Cisco Host Upgrade Utility User Guide, Release 4.2

First Published: 2021-10-20

Last Modified: 2022-07-08

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

CHAPTER 1

CHAPTER 2

CHAPTER 3

CHAPTER 4

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.

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

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

Warning IMPORTANT SAFETY INSTRUCTIONS

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

SAVE THESE INSTRUCTIONS

Related Cisco UCS Documentation

Documentation Roadmaps

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

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

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

Other Documentation Resources

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

CHAPTER 1

Overview of Cisco Host Upgrade Utility

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 or downgrade the firmware on a Cisco UCS C-Series and S-Series servers.

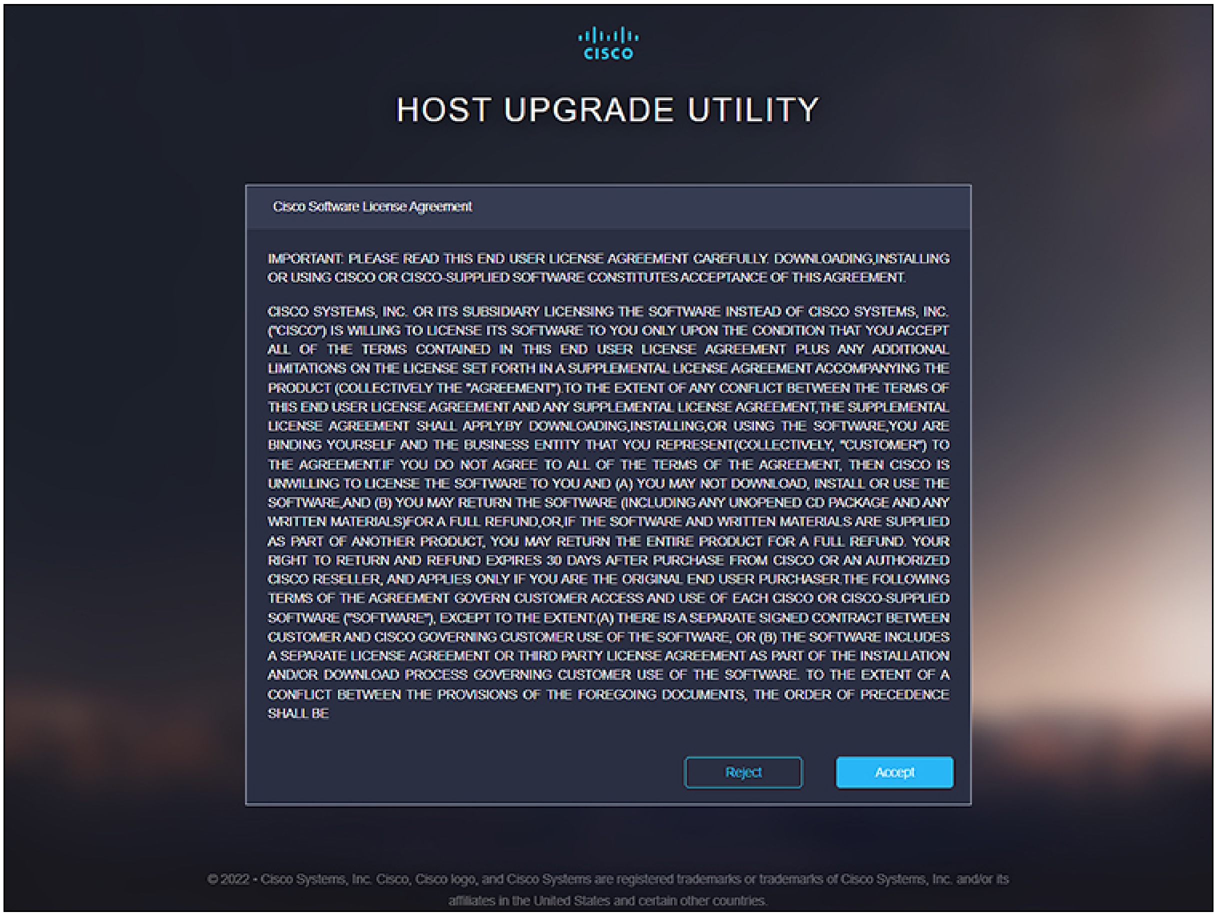
HUU provides a user interface where you can choose the firmware components that need an upgrade. Beginning with release 4.2, HUU user interface is updated with new options. Cisco recommends you to use this guide to familiarize yourself with the new interface.

