

Common Tips in UCS Firmware Management

Document ID: 110475

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Network Diagram
- Conventions

Main Task

1. Download Firmware from Cisco.com
- 2.1 Firmware Management with GUI
- 2.2 Firmware Management with CLI

Verify

Troubleshoot

Related Information

Introduction

This document presents some common tips to simplify your daily firmware management process.

Prerequisites

Requirements

Cisco recommends that you:

- Have a working knowledge of Cisco UCS Server Blade software and hardware.
- Be familiar with the UCS manager GUI.
- Understand the impact and implications of the different commands described in this document
- Be familiar with the UCS components and topology. Refer to the diagram for a typical solution

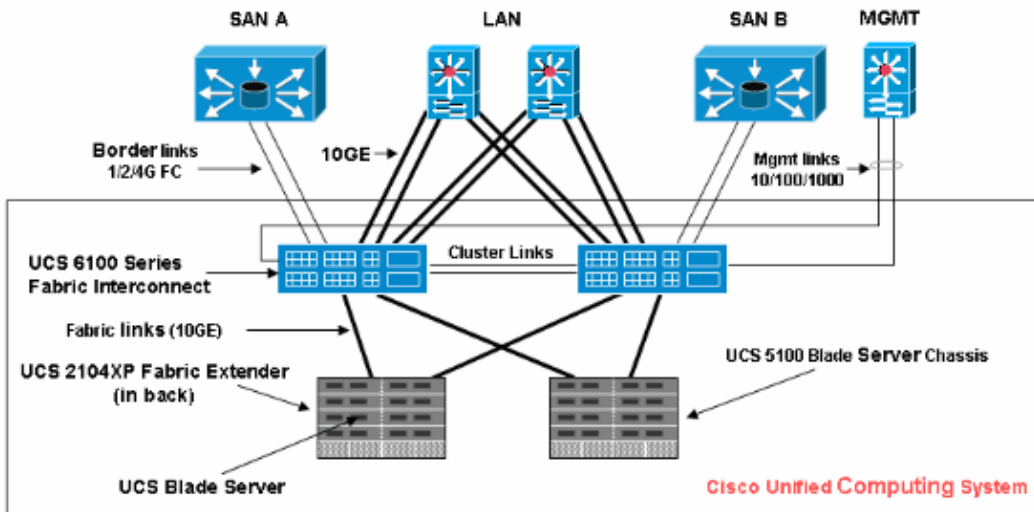
Components Used

The information in this document is based on Cisco UCS.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a default configuration. If your network is live, make sure that you understand the potential impact of any command.

Network Diagram

A typical Cisco UCS topology looks something like this:



Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Main Task

1. Download Firmware from Cisco.com

Complete these steps:

1. Navigate to the SW Center Homepage and select a Product Category.



2. Choose a product from the hierarchical tree that appears.

Download Software

1 Select Product

2 Select Software Type

3 Select Software

4 Download

[Unified Computing](#)

Select a Product

Search for a Product on this page:

[Expand all](#) | [Close all](#)

- [-] Cisco UCS 6100 Series Fabric Interconnects
- [-] Cisco UCS 5100 Series Blade Server Chassis
- [-] Cisco UCS 2100 Series Fabric Extenders
- [-] Cisco UCS B-Series Blade Servers
- [-] Cisco UCS Manager
- [-] Cisco Unified Computing System
- [-] Cisco Unified Computing System Adapters

3. Select a Software Type if multiple Software Types exist for the product you selected.

The screenshot shows the Cisco UCS Manager interface. The 'Firmware Management' tab is active, and the 'Installed Firmware' sub-tab is selected. A red arrow points to the 'Download Firmware' button, which is circled in red. Other buttons like 'Update Firmware' and 'Activate Firmware' are also circled. The table below displays the firmware details for the selected components.

