

What You Make Possible



UCS Firmware Management Architecture

BRKCOM-2008

Legal Disclaimer

Many products and features described herein remain in varying stages of development and will be offered on a when-and-if-available basis.

This roadmap is subject to change at the sole discretion of Cisco and Cisco will have no liability for delay in the delivery or failure to deliver any of the products or features set forth in this document.

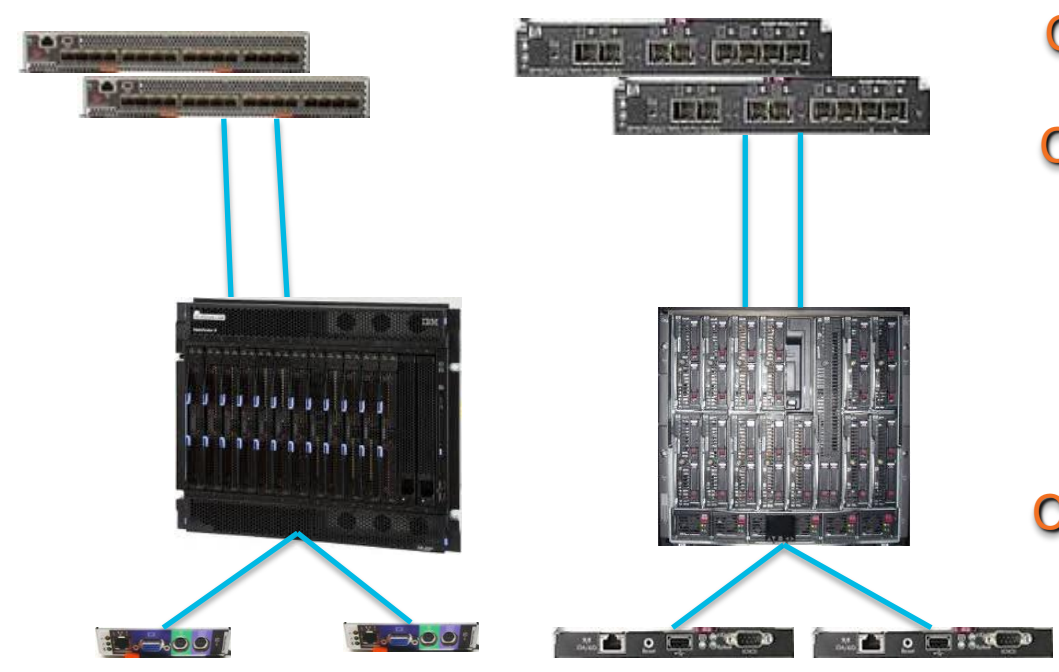
Agenda

- Firmware Component Comparison
- UCS Firmware Management Overview
- UCS Firmware Guidelines and Best Practices
- UCS Firmware Upgrade/Downgrade Sequence
- UCS Firmware Automation

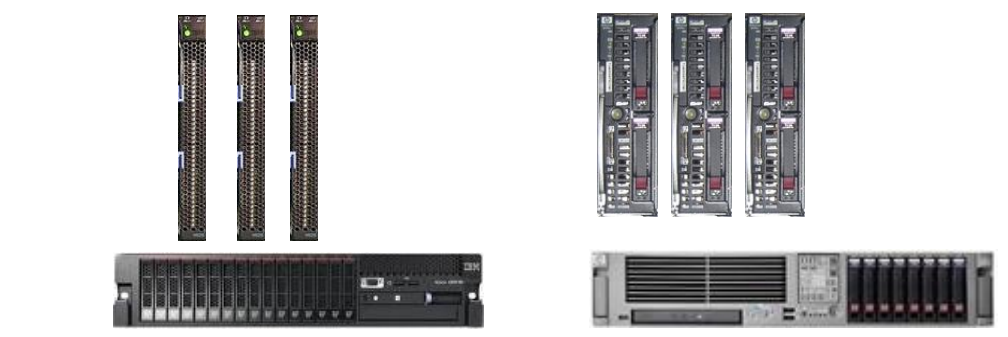
Firmware Component Comparison



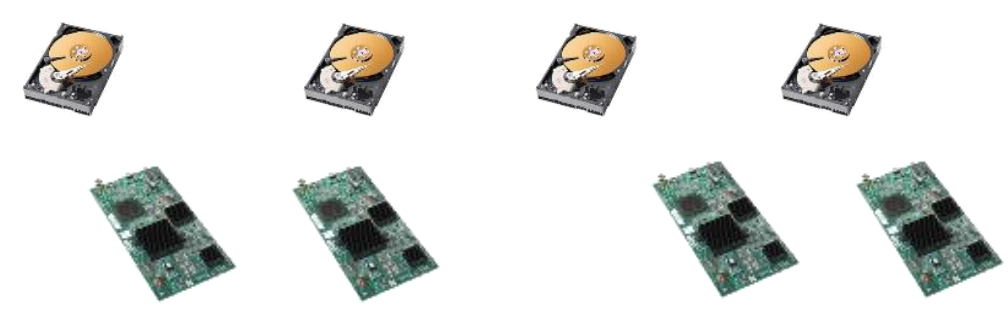
Endpoints for Legacy Compute



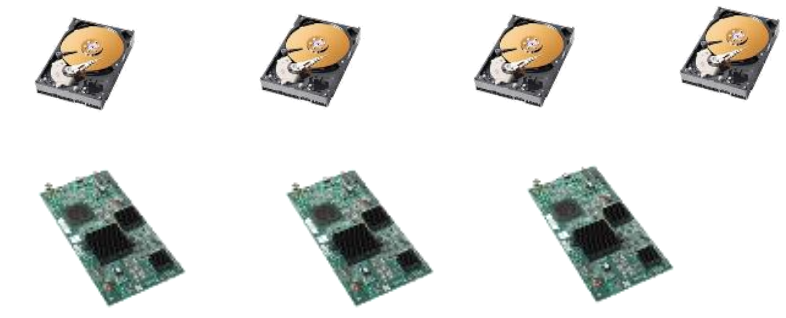
Chassis Based Ethernet Switch
Chassis Based FC Switch
Each chassis is independent
Chassis Mgmt Controller Firmware