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.

License Agreement

Whenever HUU boots, the first interface that appears is the **Welcome Screen** and then the **End User License Agreement**. Click **Accept** to agree to this license.

Figure 1: License Agreement



Cisco Software License Agreement

IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. DOWNLOADING,INSTALLING OR USING CISCO OR CISCO-SUPPLIED SOFTWARE CONSTITUTES ACCEPTANCE OF THIS AGREEMENT.

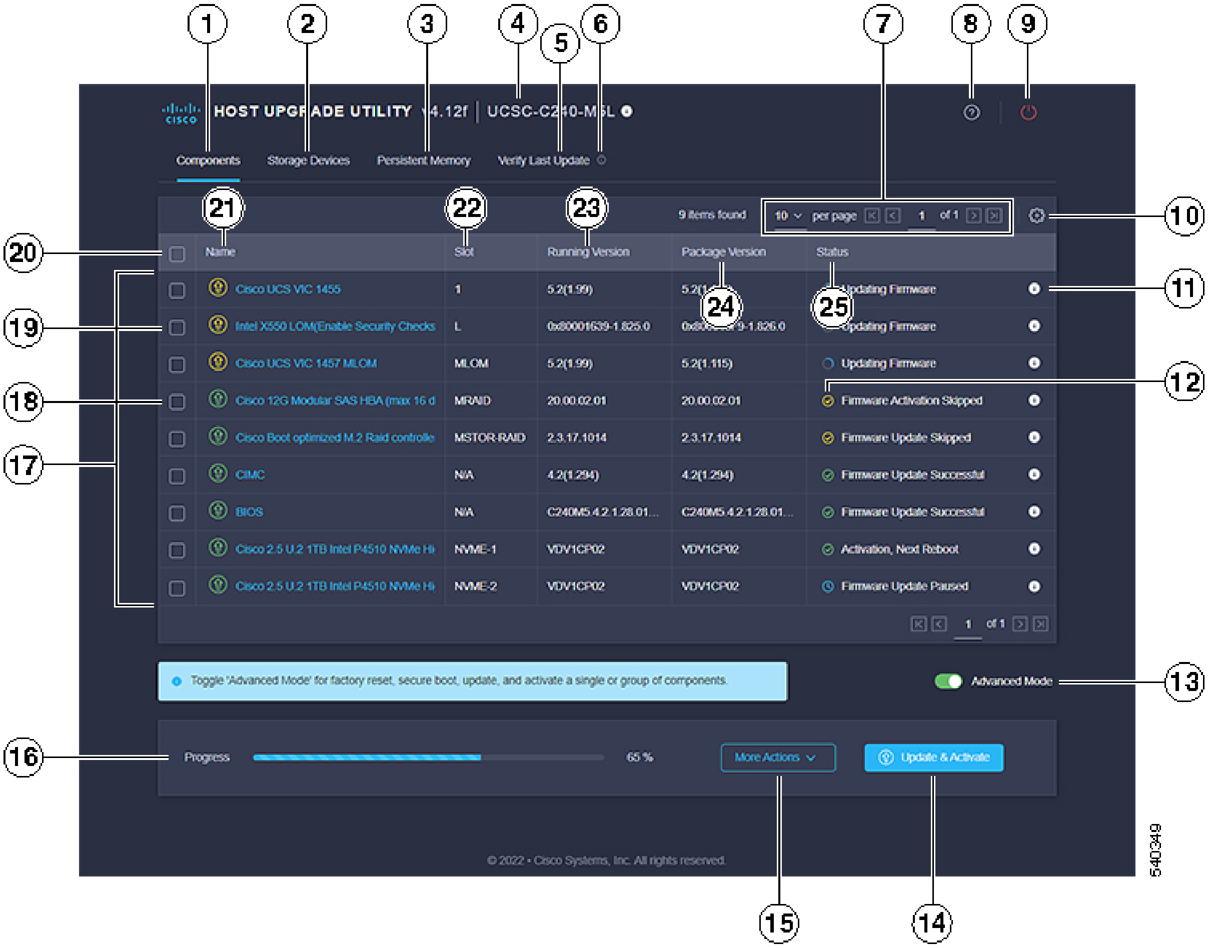
CISCO SYSTEMS, INC. OR ITS SUBSIDIARY LICENSING THE SOFTWARE INSTEAD OF CISCO SYSTEMS, INC. ("CISCO") IS WILLING TO LICENSE ITS SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS END USER LICENSE AGREEMENT PLUS ANY ADDITIONAL LIMITATIONS ON THE LICENSE SET FORTH IN A SUPPLEMENTAL LICENSE AGREEMENT ACCOMPANYING THE PRODUCT (COLLECTIVELY THE "AGREEMENT").TO THE EXTENT OF ANY CONFLICT BETWEEN THE TERMS OF THIS END USER LICENSE AGREEMENT AND ANY SUPPLEMENTAL LICENSE AGREEMENT,THE SUPPLEMENTAL LICENSE AGREEMENT SHALL APPLY.BY DOWNLOADING,INSTALLING,OR USING THE SOFTWARE,YOU ARE BINDING YOURSELF AND THE BUSINESS ENTITY THAT YOU REPRESENT(COLLECTIVELY, "CUSTOMER") TO THE AGREEMENT.IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE AGREEMENT, THEN CISCO IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE,AND (B) YOU MAY RETURN THE SOFTWARE (INCLUDING ANY UNOPENED CD PACKAGE AND ANY WRITTEN MATERIALS)FOR A FULL REFUND,OR,IF THE SOFTWARE AND WRITTEN MATERIALS ARE SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM CISCO OR AN AUTHORIZED CISCO RESELLER, AND APPLIES ONLY IF YOU ARE THE ORIGINAL END USER PURCHASER.THE FOLLOWING TERMS OF THE AGREEMENT GOVERN CUSTOMER ACCESS AND USE OF EACH CISCO OR CISCO-SUPPLIED SOFTWARE ("SOFTWARE"), EXCEPT TO THE EXTENT:(A) THERE IS A SEPARATE SIGNED CONTRACT BETWEEN CUSTOMER AND CISCO GOVERNING CUSTOMER USE OF THE SOFTWARE, OR (B) THE SOFTWARE INCLUDES A SEPARATE LICENSE AGREEMENT OR THIRD PARTY LICENSE AGREEMENT AS PART OF THE INSTALLATION AND/OR DOWNLOAD PROCESS GOVERNING CUSTOMER USE OF THE SOFTWARE. TO THE EXTENT OF A CONFLICT BETWEEN THE PROVISIONS OF THE FOREGOING DOCUMENTS, THE ORDER OF PRECEDENCE SHALL BE