Name	Running Ver...	Startup Ver...	Backup Ver...	Update St...
UCS Manager	1.3(1c)	1.3(1c)	N/A	N/A
Chassis				
Chassis 1				
IO Modules				
IO Module 1	1.3(1c)	1.3(1c)	1.2(1b)	ready
IO Module 2	1.3(1c)	1.3(1c)	1.2(1b)	ready
Servers				
Server 1				
Interface Cards				
Interface Card 1	1.0(2d)	1.0(2d)	1.0(2d)	ready
BIOS	S5500.86B.1.1...	S5500.86B.1.1...	N/A	N/A
CIMC Controller	1.3(1c)	1.3(1c)	1.0(2d)	ready
Server 2				
Server 3				
Server 4				

4. Click the Image Name, and the details for that image appear with an option to download.

Download Software

1 Select Product > 2 Select Software Type > 3 Select Software > 4 Download

[Unified Computing](#) > [Cisco UCS 2104XP Fabric Extender](#) > [Unified Computing System \(UCS\) Complete Software Bundle](#) > [1.0.1e](#)

Release 1.0.1e Software

Search Release:

[Expand all](#) | [Close all](#)

- Latest Releases
 - [1.0.1e](#)
- All Releases
 - 1

[Release Notes for UCS 1.0\(1e\)](#)

Sort By: File Name File:

[ucs-k9-bundle_1.0.1e.bin](#)
 Release Date: 20/Jul/2009
 A bundle including all UCS software upgradable through Manager
 Size: 257944.24 KB (264134892 bytes)

5. Click **Image.bin**. You must accept the standard Cisco End User License Agreement (EULA).

Once you accept the EULA, the download begins.

Conditions

1. Cisco software images are subject to United States (U.S.) national security, foreign policy, anti-terror

I agree to secure Cisco software images in a manner that prevents unauthorized access or transfer. Ce regarding compliance with U.S. use, export, re-exports, and transfer laws may be found at: <http://www.bis.doc.gov/ComplianceAndEnforcement/ListsToCheck.htm>

I shall not electronically or physically transfer Cisco software images to any unauthorized persons, cou U.S. and any local governments.

2. I am not on any of the following U.S. denied persons lists:

- [Table of Denial Orders](#) (U.S. Department of Commerce)
- [Specially Designated Nationals List](#) (U.S. Department of Treasury, Office of Foreign Assets Con
- [Debarred List](#) (U.S. Department of State)

3. I agree to abide by all [export, import, use](#), and development and/or re-export laws in the country in w

4. I agree to [contact Cisco's Export Compliance and Regulatory Affairs group](#) if I know or have reason to

5. I will not knowingly transfer (physically or electronically) [strong encryption](#) images to [denied persons](#)

6. I will not knowingly transfer (physically or electronically) [strong encryption](#) images to, or for, [governm](#)

2.1 Firmware Management with GUI

Before you perform firmware management, refer to prerequisites for firmware upgrade or downgrade. It is recommended that all firmware management be handled through the GUI.

View Installed Firmware

Complete these steps in order to view installed firmware in UCS through the GUI:

1. Log into Cisco UCS Manager.
2. In the Navigation pane, click the **Equipment** tab.
3. Click the **Firmware Management** tab in the Work pane.
4. Click the **Installed Firmware** tab.

