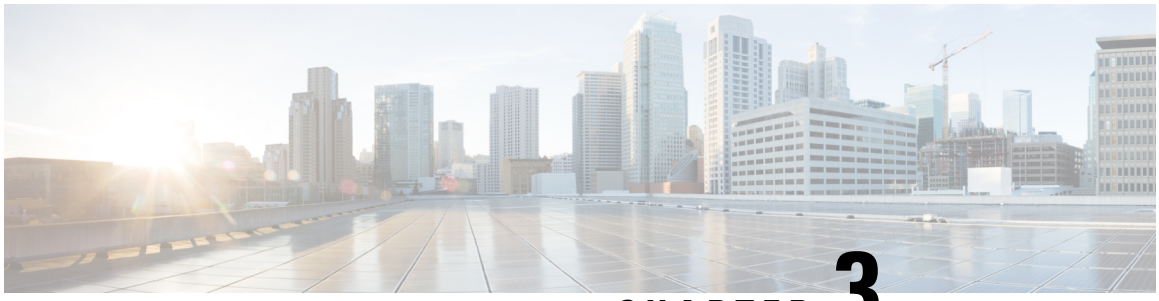
While upgrading or downgrading from one release to another, see the Upgrade Paths for Release section of the respective release notes at the following location for upgrade and downgrade scenarios: Release Notes for Cisco UCS C-Series Software

For detailed information about the available components per server and their firmware versions, see: Firmware Version Listing and Internal Dependencies for Cisco IMC Releases

Support

The Cisco Host Upgrade Utility checks for and then updates the firmware for the components on Cisco UCS C-series servers. For a complete list of server specific components supported in a release, see the Firmware Version Listing and Internal Dependencies for Cisco IMC Releases

Note If the firmware version of a component that you are trying to update to is the same as the current firmware version, then HUU skips the update for that component, but proceeds to update the firmware of the components that are not updated.



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

Note Secure adapter update is enabled once server components are updated to 2.0(13e). Subsequently supported adapters can be updated.

Important After upgrading the Cisco IMC firmware, you must check the compatibility matrix to verify if the drivers are compliant with the upgraded version of Cisco IMC. If the driver versions are non-compliant, you must upgrade the driver versions to match the Cisco IMC version.

The *Hardware and Software Interoperability Matrix* is available here:

http://www.cisco.com/en/US/products/ps10477/prod_technical_reference_list.html

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. The following procedures explain how to upgrade the firmware using the HUU:

Downloading and Preparing the ISO for Upgrade

Procedure

Step 1 Download the HUU ISO file:

a) Navigate to the following URL: Software Download
b) Search for **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** to download the `ucs-server platform-huu-version_number.iso` file.
h) Enter your credentials in the login screen.
i) Continue through the subsequent screens to accept the license agreement and browse to a location where you want to save the file.
j) Click **Download**.
ISO bundle downloads to the chosen location.

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) Perform one of the following updating the firmware procedures depending on the firmware components that you want to upgrade.

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 **Virtual Media**.
e) Click **Activate Virtual Devices** and then **Accept this session**.
f) Click **Map CD/DVD** and browse for the `ucs-server-name-huu-version_number.iso` file.
g) Click **Map Device**.
h) 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.
i) After the ISO file appears as a mapped remote device, perform one of the following procedures depending on the firmware components that you want to upgrade.

Updating Firmware Using the Update All Option

Procedure

Step 1 Boot the server and press **F6** when prompted to open the **Boot Menu** screen.

Step 2 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 3 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.

Note When you choose **I Disagree**, it cancel the upgrade and reboots the host.

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

- **Enabling Cisco IMC Secure Boot** confirmation dialog box appears.

Note This message appears for M3 servers only and only if the secure boot is not already enabled.

Step 5 Read the content on the confirmation box carefully and click **Yes**, if you want to go ahead to update the firmware and enable Cisco IMC 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 6 Reboot the server to apply firmware changes.

Updating the Firmware of Specific Components

The following procedure explains how update the firmware of individual components:

Procedure

Step 1 If you want update specific components from the list, choose the components that you want to update.