© 2022 • Cisco Systems, Inc. Cisco, Cisco logo, and Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

HUU Graphical User Interface

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

Figure 2: HUU User Interface



HOST UPGRADE UTILITY v4.12f | UCSC-C240-M5L

Components | Storage Devices | Persistent Memory | Verify Last Update

9 items found | 10 per page | 1 of 1

□	Name	Slot	Running Version	Package Version	Status
□	Cisco UCS VIC 1455	1	5.2(1.99)	5.2(1.	Updating Firmware
□	Intel X550 LOM(Enable Security Checks	L	0x80001639-1.825.0	0x800 9-1.826.0	Updating Firmware
□	Cisco UCS VIC 1457 MLOM	MLOM	5.2(1.99)	5.2(1.115)	Updating Firmware
□	Cisco 12G Modular SAS HBA (max 16 d	MRAID	20.00.02.01	20.00.02.01	Firmware Activation Skipped
□	Cisco Boot optimized M.2 Raid controlle	MSTOR-RAID	2.3.17.1014	2.3.17.1014	Firmware Update Skipped
□	CIMC	N/A	4.2(1.294)	4.2(1.294)	Firmware Update Successful
□	BIOS	N/A	C240M5.4.2.1.28.01...	C240M5.4.2.1.28.01...	Firmware Update Successful
□	Cisco 2.5 U.2 1TB Intel P4510 NVMe Hi	NVME-1	VDV1CP02	VDV1CP02	Activation, Next Reboot
□	Cisco 2.5 U.2 1TB Intel P4510 NVMe Hi	NVME-2	VDV1CP02	VDV1CP02	Firmware Update Paused

1 of 1

Toggle 'Advanced Mode' for factory reset, secure boot, update, and activate a single or group of components.

Advanced Mode

Progress 65 %

More Actions | Update & Activate

© 2022 • Cisco Systems, Inc. All rights reserved.