Blade BIOS and BMC Firmware
Rackmount Server Firmware



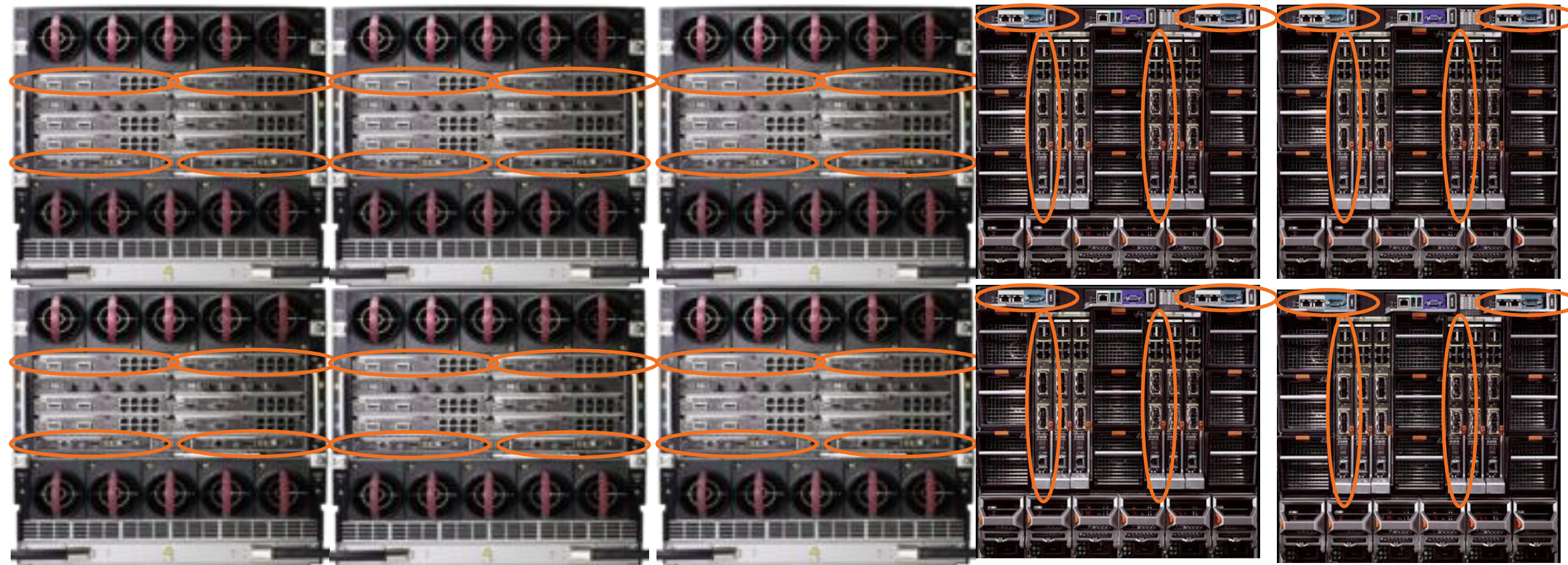
RAID and Disk Firmware
Adapter Firmware



Legacy Firmware Touch Points

160 Server Configuration

- 10 Individual Chassis with separate inter-dependent endpoints
- On board chassis management modules 2 (two) per chassis
- Minimum- pair (2) of on board switches (up to 8) per chassis
- 40 infrastructure touch points

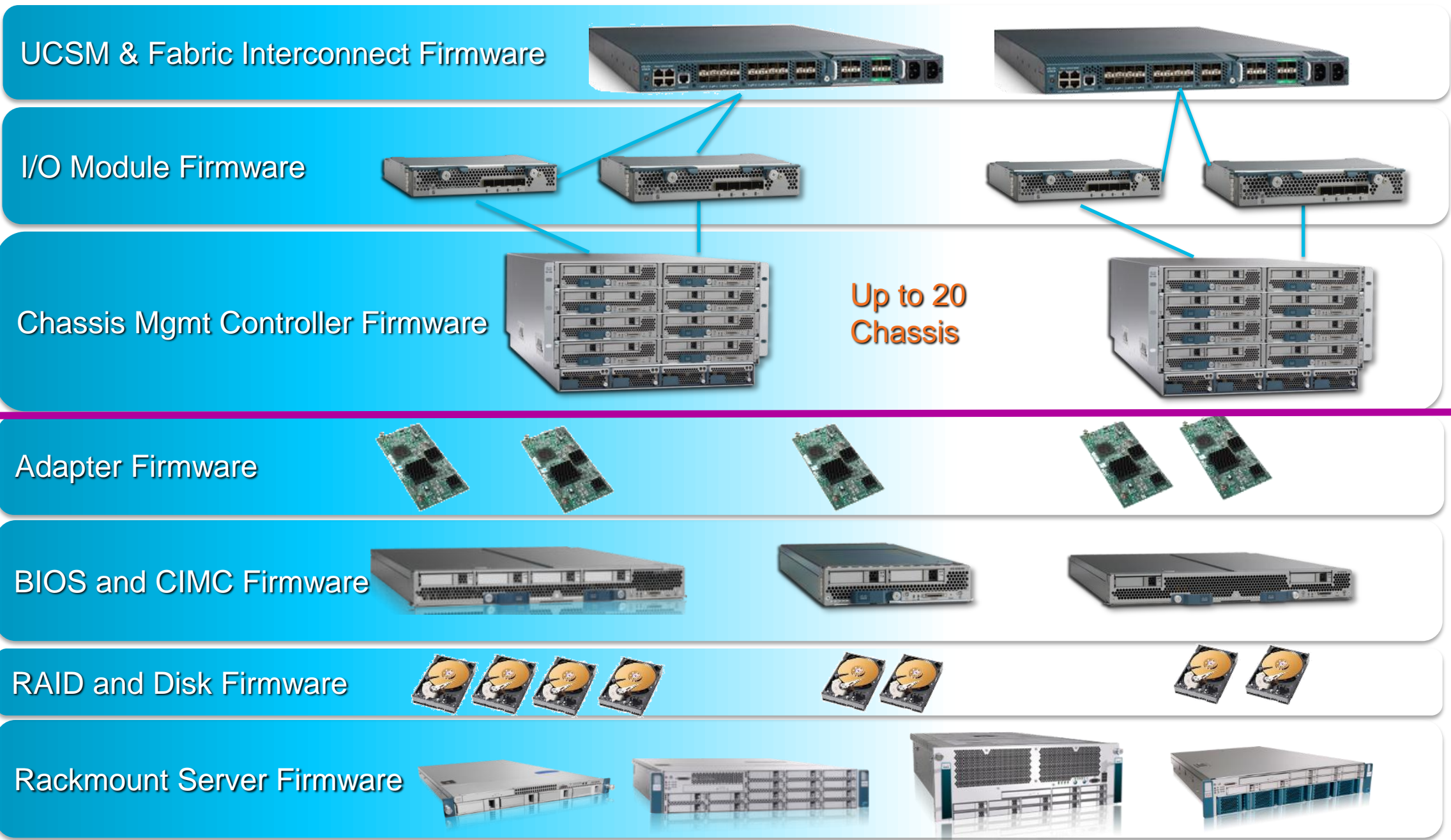


Legacy Firmware Touch Points

Endpoint Disruption

- Host Management Controllers
 - Local for each host
 - No host data plane disruption
- On board chassis administration modules
 - Active/Passive pair PER chassis
 - No host data plane disruption
- Chassis Ethernet/FC modules
 - Data plane I/O modules
 - Must be updated in precise order to prevent data plane connectivity loss
 - Typically a separate execution tool to run updates
- Host Servers
 - Updates are pushed locally through multiple tools
 - Requires host to reboot in order to activate firmware

Endpoints for UCS Domain



Infrastructure Bundle

Server Bundles:

- B-Series Blade Server Bundle
- C-Series Rack-Mount Server Bundle

- Easy change of firmware on servers from one version to another
- Mapping of applications with specific firmware through service profiles
- One step change of firmware for multiple servers

Legacy Firmware Management Complexity

Examples for non Cisco UCS

- Multiple software tools and deployment methods required to update infrastructure and component firmware
- Complex firmware methodology, some best practice implementation guides are near 200 pages long
- Many infrastructure endpoints to manage
- Hardware must be 'touched' to manage firmware across Data Centre
- No policy driven approach
- Requires an IP based network for one to many updates
- Complex authentication steps