If you want to downgrade the secure adapter update firmware, complete steps **2** through **4** below. Else continue to step **5**.

Step 2 To downgrade the secure adapter update firmware, map the HUU and allow it to boot.

Step 3 On the virtual **KVM Console**, wait for the message 'Loading firmware tools' to display, when the HUU boots up.

Step 4 Disable **enable-security-version-check** once you see the 'Loading firmware tools' message.

a) From the Cisco IMC command line interface, run the command **scope cimc->scope adapter-secure-update->enable-security-version-check yes/no/status**.

b) From the Cisco IMC web UI, log on to the **Utilities** tab.
c) From the XML API, enter the following data:

Request:

```
<configConfMo cookie='1458615470/be0d9210-2e9a-1e9a-8004-816d1e1b0ff4'
 inHierarchical='false' dn='sys/rack-unit-1'>
  <inConfig>
    <computeRackUnit dn='sys/rack-unit-1' adaptorSecureUpdate='Disabled'/>
  </inConfig>
</configConfMo><IP>/nuova
```

Response:

```
<configConfMo dn="sys/rack-unit-1"
cookie="1474315600/b51b2682-3ce2-1ce2-8038-c4ae729d8b18"
 response="yes">
 <outConfig>
  <computeRackUnit dn="sys/rack-unit-1" adminPower="policy" availableMemory="196608"
   model="UCSC-C240-M4L" memorySpeed="1866" name="UCS C240 M4L" numOfAdaptors="1"
   numOfCores="12" numOfCoresEnabled="12" numOfCpus="2" numOfEthHostIfs="2"
numOfFcHostIfs="2"
   numOfThreads="24" operPower="on" originalUuid="0CA8BC15-2499-46F2-BFFE-686B224AB52E"

   presence="equipped" serverId="1" serial="FCH1927V0FC" totalMemory="196608" usrLbl=""

   uuid="0CA8BC15-2499-46F2-BFFE-686B224AB52E" vendor="Cisco Systems Inc"
   cimcResetReason="ac-cycle" adaptorSecureUpdate="Disabled" status="modified" >
    </computeRackUnit>
 </outConfig>
</configConfMo>
```

Step 5 Click **Update** to return to the update process.

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 On the S3260 servers, 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 6 Click **Exit** to exit from the HUU.

Note After clicking **Exit** you must wait for a few minutes before the server automatically powers up, indicating the completion of updating and activating of the new firmware.

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.

Updating the HDD Firmware

The following procedure provides steps to update the HDD firmware:

Procedure

Step 1 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 2 Reboot the server to apply firmware changes.

Verifying the Update Status and Saving Logs

The following procedure provides steps to verify the last update and save logs:

Procedure

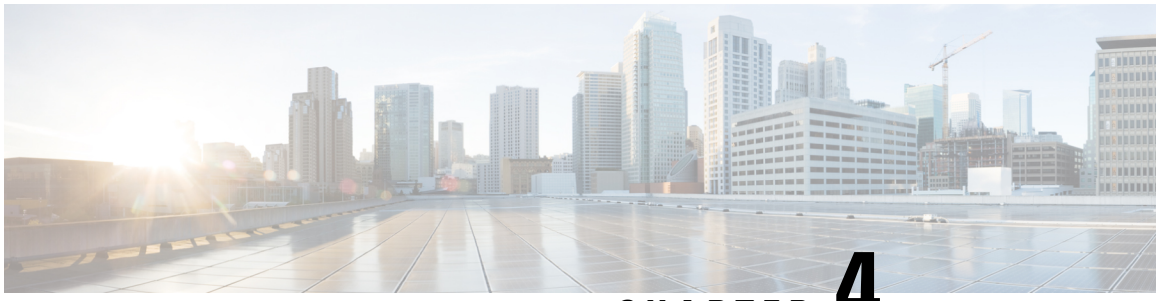
Step 1 After you have updated the firmware, boot the server back into HUU ISO, and click **Last Update Verify**.

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 2 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

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.
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.
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.

Troubleshooting