Table 1: HUU User Interface

	GUI Element	Description
1	**Components** Tab	Lists all the server components for upgrade or downgrade. You can update the firmware of all components or specific components on this list. **Note** If you choose to update the firmware of specific components, you must update the Cisco IMC, CMC and BIOS to the same version.

	GUI Element	Description
2	**Storage Devices** Tab	Lists all the external storage drives (HDDs) available on the server. You can choose to upgrade or downgrade the firmware of all the storage drives or specific drives available on this server. **Note** Cisco recommends you to take a backup before upgrading or downgrading the firmware. Cisco is not responsible for any data loss due to firmware upgrade or downgrade.
Note 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.		
3	**Persistent Memory** Tab	Lists all the external Persistent Memory available on the server. You can choose to upgrade or downgrade the firmware of all or specific memrories available on this server. **Note** Cisco recommends you to take a backup before upgrading or downgrading the firmware. Cisco is not responsible for any data loss due to firmware upgrade or downgrade.
4	**Server Info**	Provides the name of the server. Hover the cursor over the icon to view the following information about the server: • Host Name • System Type • Model • Serial Number • Manufacturer • UUID

	GUI Element	Description
5	**Verify Last Update** Tab	Provides information about firmware update status of the components after the last HUU boot. To verify the firmware update status, reboot again to same HUU image.
6	**Verify Last Update** info icon	Hover the cursor to view help text.
7	**Table Setting** options	You can use the drop list to set the number of components listed in the table per page. You can also use the forward and backward buttons to navigate through the table.
8	**HUU Help** icon	Displays the following options: • Site Tour—Provides a guided tour of the application to show the main features and help you understand the GUI. • Help—Displays the online help page for HUU. • About—Displays a brief description of HUU along with the HUU version.
9	**Server Power Cycle** icon	You can use this to recycle the server. You can also recycle the server using the power cycle option in KVM console. **Note** Server may power cycle multiple times to activate firmware. Do not interrupt power cycle. Once power cycle is complete, boot menu is displayyed.

	GUI Element	Description
10	**Table Setting** icon	

	GUI Element	Description
		Use this option to edit the table view. Following options are available in **Components** tab: • Name • Product ID • Vendor • Slot • Running Version • Package Version • Status Following options are available in **Storage Devices** tab: • Name • Product ID • Vendor • Enclosure • Drive Type • Model Number • Serial Number • Controller Name • Controller Set • Slot • Running Version • Package Version • Status Following options are available in **Persistent Memory** tab: **Note** **Persistent Memory** tab is applicable only for few servers. • Name • Product ID

	GUI Element	Description
		• Vendor • Enclosure • Drive Type • Model Number • Serial Number • Controller Name • Controller Set • Slot • Running Version • Package Version • Status
11	**Component Firmware Upgrade Status** info icon	Provides all the information about the update status.
12	**Component Firmware Upgrade Status** icon	Provides the current firmware update status of the component. This can be one of the following: • Green—Firmware update successful. • Red—Firmware update fail. • Yellow—Firmware update skipped.
13	**Advanced Mode** Toggle button	Allows you the following options: • Update or Activate individual components or drives through **More Actions** drop-down list. If you do not select any component, this action updates all the components together. • Perform a Factory Reset through **More Actions** drop-down list.

	GUI Element	Description
14	**Update and Activate** button	When **Advanced Mode** is off: • Allows you to update and activate all components/drives with single click. When **Advanced Mode** is on: • Allows you to either update and activate all components/drives with single click. • Or, allows to you update and activate selected components/drives with single click.
15	**More Actions** drop-down list	**Note** **More Actions** drop-down list is available only when **Advanced Mode** is on. Following drop-down options are available: • When no components/drives are selected, allows you to update or activate all components/drives. • When one or more components/drives are selected, allows to you update or activate selected components/drives. • Perform a Factory Reset. • Allows you to enable secure boot in Cisco UCC S3260 M5 servers.
16	**Progress** bar	Shows firmware update or activation status in percentage.