Fault Summary

2 20 20 14

Equipment Servers LAN SAN VM Admin

Filter: All

Equipment

Chassis

Fabric Interconnects

Equipment

Main Topology View Fabric Interconnects Servers

Decommissioned Firmware Management Policies

Installed Firmware Download Tasks Packages Images Faults

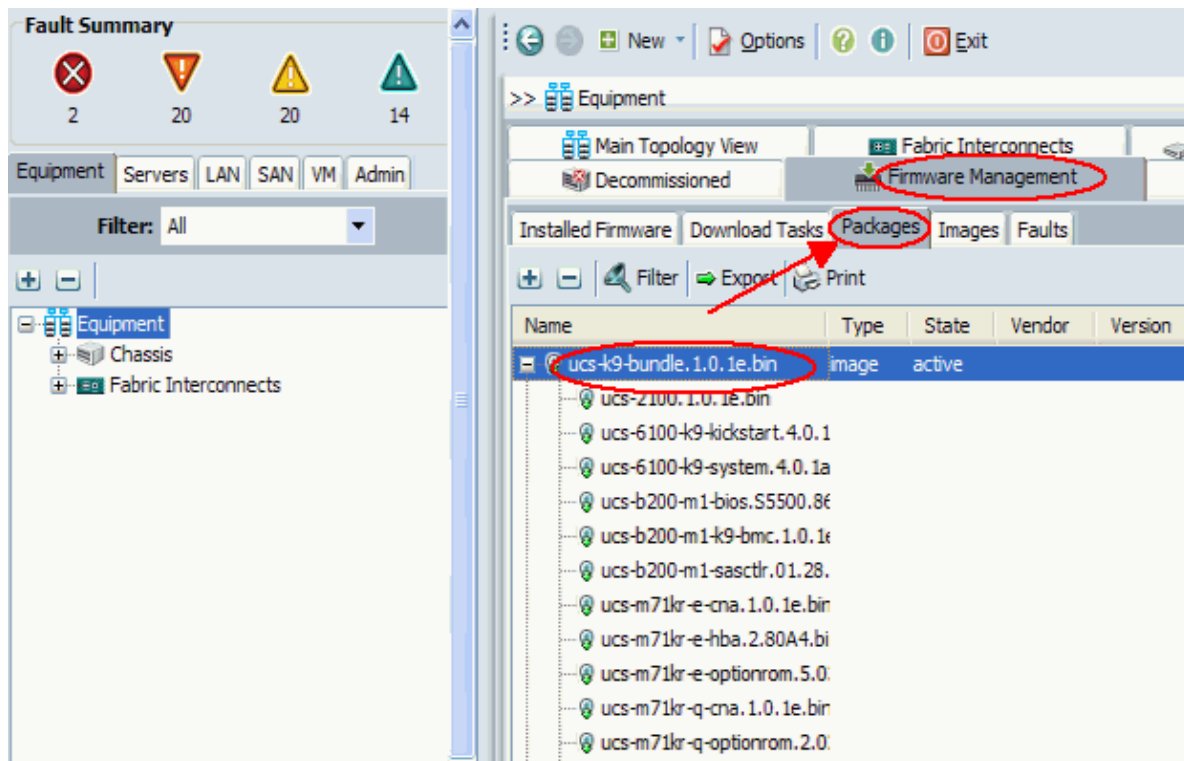
Filter Export Print Download Firmware Update Firmware

Name	Running Ver.	Startup Ver.	Backup Ver.
UCS Manager	1.3(1c)	1.3(1c)	N/A
Chassis			
Chassis 1			
IO Modules			
IO Module 1	1.3(1c)	1.3(1c)	1.2(1b)
IO Module 2	1.3(1c)	1.3(1c)	1.2(1b)
Servers			
Server 1			
Interface Cards			
BIOS	S5500.86B.1....	S5500.86B.1....	N/A
CIMC Controller	1.3(1c)	1.3(1c)	1.0(2d)
Server 2			
Server 3			
Server 4			
Server 5			

Packages

The Packages tab:

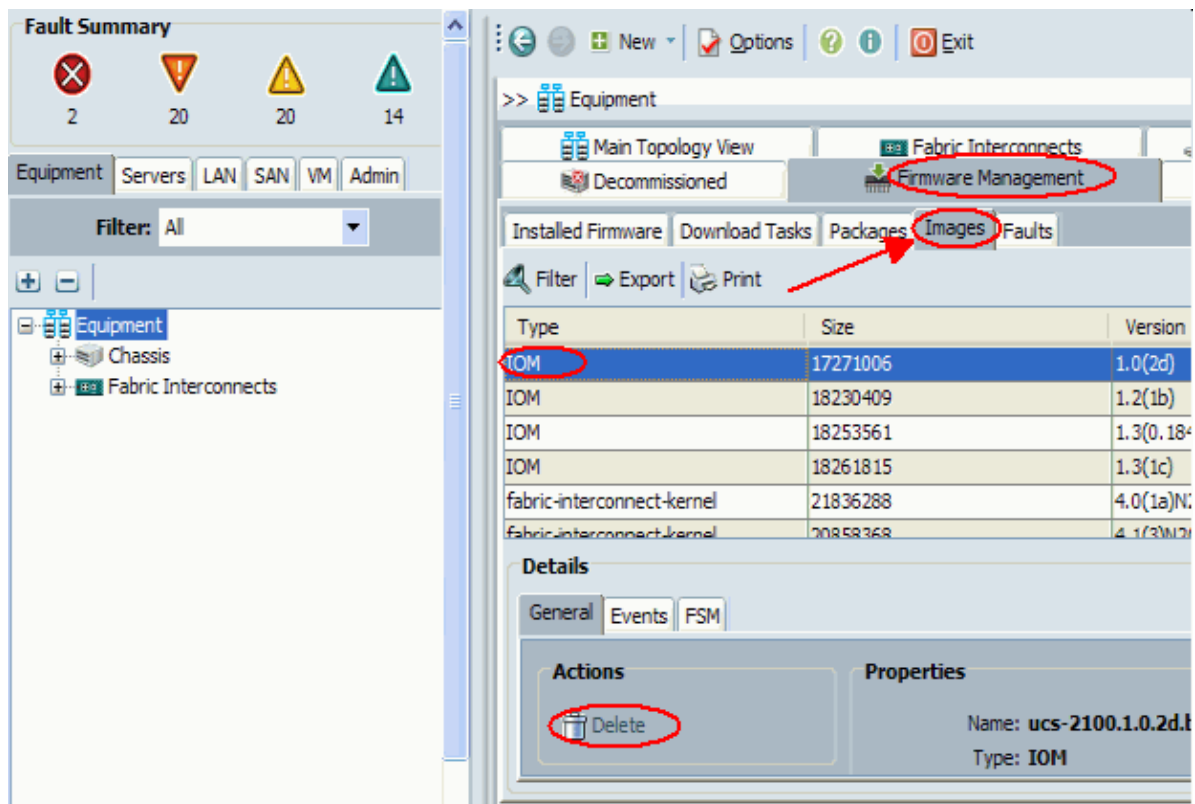
- Keeps track of all packages on the system
- Shows deleted Images
- When all Images are deleted, the package is removed from the tab