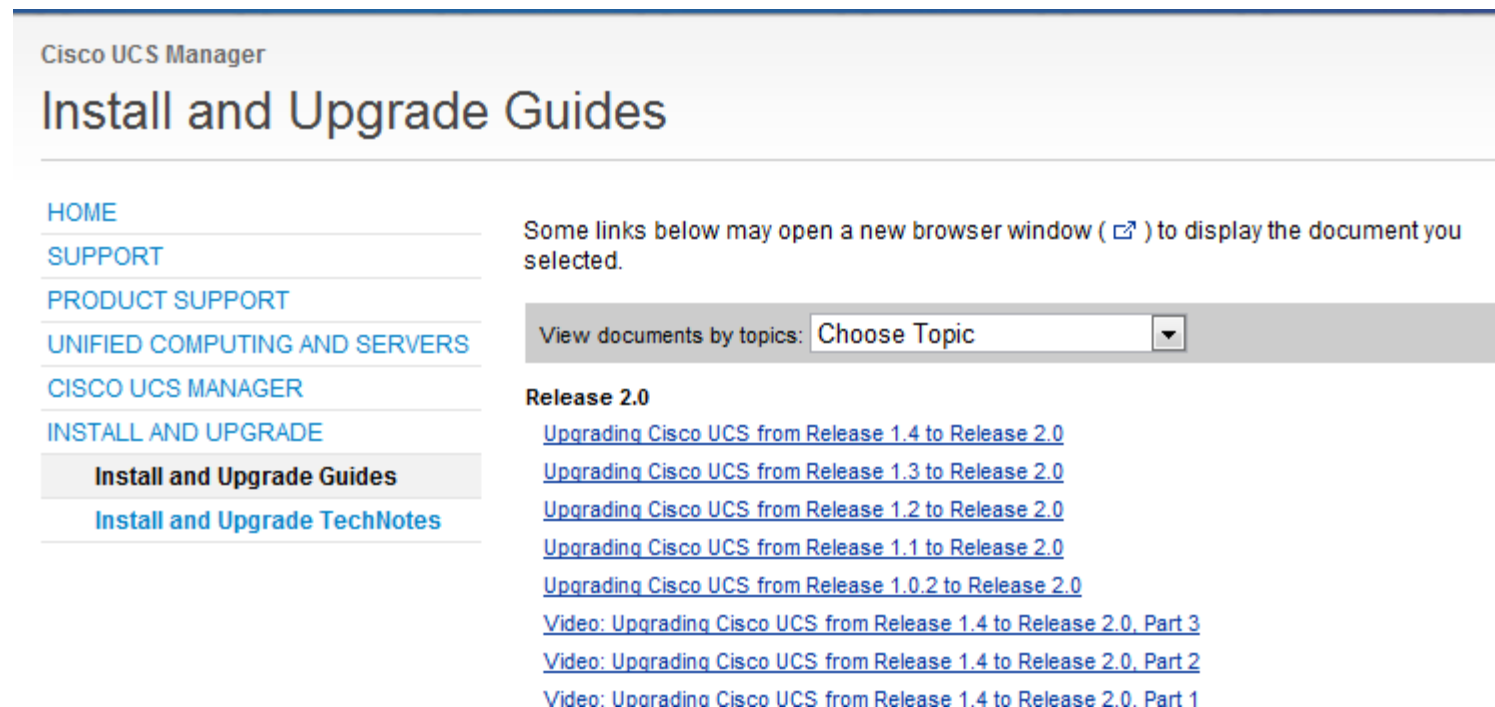
Firmware Management Overview



Documentation and Release Notes

Where to Find Update Documentation


- Important to review the release notes for the appropriate version of FW upgrading or downgrading to.
- Upgrade Guides and videos located at:
http://www.cisco.com/en/US/products/ps10281/prod_installation_guides_list.html



Cisco UCS Manager

Install and Upgrade Guides

HOME
SUPPORT
PRODUCT SUPPORT
UNIFIED COMPUTING AND SERVERS
CISCO UCS MANAGER
INSTALL AND UPGRADE
Install and Upgrade Guides
Install and Upgrade TechNotes

Some links below may open a new browser window () to display the document you selected.

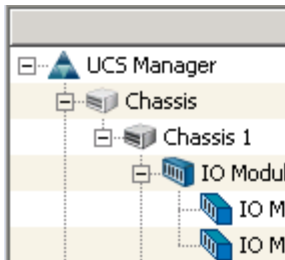
View documents by topics: Choose Topic

Release 2.0

- [Upgrading Cisco UCS from Release 1.4 to Release 2.0](#)
- [Upgrading Cisco UCS from Release 1.3 to Release 2.0](#)
- [Upgrading Cisco UCS from Release 1.2 to Release 2.0](#)
- [Upgrading Cisco UCS from Release 1.1 to Release 2.0](#)
- [Upgrading Cisco UCS from Release 1.0.2 to Release 2.0](#)
- [Video: Upgrading Cisco UCS from Release 1.4 to Release 2.0, Part 3](#)
- [Video: Upgrading Cisco UCS from Release 1.4 to Release 2.0, Part 2](#)
- [Video: Upgrading Cisco UCS from Release 1.4 to Release 2.0, Part 1](#)

Firmware Terminology

Used by UCSM

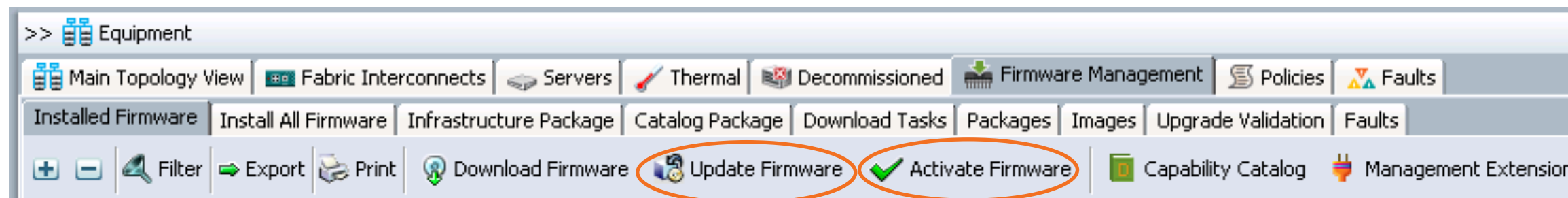


Name	Model	Running Version	Startup Version	Backup Version
UCS Manager		2.1(0.237)	2.1(0.237)	N/A
Chassis				
Chassis 1	Cisco UCS 5108			
IO Modules				
IO Module 1	Cisco UCS 2208XP	2.0(1s)	2.0(1s)	2.0(1s)
IO Module 2	Cisco UCS 2208XP	2.0(1s)	2.0(1s)	2.0(1s)

- Running Version
 - Firmware that is active and in use by an endpoint
- Startup Version
 - Firmware that will be used on next reboot
 - UCSM uses the activate operation to change the startup version
- Backup Version
 - Firmware in secondary slot and not in current use by endpoint
 - Older firmware version stored here
 - Update operation replaces the image in the backup slot

Firmware Management Definition

- Update
 - Copies the firmware to the backup partition on an endpoint
 - Not disruptive
 - Can be done to all devices at the same time
- Activate
 - Firmware in the backup partition is set to active (startup version)
 - Activates the startup version on the endpoint
 - Disruptive
 - Follow specific order according to documentation



Firmware Management - Download

Placing Firmware on the Fabric Interconnect

- Before downloading a new bundle check the available free space on the Fabric Interconnects
- Images stored in dedicated /bootflash partition of Fabric Interconnect
- Delete Images and Packages if space is limited
- Can use multiple methods for downloading firmware to the Fabric Interconnect

- Local
- SCP
- FTP
- SFTP
- TFTP

The screenshot shows the Cisco Unified Computing System Manager (UCSCOMPLAB2) interface. The main content area is titled "Fabric Interconnect A (primary)" and includes several sections:

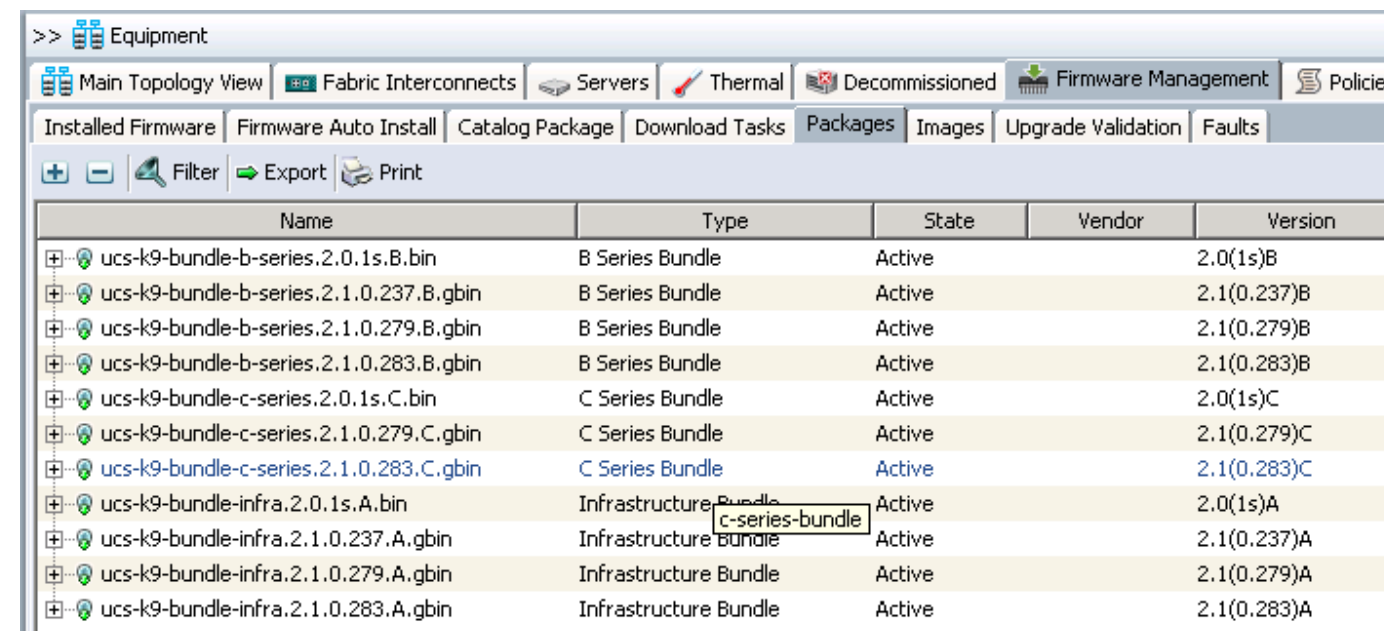
- Fault Summary:** Shows 0 critical, 0 major, 0 minor, and 0 warning faults. Suppression Status is N/A.
- Status:** Overall Status is Operable. Thermal is N/A. Ethernet Mode is End Host. FC Mode is End Host.
- Physical Display:** Shows a visual representation of the hardware with status indicators for Up, Admin Down, Fail, and Link Down.
- Properties:** Name: A, Product Name: Cisco UCS 6248UP, Vendor: Cisco Systems, Inc., PID: UCS-FI-6248UP, Revision: 0, Serial Number (SN): 55115300M4D, Available Memory: 13.881 (GB), Total Memory: 16.232 (GB), Locator LED: checked.
- Part Details:** Section for additional hardware information.
- Local Storage Information:** A table showing the usage of local storage partitions.

Partition	Size (MB)	Used
bootflash	14,669	38%
opt	3,877	2%
workspace	3,852	1%

Firmware Bundles

What is a Bundle?

- Firmware bundles (packages) contain individual endpoint images
- A package is only meant for ease of distribution
- Multiple images are bundled together to form an bundle package
- Images contain endpoint Firmware and BIOS (.bin files)
- Bundles (packages) are logical representations in UCSM
- Bundles (packages) may be removed by deleting all images associated with the bundle













The screenshot shows the UCSM Firmware Management interface. The 'Packages' tab is selected, displaying a table of firmware bundles. The table has columns for Name, Type, State, Vendor, and Version. The bundles listed include B Series Bundles, C Series Bundles, and Infrastructure Bundles for various UCS models and versions.

Name	Type	State	Vendor	Version
ucs-k9-bundle-b-series.2.0.1s.B.bin	B Series Bundle	Active		2.0(1s)B
ucs-k9-bundle-b-series.2.1.0.237.B.gbin	B Series Bundle	Active		2.1(0.237)B
ucs-k9-bundle-b-series.2.1.0.279.B.gbin	B Series Bundle	Active		2.1(0.279)B
ucs-k9-bundle-b-series.2.1.0.283.B.gbin	B Series Bundle	Active		2.1(0.283)B
ucs-k9-bundle-c-series.2.0.1s.C.bin	C Series Bundle	Active		2.0(1s)C
ucs-k9-bundle-c-series.2.1.0.279.C.gbin	C Series Bundle	Active		2.1(0.279)C
ucs-k9-bundle-c-series.2.1.0.283.C.gbin	C Series Bundle	Active		2.1(0.283)C
ucs-k9-bundle-infra.2.0.1s.A.bin	Infrastructure Bundle	Active		2.0(1s)A
ucs-k9-bundle-infra.2.1.0.237.A.gbin	Infrastructure Bundle	Active		2.1(0.237)A
ucs-k9-bundle-infra.2.1.0.279.A.gbin	Infrastructure Bundle	Active		2.1(0.279)A
ucs-k9-bundle-infra.2.1.0.283.A.gbin	Infrastructure Bundle	Active		2.1(0.283)A

Firmware Bundles

Cisco UCS Infrastructure Software Bundle

- Infrastructure Bundle includes the following firmware images
 - Cisco UCS Manager software
 - Kernel and system firmware for fabric interconnects
 - I/O module firmware

<input type="checkbox"/>	 ucs-k9-bundle-b-series.2.1.0.283.B.gbin	B Series Bundle	Active	2.1(0.2)
<input type="checkbox"/>	 ucs-k9-bundle-c-series.2.0.1s.C.bin	C Series Bundle	Active	2.0(1s)
<input type="checkbox"/>	 ucs-k9-bundle-c-series.2.1.0.279.C.gbin	C Series Bundle	Active	2.1(0.2)
<input type="checkbox"/>	 ucs-k9-bundle-c-series.2.1.0.283.C.gbin	C Series Bundle	Active	2.1(0.2)
<input checked="" type="checkbox"/>	 ucs-k9-bundle-infra.2.0.1s.A.bin	Infrastructure Bundle	Active	2.0(1s)
<input type="checkbox"/>	 ucs-2100.2.0.1s.bin			
<input type="checkbox"/>	 ucs-2200.2.0.1s.bin			
<input type="checkbox"/>	 ucs-6100-k9-kickstart.5.0.3.N2.2.1s.bin			
<input type="checkbox"/>	 ucs-6100-k9-system.5.0.3.N2.2.1s.bin			
<input type="checkbox"/>	 ucs-manager-k9.2.0.1s.bin			

Firmware Bundles

Cisco UCS B-Series Blade Server Software Bundle

- Bundle includes the following Blade firmware images
 - CIMC firmware
 - BIOS firmware
 - Adapter firmware
 - Board controller firmware
 - Third-party firmware images as required
- New bundles may be released between infrastructure bundles to support new hardware.

ucs-k9-bundle-b-series.2.1.0.237.B.gbin	B Series Bundle	Active	2.1(0.237)B
ucs-b200-m1-bios.55500.2.0.2b.0.020120121754.gbin			
ucs-b200-m1-k9-cimc.2.1.0.237.gbin			
ucs-b200-m1-sasctrl.01.32.04.00_06.34.00.00_03.22.			
ucs-b200-m2-bios.55500.2.0.2b.0.020120121754.gbin			
ucs-b200-m3-bios.B200M3.2.0.2b.0.030720121106.gb			
ucs-b200-m3-k9-cimc.2.1.0.237.gbin			
ucs-b200-m3-mrsasctrl.20.10.1-0061_4.29.00_NA.gbir			
ucs-b22-m3-bios.B22M3.2.0.2.10.030820121044.gbin			
ucs-b22-m3-k9-cimc.2.1.0.237.gbin			
ucs-b22-m3-mrsasctrl.20.10.1-0072_4.30.00_NA.gbin			
ucs-b230-m1-bios.B230.2.0.2b.0.030720121455.gbin			
ucs-b230-m1-k9-cimc.2.1.0.237.gbin			
ucs-b230-m1-mrsasctrl.20.10.1-0042_4.24.00_NA.gbir			
ucs-b230-m1-pld.B230100C.gbin			
ucs-b230-m2-bios.B230.2.0.2b.0.030720121455.gbin			
ucs-b230-m2-k9-cimc.2.1.0.237.gbin			
ucs-b230-m2-pld.B230100C.gbin			
ucs-b250-m1-bios.55500.2.0.2c.0.020920121737.gbin			
ucs-b250-m1-k9-cimc.2.1.0.237.gbin			
ucs-b250-m1-pld.111026-111026.gbin			
ucs-b250-m2-bios.55500.2.0.2c.0.020920121737.gbin			
ucs-b440-m1-bios.B440.2.0.2b.0.030720121505.gbin			
ucs-b440-m1-k9-cimc.2.1.0.237.gbin			
ucs-b440-m1-mrsasctrl.12.12.0-0050_3.22.00_NA.gbir			
ucs-b440-m1-pld.B440100C-B4402006.gbin			
ucs-b440-m2-bios.B440.2.0.2b.0.030720121505.gbin			
ucs-b440-m2-k9-cimc.2.1.0.237.gbin			
ucs-b440-m2-pld.B440100C-B4402008.gbin			
ucs-m51kr-b.6.2.15.23.7.1.gbin			