	GUI Element	Description
17	List of components or drives	Under **Components** tab, list of components available in the server are displayed. Under **Storage Drives** tab, list of drives available in the server are displayed.
18	**Component** checkbox	**Note** Checkbox is available only when **Advanced Mode** is on. Allows you to select individual component/drive.
19	**Firmware information** icon	Firmware information is color coded: • Green—Firmware is up to date for the component/drive. • Yellow—updated firmware is available for the component/drive.
20	**Select All** checkbox	**Note** Checkbox is available only when **Advanced Mode** is on. Allows you to select all the components/drives listed on the page.
21	**Name** column	Displays the name of the component.
22	**Slot** column	Displays the slot on the server for the component.
23	**Running Version** column	Current version of the firmware.
24	**Package Version** column	Updated version available for upgrade.
25	**Status** column	Displays the firmware update status.

	GUI Element	Description
26 (not shown in the image	**Enclosure** column	**Note** This column is available only under **Storage Devices** tab. Displays the enclosure number of the storage device.
27 (not shown in the image	**Bank Label** column	**Note** This column is available only under **Persistent Memory** tab. Displays the node and DIMM channel of the persistent memory.

CHAPTER 2

Requirements and Support

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 upgrades 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.

CHAPTER 3

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

Updating the Firmware

This section describes procedure to upgrade or downgrade the C-Series and S-Series servers firmware and various options available for upgrade or downgrade.

Note After updating the Cisco IMC firmware, you must check the compatibility matrix to verify if the drivers are compliant with the updated version of Cisco IMC. If the driver versions are non-compliant, you must update 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

Downloading the ISO File for Update

Step 1 Navigate to the following URL: Software Download

You must be logged in to continue.

Step 2 Search for—**Unified Computing**.

Step 3 In the center column, click **Cisco UCS C-Series Rack-Mount Standalone Server Software**.

Step 4 Choose the name of your model of server in the right column.

Step 5 Click **Unified Computing System (UCS) Server Firmware**.

Step 6 From the left pane, choose the release number

Step 7 Click the Download icon to download the `ucs-server platform-huu-version_number.iso` file.

Step 8 Click **Accept License Agreement** to start the download.

What to do next

Prepare the ISO file.

Preparing the ISO File for Firmware Update

Before you begin

Ensure that the ISO file is downloaded and saved.

If you want to prepare the ISO for a local update, perform these steps before starting the procedure:

1. Burn the ISO image onto a writable disk (CD/DVD) or copy it on a USB drive.
2. Connect a VGA monitor and USB keyboard to the server.
3. Insert the disk into the USB DVD drive of the server or the USB drive into the USB port.

Step 1 Use a browser to connect to the software on the server that you are upgrading.

Step 2 In the address field of the browser, enter the IP address for that server, and then enter your username and password.

Step 3 Click **Launch KVM Console** from the toolbar.

Ensure that your browser allows pop up windows. KVM console opens in a different window.

Step 4 In the KVM Console, click **Virtual Media**.

Note Virtual Media is not available for read-only users.

You can use one of the following options to create a virtual media:

Name	Description
Create Image	Allows you to create an ISO image. Drag and drop files or folders in the Create Image dialog box; these files or folders are converted to an ISO image. You can use the **Download ISO Image** button to save the ISO image to your local machine. **Note** Create Image option is not available in Safari browser.
vKVM-Mapped vDVD	Opens the **Map Virtual Media - CD/DVD** dialog box, which allows you to select an ISO image from your local computer and map the drive.

Name	Description
vKVM-Mapped vHDD	Opens the **Map Virtual Media - Removable Disk** dialog box, which allows you to select an ISO image from your local computer and map the drive.
vKVM-Mapped vFDD	Opens the **Map Virtual Media - Floppy Disk** dialog box, which allows you to select an ISO image from your local computer and map the drive.
CIMC-Mapped vDVD	Opens the **Map Virtual Media - CD/DVD** dialog box, which allows you to select an ISO image from your local computer and map the drive. It also allows you to save, edit, and delete mappings. Refer Table 2: Add New Mapping Dialog Box, on page 17.
CIMC-Mapped vHDD	Opens the **Map Virtual Media - CD/DVD** dialog box, which allows you to select an ISO image from your local computer and map the drive. It also allows you to save, edit, and delete mappings. Refer Table 2: Add New Mapping Dialog Box, on page 17.