Images

The Images tab:

- Allows you to obtain information on individual Images in the package
- Allows you delete the Images
- Once all Images associated to a Package are deleted, the Package is removed from the Package tab



Download Tasks

When you download a firmware image bundle, a Fabric Interconnect needs at least twice as much available space as the size of the firmware image bundle. If the bootflash does not have sufficient space, delete the obsolete firmware, core files, and other unnecessary objects from the fabric interconnect. Before you download a new bundle, check the available free space on the Fabric Interconnects:

1. In the Navigation pane, select **Equipment**.
2. Expand Fabric Interconnects, and select **Fabric Interconnect #**.
3. Click the **General** tab in the Work pane to the right.
4. Expand **Local Storage Information**.
5. Check both fabric interconnects.
6. Delete Images and Packages if space is limited.

The screenshot displays the network management interface. On the left, the 'Fault Summary' panel shows 2 errors, 19 warnings, and 20 alerts. The navigation tree on the left shows 'Equipment' expanded to 'Fabric Interconnects', with 'Fabric Interconnect A' selected. The main work area shows the 'General' tab selected, displaying 'Part Details' with 'Available Memory: 1.482 (GB)' and 'Total Memory: 3.549 (GB)'. Below this, the 'Local Storage Information' section is expanded, showing a table of partitions:

Partition	Size (MB)	Used
bootflash	8,658	24%
opt	1,917	2%
workspace	277	2%

Use the **Download Tasks** tab in order to download firmware. The firmware image name can be between one and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved. The system downloads and unpackages the bundle and distributes it to both fabric interconnects. You can watch the progress on the FSM tab.

Fault Summary

2 (Critical) 20 (Warning)

Equipment Servers LAN SAN VM

Filter: All

Equipment

- Chassis
- Fabric Interconnects
 - Fabric Interconnect A
 - Fabric Interconnect B

>> Equipment

Main Topology View Fabric Interconnects

Thermal Decommissioned **Firmware Management** Policies

Installed Firmware **Download Tasks** Packages Images Faults

Filter Export Print Download Firmware

Filename	Remote Path	Transfer State	FSM Status
ucs-k9-bundle.1.3.1i.bin		downloading	DownloadLocal