Firmware Bundles

Cisco UCS C-Series Rack Server Software Bundle

- Bundle includes the following firmware images for Rack servers integrated with UCSM
 - CIMC firmware
 - BIOS firmware
 - Adapter firmware
 - Storage controller firmware
- Only used for UCSM integrated C-Series servers

ucs-k9-bundle-c-series.2.0.1s.C.bin	C Series Bundle	Active
ucs-c-lsi-mezz-1064E.1.30.00.00_6.30.00.00_NA.bin		
ucs-c-lsi-mrsas-8708EM2.11.0.1-0030.bin		
ucs-c-lsi-mrsas-926x.12.9.0-0050.bin		
ucs-c-lsi-sasctlr-30813E.1.30.00.00_6.30.00.00_NA.bin		
ucs-c-pci-n2xx-abpci02.5.2.51.15.1.bin		
ucs-c-pci-n2xx-aepci01.2.702.517.6.bin		
ucs-c-pci-n2xx-aipci01.2.1.60.bin		
ucs-c-pci-n2xx-aqpci01.01.01.98.bin		
ucs-c200-bios.C200.1.2.2f.0.112720102041.bin		
ucs-c200-k9-cimc.1.2.2l.bin		
ucs-c250-bios.C250.1.2.2f.0.112820100448.bin		
ucs-c250-k9-cimc.1.2.2l.bin		
ucs-mgmtxt.2.0.1s.bin		
ucs-p81e-vic.2.0.1s.bin		

Firmware Management - Images

Image Maintenance

- Images tab presents information on individual images in the package
- Allows the deletion of the Images
- Once all images associated to a package are deleted, the package will be removed from the Packages tab
- Delete Bundle to remove all image files from Fabric Interconnect

Name	Type	State	Vendor	Version
ucs-k9-bundle-b-series.2.0.1s.B.bin	B Series Bundle	Active		2.0(1s)B
ucs-k9-bundle-b-series.2.1.0.237.B.gbin	B Series Bundle	Active		2.1(0.237)B
ucs-k9-bundle-c-series.2.0.1s.C.bin	C Series Bundle	Active		2.0(1s)C
ucs-k9-bundle-infra.2.0.1s.A.bin	Infrastructure Bundle	Active		2.0(1s)A
ucs-k9-bundle-infra.2.1.0.237.A.gbin	Infrastructure Bundle	Active		2.1(0.237)A

Type	Size	Version
IOM	19223413	2.0(1s)
IOM	21493667	2.1(0.237)
IOR	29842156	2.0(1s)
IOR	34781140	2.1(0.237)
Fat	26066944	5.0(3)N2(2.10.237)
Fat	26002432	5.0(3)N2(2.1s)
Fat	332056168	5.0(3)N2(2.10.237)
Fabric Interconnect System	329063371	5.0(3)N2(2.1s)
Server BIOS	3217944	55500.2.0.1d.0.093020111102
Server BIOS	3217944	55500.2.0.2b.0.020120121754
CIMC	6586168	2.0(1s)
CIMC	6809574	2.1(0.237)
RAID Controller	453103	01.32.04.00 06.34.00.00 03.20.00.00
RAID Controller	453249	01.32.04.00 06.34.00.00 03.22.00.00
Server BIOS	3217944	55500.2.0.1d.0.093020111102
Server BIOS	3217944	55500.2.0.2b.0.020120121754
Server BIOS	16779264	B200M3.2.0.2b.0.030720121106
CIMC	9232142	2.1(0.237)
RAID Controller	4456448	20.10.1-0061 4.29.00 NA
Server BIOS	16779264	B22M3.2.0.2.10.030820121044
CIMC	8124904	2.1(0.237)
RAID Controller	4456448	20.10.1-0072 4.30.00 NA
Server BIOS	2649303	B230.2.0.1c.0.100520111716
Server BIOS	2650840	B230.2.0.2b.0.030720121455
CIMC	6902552	2.0(1s)
CIMC	6986509	2.1(0.237)
RAID Controller	4456448	20.10.1-0042 4.24.00 NA
RAID Controller	4456448	20.10.1-0042 4.24.00 NA

Firmware Guidelines and Best Practices



Firmware Update Guidelines

Configuration Validation Before Upgrading to 2.x

- Ensure that overlapping FCoE VLAN IDs and Ethernet VLAN IDs are not present
 - VLAN configured as the FCoE VLAN for a VSAN cannot carry Ethernet traffic
- Do not use both Fabric Failover AND Host NIC Teaming on the same vNIC
 - May cause connectivity loss when upgrading adapter firmware
- Ensure that iSCSI IQN names are unique for each iSCSI vNIC
 - Only applicable on 2.0(1) upgrades to 2.0(2)
- VLAN 4048 is reserved in release 1.4(1) and higher

Firmware Update Guidelines

Upgrading Endpoints

- Do not perform any server or chassis maintenance during updates
 - Do not remove hardware that contains endpoints
 - Do not perform maintenance on hardware
- Avoid replacing RAID hard disks prior to upgrade
 - Perform any physical disk maintenance after upgrade process is complete
- Update adapters through a host firmware package policy
- Redundant Fabric Interconnects can be updated without disrupting data traffic

Firmware Update Best Practices

Best Practices for Upgrades

- Backup All Configuration from UCSM to a backup file
- Select Ignore Compatibility Check when upgrading
 - Set when performing a direct upgrade to a newer release
 - Ensures that the upgrade can proceed and avoids compatibility issues
- Disable Call Home
 - Ensure that Call Home is off before starting upgrade process
 - Restarts cause events that are identical to service disruptions and component failures to trigger alerts

Firmware Update Best Practices

Best Practices for Upgrades

- Use Host Firmware Package Policies for all host endpoint management for production systems
- Set and use Maintenance Policies to control host outage windows
- Ensure HA State is healthy before updating Fabric Interconnects
- Optional – Administratively shut down uplink Ethernet and FC ports on Fabric Interconnect being updated.
 - Validate operation of Fabric Failover/MPIO on host OS's
 - Prevent any obscure issues on upstream switch devices

Mismatched Firmware Support

Starting with UCS 2.1

- May have Infrastructure and Host server firmware at different levels starting with UCS 2.1 and above
 - Infrastructure will need to be at 2.1
 - Host firmware may be at 2.0(x)
- Support for host firmware levels throughout an entire major release of UCS
 - Ex 2.1 up to 2.1(X) supported; 2.1(x) mix with 2.2(x) not supported
 - Maintenance releases, incremental updates or patch version differences are supported
- Pre-2.1 Firmware levels in a domain must be the same version for support