Table 2: Add New Mapping Dialog Box

Name	Description
Name field	User defined name of the virtual media.
NFS button	Network File System based mapping.
CIFS button	Common Internet File System based mapping.
HTTP/S	HTTP-based or HTTPS-based mapping.
File Location field	Location of the .iso file in the following format: • *<IP Address or DNS Name>*[:*Port*]/*.iso file path*
Username field	**Note** Available only for **CIFS** and **HTTP/S** based mappings. The username, if any.
Password field	**Note** Available only for **CIFS** and **HTTP/S** based mappings. The password for the selected username, if any.

Name	Description
Mount Options field	**Note** Available only for **CIFS** and **NFS** based mappings. The selected mount options. • NFS—For NFS, either leave the field blank or enter one or more of the following: • wsize=VALUE • vers=VALUE • timeo=VALUE • retrans=VALUE • retry=VALUE • rsize=VALUE • For CIFS, either leave the field blank or enter one or more of the following: • nounix • noserverino • sec=VALUE • vers=VALUE
Auto-remap check box	Cisco IMC automatically remaps the device when the host system ejects the media.
Stored vMedia button	Opens an additional area on the right to select stored vMedia from the respective list.
Save button	Saves the vMedia.
Map Drive button	Saves and maps the mounted vMedia.
CD/DVD panel	Provides a list of stored vMedia. If you are mapping using **CIMC-Mapped vDVD** option, then you can also edit or delete any vMedia from this list.
Removable Disk panel	Provides a list of stored vMedia. If you are mapping using **CIMC-Mapped vHDD** option, then you can also edit or delete any vMedia from this list.

What to do next

Update and activate the firmware.

Updating and/or Activating the Firmware

Before you begin

Ensure that the ISO file is ready.

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 update, choose the physical or externally connected CD/DVD device and then press **Enter**.
- For remote update choose one of following where you have mounted the ISO image:
  - Cisco vKVM-Mappred vDVD
  - UEFI: CIMC-Mapped vDVD
  -

Step 3 After the HUU boots, **Cisco End User License Agreement** (EULA) appears, read the EULA and click **Accept** to continue.

Step 4 You can now update the firmware for components or drives using the following options:

- To update and/or activate all components and drives with single click, perform Step 5.
- To update and/or activate specific components and drives, perform Step 6.

Note Ensure that **Advanced Mode** is enabled.

Step 5 Click **Update & Activate**.

In the **Update-activate All** dialog box, check:

- **Exclude Persistent Memory** to exclude the persistent memory from update.
- **Exclude Storage Drives** to exclude the drives from update.
- **Power cycle to activate** to automatically reboot the server after update.

HUU updates all the applicable firmware and reboots the server (if **Power cycle to activate** option was checked) or waits for you to reboot server. Updated firmware are activated on next reboot.

Step 6 To update the firmware for specific components and drives, use the checkbox against each component or drive to select it.

In **Update-activate Selected Components** dialog box, check:

- **Exclude Persistent Memory** to exclude the persistent memory from update (if persistent memory are selected).
- **Exclude Storage Drives** to exclude the drives from update (if storage drives are selected).
- **Power cycle to activate** to automatically reboot the server after update.

HUU updates all the applicable firmware and reboots the server (if **Power cycle to activate** option was checked) or waits for you to reboot server. Updated firmware are activated on next reboot.

Alternatively, after selecting the desired components and drives, you can select **Update** or **Activate** from **More Actions** drop-down list.

Viewing Last Updated Firmware Information

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 update, choose the physical or externally connected CD/DVD device and then press **Enter**.
- For remote update choose one of following where you have mounted the ISO image:
  - Cisco vKVM-Mappred vDVD
  - UEFI: CIMC-Mapped vDVD
  -

Step 3 After the HUU boots, **Cisco End User License Agreement** (EULA) appears, read the EULA and click **Accept** to continue.

Step 4 You can now update the firmware for components or drives using the following options:

Step 5 From the home page, click the **Verify Last Update** tab.

You can view the firmware update history.

CHAPTER 4

Updating the Firmware on a Cisco UCS C-Series Server Using the Non-Interactive HUU (NI-HUU)

Overview

Non Interactive Host upgrade utility or NI-HUU is an application that is used to update firmware on Cisco C-Series servers. With the Multi server NI-HUU, you can update multiple C-Series servers using scripts simultaneously. To use this feature there are tools available for Linux.