Details

General Events FSM

Actions

- Delete
- Restart Download

Properties

Protocol: FTP TFTP SCP SFTP

Server: _____

Filename: **ucs-k9-bundle.1.3.1i.bin**

Remote Path: _____

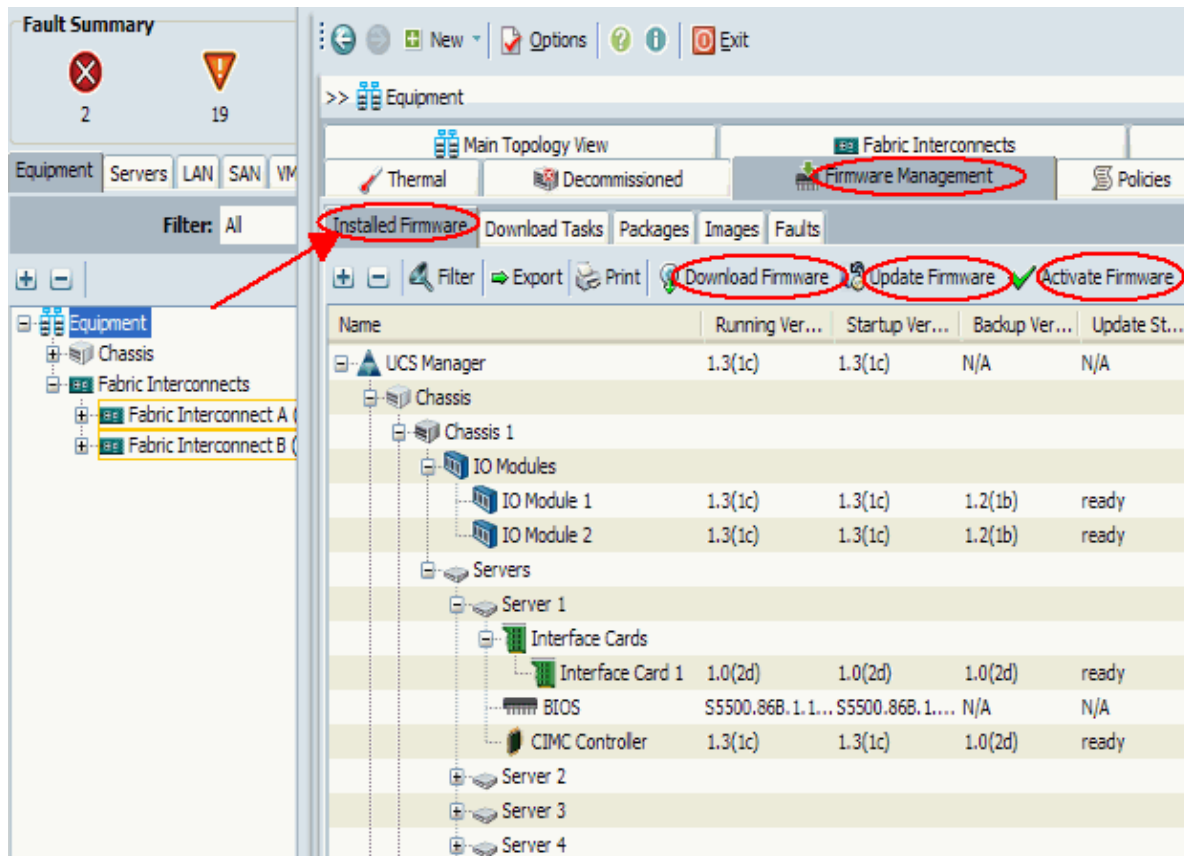
Status: _____

Transfer State: **downloading**

Downloaded Image Size (KB): **0**

Progress Status: **2%**

From this screen, you can download, update, and activate firmware.



2.2 Firmware Management with CLI

Complete these steps in order to view installed firmware in UCS through the CLI:

1. Log into Cisco UCS through the CLI.
2. Issue the **scope system** command.
3. Enter the **show firmware expand** command.

```

View Installed Firmware
F340-31-17-FI-A#
F340-31-17-FI-A# scope system
F340-31-17-FI-A /system # show firmware expand
UCSM:
  Running-Vers: 1.0(1e)
  Activate-Status: Ready

Fabric Interconnect A:
  Running-Kern-Vers: 4.0(1a)N2(1.1e)
  Running-Sys-Vers: 4.0(1a)N2(1.1e)
  Startup-Kern-Vers: 4.0(1a)N2(1.1e)
  Startup-Sys-Vers: 4.0(1a)N2(1.1e)
  Act-Kern-Status: Ready
  Act-Sys-Status: Ready
  Bootloader-Vers: v1.2.0(06/19/08)

```

scope firmware is a useful CLI command that allows you to:

- Delete
- Download
- Scope to download tasks

- Show download tasks, event, fsm, image, and package

Image update and activation is done from the scope of individual components

```
scope firmware
F340-31-17-FI-A#
F340-31-17-FI-A# scope firmware
F340-31-17-FI-A /firmware # ?
  delete      Delete managed objects
  download    Download
  exit        Exit from command interpreter
  scope       Changes the current mode
  show        Show system information

F340-31-17-FI-A /firmware #
```

Verify

There is currently no specific verification information available for this configuration

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- [Technical Support & Documentation – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2014 – 2015 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Aug 10, 2010

Document ID: 110475