Firmware Upgrade Outage Impacts

Online or Offline Updates

- Fabric Interconnect upgrade
 - Redundant Fabric Interconnects can failover to other fabrics to keep data plane operational
 - Fabric Interconnect reboots disrupting data plane on corresponding fabric
 - Reboots all I/O modules on corresponding fabric
- UCS Manager upgrades
 - **NO** data plane disruption, can be done online
 - All users logged into UCSM GUI or CLI will be logged out
- CIMC upgrades
 - **NO** data plane disruption can be done online
 - Any activity on KVM/SoL/IPMI is interrupted

Firmware Upgrade Outage Impacts

Online or Offline Updates

- I/O Module firmware upgrade
 - Using Set Startup Version Only, **NO** data plane disruption
 - Corresponding I/O modules reboot only when Fabric Interconnect reboots
 - Data traffic fails over to the other I/O module and data path
- Host firmware upgrade
 - Use Host Firmware Package policies to manage host endpoints
 - Using Maintenance Policy can stage host reboot for later time
 - Host must reboot to activate all endpoint firmware

Firmware Upgrade/Downgrade Sequence



Firmware Upgrade Sequence

Upgrade/Downgrade Procedure

1. Download firmware images
2. Disable Call Home (If enabled)
3. Update CIMC and IOMs – **NO** host OS impact
4. Activate CIMC – **NO** host OS impact
 - Best Practice to use management/host firmware package policy
5. Activate UCSM – **NO** host OS impact

Firmware Upgrade Sequence

Upgrade/Downgrade Procedure

6. Activate I/O Modules – Set Startup Version Only – **NO** host OS impact
7. Activate Subordinate fabric interconnect
8. Verify cluster health / data path has been restored
9. Activate Primary fabric interconnect
10. Update and apply Host Firmware Package Policies
11. Enable Call Home

Firmware Steps

Download Firmware Images

- Before Downloading check available space on Fabric Interconnect
- Delete Images and Packages if space is limited

The screenshot shows the Physical Display of a Cisco UCS Fabric Interconnect. The display is a rack-mounted server with multiple ports. Below the display is a legend: **Up** (green square), **Admin Down** (brown square), **Fail** (red square), and **Link Down** (yellow square).

Properties

Name: **A**
Product Name: **Cisco UCS 6248UP**
Vendor: **Cisco Systems, Inc.** PID: **UCS-FI-6248UP**
Revision: **0** Serial Number (SN): **SSI15300M4D**
Available Memory: **13.635 (GB)** Total Memory: **16.232 (GB)**
Locator LED:

Part Details

Local Storage Information

Filter | Export | Print

Partition	Size (MB)	Used	
bootflash	14,669	20%	
opt	3,877	2%	
workspace	3,852	1%	

Firmware Steps

Download Firmware Images

- To download firmware use the download tab



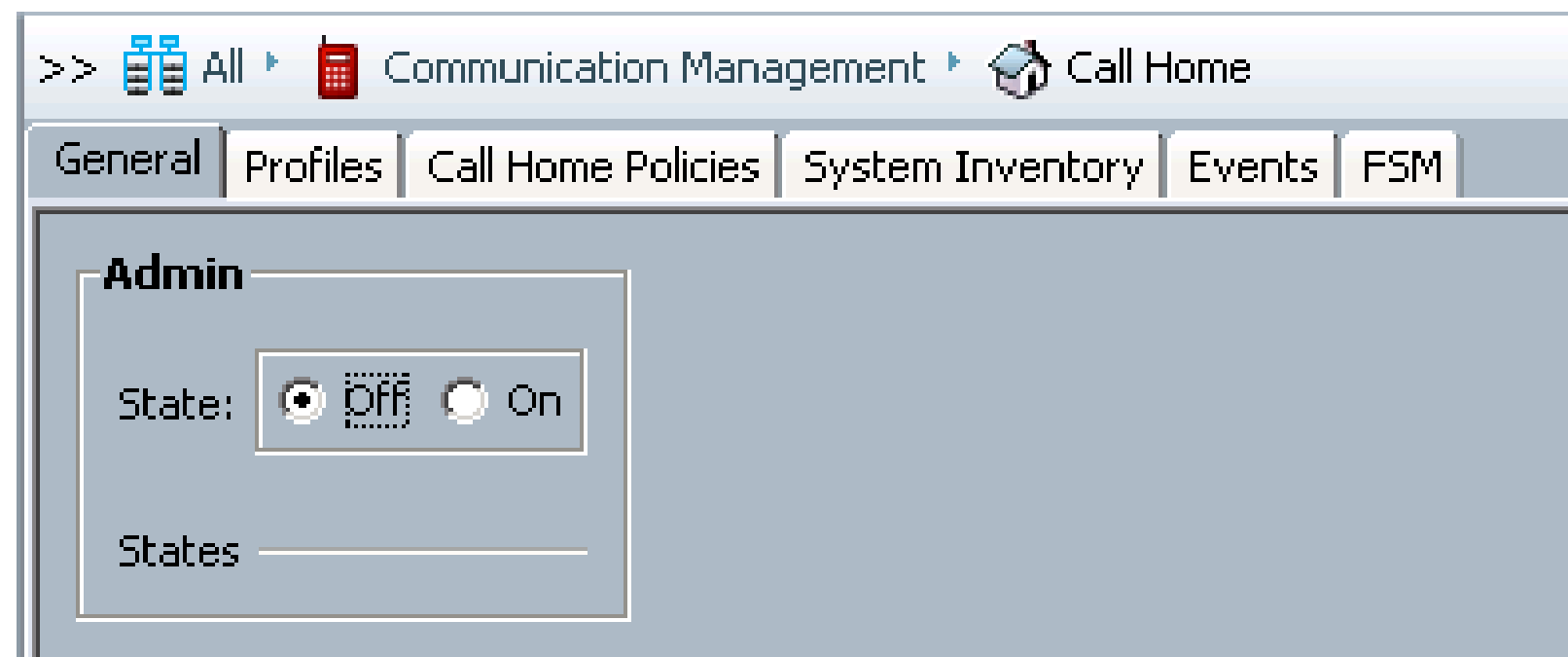
The screenshot shows the 'Download Firmware' dialog box. The 'Location of the Image File' is set to 'Remote File System'. The 'Protocol' is set to 'FTP'. The 'Server' is 'demo.demolab.lab', the 'Filename' is 'ucs-k9-bundle-infra.2.1.0.237.A.gbin', and the 'User' is 'anonymous'. The 'Password' field is masked with asterisks. The 'Remote Path' field is empty.

The screenshot shows the 'Download Firmware' dialog box. The 'Location of the Image File' is set to 'Local File System'. The 'Filename' field contains the path 'Z:\UCS Firmware\DelMar 2.1\ucs-k9-bundle-infra.2.1.0.237.A.gbin' and has a 'Browse' button next to it. The 'Remote File System' option is unselected.

Firmware Steps

Disable Call Home

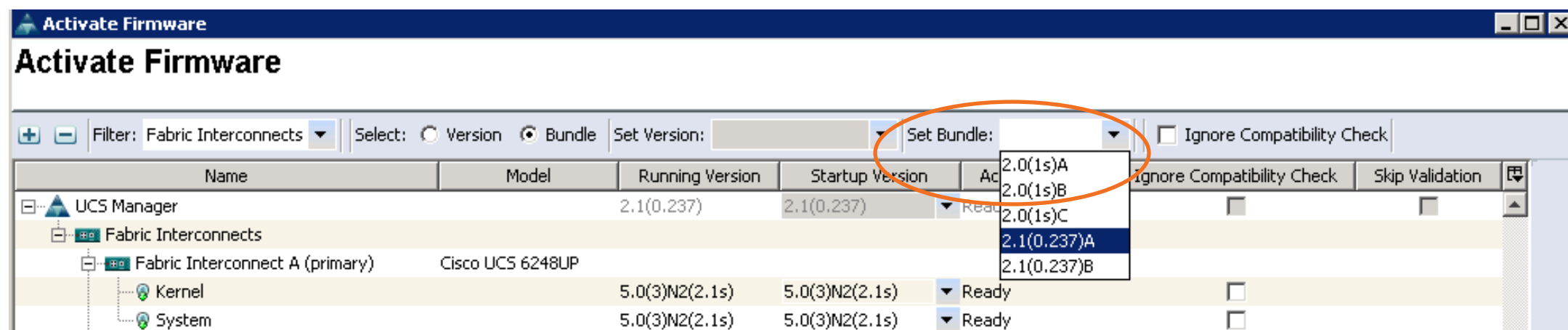
- Prevents unnecessary alerts or notifications being sent
- Admin Tab → Communication Management → Call Home
- Set State to Off
- Building in alert suppression