Pre-Requisite

Ensure that you have the following installed:

1. Python version 3.x
2. Python-multiprocessing package
3. Pycrypto-2.6

Linux Tool and Commands

This is a python based utility. This utility can be used to update multiple C-Series servers from a Linux host machine simultaneously. The usage of the utility is as follows:

`Usage: update_firmware.py` ***`[options]`***

The parameters for this utility can be given from the command line or in a configuration file.

Table 3: Options

Command	Description
--version	Shows the version number of the program and exit.
-h, --help	Show this help message and exit

Table 4: Single Server Options

Command	Description
-a a.b.c.d, --address=a.b.c.d	CIMC IP address
-u USERNAME, --user=USERNAME	Username of the CIMC admin user
-p PASSWORD, --password=PASSWORD	Password of the CIMC admin user
-q SKIPMEMORYTEST, --skipMemoryTest=Enabled/Disabled	Skip Memory Test Feature can be either Enabled or Disabled
-m ucs-c240-huu-146.iso, --imagefile=ucs-c240-huu-146.iso	HUU iso image file name
-i a.b.c.d, --remoteshareip=a.b.c.d	IP address of the remote share
-d /data/image, --sharedirectory=/data/image	Directory location of the image file in remote share
-t cifs/nfs/www, --sharetype=cifs/nfs/www	Type of remote share
-r REMOTESHAREUSER, --remoteshareuser=REMOTESHAREUSER	Remote share user name
-w REMOTESHAREPASSWORD, --remotesharepassword=REMOTESHAREPASSWORD	Remote share user password
-y COMPONENTLIST, --componentlist=COMPONENTLIST	Component List
-f LOGFILE, --logrecordfile=LOGFILE	Log file name where log data is saved
-b CIMCSECUREBOOT, --cimcsecureboot=CIMCSECUREBOOT	Use CimcSecureBoot. Default is NO. Options yes/no
-k CMCSECUREBOOT, --cmcsecureboot=CMCSECUREBOOT	Use CmcSecureBoot. Default is NO. Options yes/no
-M MOUNTOPTION, --mountOption=MOUNTOPTION	Use mountOption in case of CIFS share to specify the security option
-R REBOOTCIMC, --reboot=REBOOTCIMC	Reboot CIMC before starting update. Options yes/no
-T UPDATETIMEOUT, --timeoutalue=UPDATETIMEOUT	Timeout Value for update

Command	Description
-o UPDATESTOPONERROR, --stopOnError=UPDATESTOPONERROR	Use this option if you want to stop the firmware update once an error is encountered?
-v UPDATEVERIFY, --updateverify=UPDATEVERIFY	Use this option to verify update after reboot
-S USESECURE, --Secure=USESECURE	Use HTTPS. Default is yes. Options yes/no

Table 5: Multiple Server Update Options

Command	Description
-c CONFIGFILE, --configfile=CONFIGFILE	Name of the file with the list of CIMC IP address and other data
-l LOGFILE, --logfile=LOGFILE	Log file name where the log data will be saved
-s USESECURE, --secure=USESECURE	Use HTTPS. Default is yes. Options yes/no
-e INFILE, --encrypt=INFILE	Public key file.
-g, --generatekey	Generate public and private keys
-j, --displayComponentList	Display List of component
-V, --Version	Display version.

Sample Configuration

```
#--------------START CNF--------------------------
#
# Use this flag use_http_secure to toggle betwwen https and http protocol
use_http_secure=yes
# Firmware update should complete within this many minutes. This value will be
# sent along with the firmware update XML request to the CIMC
update_timeout=60
graceful_timeout=3
doForceDown=yes
# Should the firmware update process stop the update once an error is encountered?
update_stop_on_error=no
# Is it required to verify the update by rebooting to the same HUU image after the update
# gets completed?
update_verify=no
# Do you wish to secure Cimc Boot.Use this flag use_cimc_secure.
use_cimc_secure=no
# Do you wish to secure Cmc Boot.Use this flag use_cimc_secure.
use_cmc_secure=no
# Feature is used for skip Memory Test and it reduce the boot time. It support Enabled or
Disabled options.
#skipMemoryTest=Disabled
# List of components to be updated. Check the HUU release note for the list of
# supported components. Multiple components should be comma separated.
update_component=I350
#update_component=9266-8i, BIOS, CIMC, I350
#update_component=all
#update_component=HDD
```

```
#update_type=immediate
#update type can be either delay for a delayed firmware update upon host reboot or immediate,

to start firmware update

#reboot CIMC before Update
reboot_cimc=no
# IP address of the remoted share (cifs/nfs/www) holding the HUU image for booting
# for www share ip address can be given as http://<IPAddr>, https://<IPAddr> or <IPAddr>
remoteshareip=10.104.255.254
# Directory within the share where the HUU image is being kept
sharedirectory=/CIFSShare
# Type of share (nfs/cifs/www)
sharetype=cifs
# Username of the remote share to login to
remoteshareuser=username
# Password corresponding to the remote user
remotesharepassword=password
#Optional mount parameter for CIFS share only. Provide "ntlm,vers=2.0" for CIFS server
version 2.0
(SMB protocol version), default supported version is 3.0
#mountOption=ntlm
#If the running CIMC version is 4.2.2a and above, please provide "ntlmssp or ntlmv2,vers=2.0".
#mountOption=ntlmv2,vers=2.0 or
#mountOption=ntlmssp,vers=2.0

# Password file for remoteshare. If this option is provided, then the above option
(remotesharepassword) should not be given
#remoteshare_passwordfile=/home/arunven/Python_Script/python_script_old/Pyrhon_loop/CRYPTO/remshare.pass

#Common CIMC password --> The password provided below along with CIMC information will be
ignored.
#cimc_password_file=/home/arunven/Python_Script/python_script_old/Pyrhon_loop/CRYPTO/cimc.pass


# Enter the list of CIMC ip addresses where the firmware needs to be updated
address=10.104.255.180, user=cimc_user, password=cimc_password, imagefile=huu.iso

#--------------------------END CNF-------------------------
```

Save this to a file (example config.in) and use the following command:

```
./update_firmware.py -c config.in
```

Canceling a Delayed Update

The same configuration file, which was used for server firmware update, has to be passed with details of all the servers where the update has to be canceled.

Note Firmware update cancel request is to be sent only in delayed firmware update and when update has not started to avoid corruption of firmware.

```
./update_firmware.py cancel -c config.in
```

A sample config file multiserver_config is also available in the SVN location.

This utility assumes that the Python interpreter is installed at `/usr/bin/`. In case the Python interpreter is installed at some other location, this utility can also be invoked as follows:

```
/usr/location/python update_firmware.py -c config.in
```

This utility will connect to the CIMC(s) mentioned in the configuration file and boot the host into the mentioned HUU iso. On booting the HUU ISO will detect that a non-Interactive update needs to be done. HUU completes the update and send the results to the CIMC(s), which is responded back to the python utility to be displayed. If a **Verify** option is also mentioned in the Python utility configuration file, the host reboots in HUU and complete the verification.

Encrypting Passwords

Generating Public and Private Keys

This utility allows users to generate encrypted passwords and make use of them. To generated public and private keys use **-g** option.

Example:

```
./update_firmware.py -g
```

This option prompts for a passphrase for the keys. Press **Enter** if you do not want to provide the passphrase. The output of this command are the following two files:

- Private key file—keys.pem
- Public key file—keys.pub

Generating Encrypted Passwords

To generate encrypted passwords use the **-e** option. This also prompts for passphrase. You must enter the passphrase provided during key generation and the TEXT to be encrypted. This TEXT is the password. This command generates a file containing the encrypted password. The parameter for the option **-e** is the public key file.

Example:

```
./update_firmware.py -e keys.pub
```

Encrypted password file—password.key

You must rename it and save it. You need to generate different encrypted password files for Remote Share Password and CIMC passwords, if they are different from each other.

Using the Encrypted Password Files

Only configuration file can make use of these encrypted passwords. There are two options in the configuration file using which you can use to provide the encrypted password files for CIMC and Remote Share passwords.

- remoteshare_passwordfile=<File Path>
- cimc_password_file=<File Path>

Password file for remoteshare—If this option is provided, then the above option should not be given

```
remoteshare_passwordfile=/home/arunven/Python_Script/python_script_old/Pyrhon_loop/CRYPTO/remshare.pass
```

Common CIMC password—The password provided below is ignored

```
cimc_password_file=/home/arunven/Python_Script/python_script_old/Pyrhon_loop/CRYPTO/cimc.pass
```

Note Once you use the **cimc_password_file** option all the CIMC(s) mentioned in the configuration use this common file.

When you run the `update_firmware.py` script to start the update, it prompts for the passphrase that you had provided during the key generation.