Firmware Steps

Set Version or Set Bundle

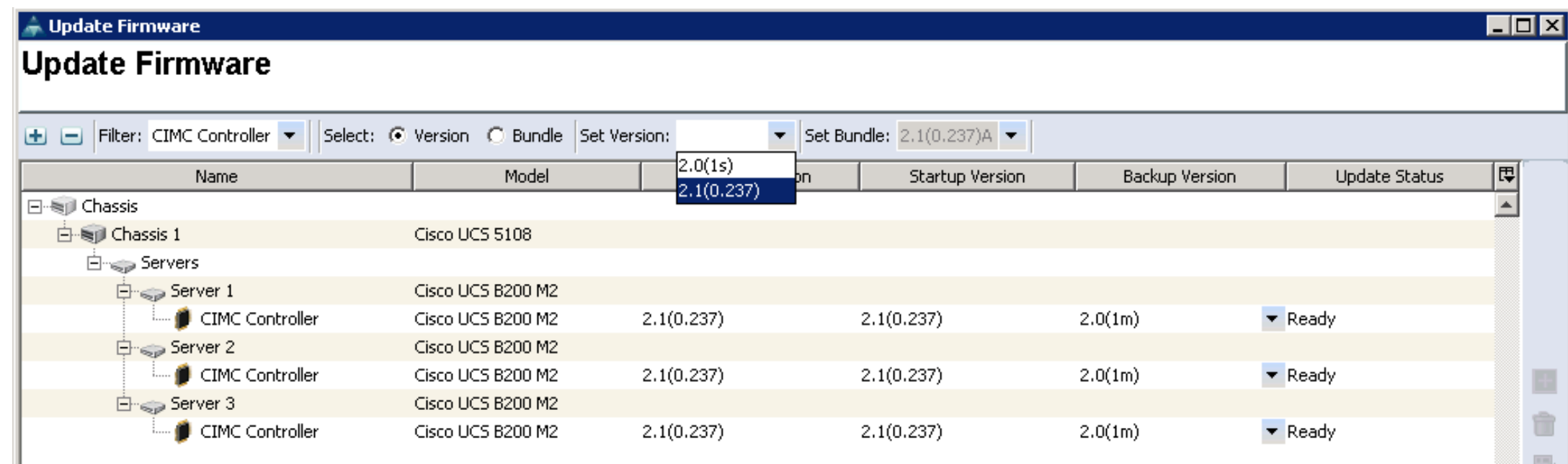
- Set Version
 - Original method of selecting firmware for endpoints
 - Used for Update and Activation of an endpoint
 - Firmware version may not match the bundle numbering scheme
- Set Bundle
 - New option for selecting a full bundle without having to know the version numbers
 - Simplified image selection for endpoints
 - Used by Firmware Auto Install



Firmware Steps

Update CIMC

- No impact to host OS on updates or activation
- Centralised distribution from the fabric interconnect
- Equipment Tab → Equipment → Firmware Management → Installed Firmware → Update Firmware
- Filter: Select all CIMC Controller



The screenshot shows the 'Update Firmware' window in a web-based management interface. The window title is 'Update Firmware'. Below the title bar, there are controls for filtering and selecting items. The 'Filter' is set to 'CIMC Controller'. The 'Select' options are 'Version' (selected) and 'Bundle'. The 'Set Version' dropdown is open, showing '2.0(1s)' and '2.1(0.237)'. The 'Set Bundle' dropdown is set to '2.1(0.237)A'. Below these controls is a table with the following columns: Name, Model, Version, Startup Version, Backup Version, and Update Status. The table is filtered to show only CIMC controllers. The data is organized into a tree structure: Chassis 1 (Cisco UCS 5108) contains Server 1, Server 2, and Server 3, each with a CIMC Controller. All three CIMC controllers are currently at version 2.1(0.237) and are ready to be updated to 2.0(1m).

Name	Model	Version	Startup Version	Backup Version	Update Status
Chassis 1	Cisco UCS 5108				
Server 1	Cisco UCS B200 M2				
CIMC Controller	Cisco UCS B200 M2	2.1(0.237)	2.1(0.237)	2.0(1m)	Ready
Server 2	Cisco UCS B200 M2				
CIMC Controller	Cisco UCS B200 M2	2.1(0.237)	2.1(0.237)	2.0(1m)	Ready
Server 3	Cisco UCS B200 M2				
CIMC Controller	Cisco UCS B200 M2	2.1(0.237)	2.1(0.237)	2.0(1m)	Ready

Firmware Steps

Update I/O Modules

- Update pushes firmware to I/O Module no host impact
- Equipment Tab → Equipment → Firmware Management → Installed Firmware → Update Firmware
- Filter: Select all I/O Modules
- Only 2 per Chassis

Name	Model	RU	Version	Startup Version	Backup Version	Update
Chassis						
Chassis 1	Cisco UCS 5108					
IO Modules						
IO Module 1	Cisco UCS 2208XP		2.0(1s)	2.0(1s)	2.0(1s)	Ready
IO Module 2	Cisco UCS 2208XP		2.0(1s)	2.0(1s)	2.0(1s)	Ready

Firmware Steps

Activate CIMC

- No host data plane impact
- Equipment Tab → Equipment → Firmware Management → Installed Firmware → Update Firmware
- Filter: All CIMC Controller can be activated at the same time across domain

Activate Firmware

Filter: CIMC Controller | Select: Version Bundle | Set Version: | Set Bundle: 2.0(1s)A | Ignore Compatibility Check

Name	Model	Running Version	Startup	Activate Status	Ignore Compatibility Check	Skip Validation
UCS Manager		2.1(0.237)	2.1(0.237)	Ready	<input type="checkbox"/>	<input type="checkbox"/>
Chassis						
Chassis 1 Cisco UCS 5108						
Serve						
SeCisco UCS B200 M2						
Cisco UCS B200 M2		2.1(0.237)	2.1(0.237)	Ready	<input checked="" type="checkbox"/>	
SeCisco UCS B200 M2						
Cisco UCS B200 M2		2.1(0.237)	2.1(0.237)	Ready	<input checked="" type="checkbox"/>	
SeCisco UCS B200 M2						
Cisco UCS B200 M2		2.1(0.237)	2.1(0.237)	Ready	<input checked="" type="checkbox"/>	

Firmware Steps

Activate UCSM

- No host data plane impact
- Equipment Tab → Equipment → Firmware Management → Installed Firmware → Update Firmware
- Filter: UCS Manager
- One Activation per domain

Activate Firmware

Filter: UCS Manager | Select: Version Bundle | Set Version: 2.0(1s) | Set Bundle: 2.0(1s)A | Ignore Compatibility Check

Name	Model	Running Version	Startup Version	Activate Status	Ignore Compatibility Check
..... UCS Manager		2.1(0.283)	2.0(1s)	Ready	<input checked="" type="checkbox"/>

Firmware Steps

Activate I/O Modules

- No host data plane impact
- Equipment Tab → Equipment → Firmware Management → Installed Firmware → Update Firmware
- Filter: IO Modules can be activated at the same time across domain
- Check: Set Startup Version Only (prevents IO Modules from rebooting)

The screenshot shows the 'Activate Firmware' window with the following configuration and table:

Filter: IO Modules | Select: Version Bundle | Set Version: 2.0(1s) | Set Bundle: 2.1(0.237)A | Ignore Compatibility Check | Set Startup Version Only

Name	Model	Running Version	Startup Version	Activate Status	Ignore Compatibility Check	Skip Validation
UCS Manager		2.1(0.237)	2.1(0.237)	Ready	<input type="checkbox"/>	<input type="checkbox"/>
Chassis						
Chassis 1	Cisco UCS 5108					
IO Modules						
IO Module 1	Cisco UCS 2208XP	2.0(1s)	2.0(1s)	Ready	<input checked="" type="checkbox"/>	<input type="checkbox"/>
IO Module 2	Cisco UCS 2208XP	2.0(1s)	2.0(1s)	Ready	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Firmware Steps

Activate Subordinate Fabric Interconnect

- No host impact if Ethernet and FC teaming are used
- Equipment Tab → Equipment → Firmware Management → Installed Firmware → Update Firmware
- Verify HA State
- Filter: Fabric Interconnect ONLY Select the Subordinate
- I/O Modules on corresponding fabric will be rebooted

Activate Firmware

Filter: Fabric Interconnects | Select: Version Bundle | Set Version: | Set Bundle: 2.0(1s)A | Ignore Compatibility Check

Name	Model	Running Version	Startup Version	Activate Status	Ignore Compatibility Check	Skip Validation
UCS Manager		2.1(0.237)	2.1(0.237)	Ready	<input type="checkbox"/>	<input type="checkbox"/>
Fabric Interconnects						
Fabric Interconnect A (primary)	Cisco UCS 6248UP					
Kernel		5.0(3)N2(2.1s)	5.0(3)N2(2.1s)	Ready	<input type="checkbox"/>	
System		5.0(3)N2(2.1s)	5.0(3)N2(2.1s)	Ready	<input type="checkbox"/>	
Fabric Interconnect B (subordinate)	Cisco UCS 6248UP					
Ker...		5.0(3)N2(2.1s)	5.0(3)N2(2.1s)	Ready	<input checked="" type="checkbox"/>	
Syst...		5.0(3)N2(2.1s)	5.0(3)N2(2.10.237) 5.0(3)N2(2.1s)	Ready	<input checked="" type="checkbox"/>	

High Availability Details

Ready: **Yes**

State: **Up**

Leadership: **Subordinate** Cluster Link State: **Full**

Firmware Steps

Activate Primary Fabric Interconnect

- No host impact if Ethernet and FC teaming are used
- Equipment Tab → Equipment → Firmware Management → Installed Firmware → Update Firmware
- Filter: Fabric Interconnect Select only the Primary
- I/O Modules on corresponding fabric will be rebooted

Name	Model	Running Version	Startup Version	Activate Status	Ignore Compatibility Check	Skip Validation
UCS Manager		2.1(0.237)	2.1(0.237)	Ready	<input type="checkbox"/>	<input type="checkbox"/>
Fabric Interco						
Fabric IntCisco UCS 6248UP						
Ker...		5.0(3)N2(2.1s)	5.0(3)N2(2.1s)	Ready	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Syst...		5.0(3)N2(2.1s)	5.0(3)N2(2.10.237)	Ready	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Fabric IntCisco UCS 6248UP			5.0(3)N2(2.1s)			
Kernel		5.0(3)N2(2.1s)	5.0(3)N2(2.1s)	Ready	<input type="checkbox"/>	<input type="checkbox"/>
System		5.0(3)N2(2.1s)	5.0(3)N2(2.1s)	Ready	<input type="checkbox"/>	<input type="checkbox"/>

Firmware Polices and Service Profiles

How to Leverage Polices to Manage Firmware

- Host Firmware package policies
 - Included in one or more service profiles
 - Included in an updating service profile template
 - Management Firmware Package is being deprecated
- Configure Maintenance Policy
 - Update immediately
 - User Acknowledged
 - Scheduled for maintenance window

Firmware Polices and Service Profiles

Firmware Updated in a Host Firmware Package

- BIOS
- CIMC
- Adapter
- Board Controller
- FC Adapters
- HBA Option ROM
- Storage Controller

General Events

Actions

- Delete
- Show Policy Usage
- Make Global

Properties

Name: **CiscoLive**

Description:

Owner: **Local**

Blade Package Version: **2.1(0.237)B**

Adapter CIMC **BIOS** Board Controller FC Adapters HBA Option ROM Storage Controller

Filter Export Print

Select	Vendor	Model	PID	Presence	Version
<input checked="" type="checkbox"/>	Cisco Systems, Inc.	Cisco UCS B230 M2	B230-BASE-M2	Present	B230.2.0.2b.0.030720121455
<input checked="" type="checkbox"/>	Cisco Systems, Inc.	Cisco UCS B440 M2	B440-BASE-M2	Present	B440.2.0.2b.0.030720121505
<input checked="" type="checkbox"/>	Cisco Systems, Inc.	Cisco UCS B200 M1	N20-B6620-1	Present	S5500.2.0.2b.0.020120121754
<input checked="" type="checkbox"/>	Intel Corp.	Cisco UCS B200 M1	N20-B6620-1	Present	S5500.2.0.2b.0.020120121754
<input checked="" type="checkbox"/>	Cisco Systems, Inc.	Cisco UCS B250 M1	N20-B6620-2	Present	S5500.2.0.2c.0.020920121737
<input checked="" type="checkbox"/>	Intel Corp.	Cisco UCS B250 M1	N20-B6620-2	Present	S5500.2.0.2c.0.020920121737
<input checked="" type="checkbox"/>	Cisco Systems, Inc.	Cisco UCS B200 M2	N20-B6625-1	Present	S5500.2.0.2b.0.020120121754
<input checked="" type="checkbox"/>	Cisco Systems, Inc.	Cisco UCS B250 M2	N20-B6625-2	Present	S5500.2.0.2c.0.020920121737
<input checked="" type="checkbox"/>	Cisco Systems, Inc.	Cisco UCS B230 M1	N20-B6730-1	Present	B230.2.0.2b.0.030720121455
<input checked="" type="checkbox"/>	Cisco Systems, Inc.	Cisco UCS B440 M1	N20-B6740-2	Present	B440.2.0.2b.0.030720121505
<input type="checkbox"/>	Cisco Systems, Inc.	Cisco UCS C200 M1	R200-1120402	N/A	<not set>
<input type="checkbox"/>	Cisco Systems, Inc.	Cisco UCS C200 M2	R200-1120402W	N/A	<not set>
<input type="checkbox"/>	Cisco Systems, Inc.	Cisco UCS C210 M1	R210-2121605	N/A	<not set>
<input type="checkbox"/>	Cisco Systems, Inc.	Cisco UCS C210 M2	R210-2121605W	N/A	<not set>
<input type="checkbox"/>	Cisco Systems, Inc.	Cisco UCS C250 M1	R250-2480805	N/A	<not set>
<input type="checkbox"/>	Cisco Systems, Inc.	Cisco UCS C250 M2	R250-2480805W	N/A	<not set>
<input checked="" type="checkbox"/>	Cisco Systems, Inc.	Cisco UCS B200 M3	UC5B-B200-M3	Present	B200M3.2.0.2b.0.030720121...
<input checked="" type="checkbox"/>	Cisco Systems, Inc.	Cisco UCS B22 M3	UC5B-B22-M3	Present	B22M3.2.0.2.10.030820121044
<input type="checkbox"/>	Cisco Systems, Inc.	Cisco UCS C200 M2	UCSC-B5E-SFF-C200	N/A	<not set>

Firmware Steps

Host Firmware Package Policies

- Policies for defining rules and consistency for hardware
- Create a host firmware package policy
- May use simple (select a bundle) or Advanced (customise) method, starting with UCSM 2.1.x

Create Host Firmware Package

Create Host Firmware Package

Name:

Description:

How would you like to configure Host Firmware Package? Simple Advanced

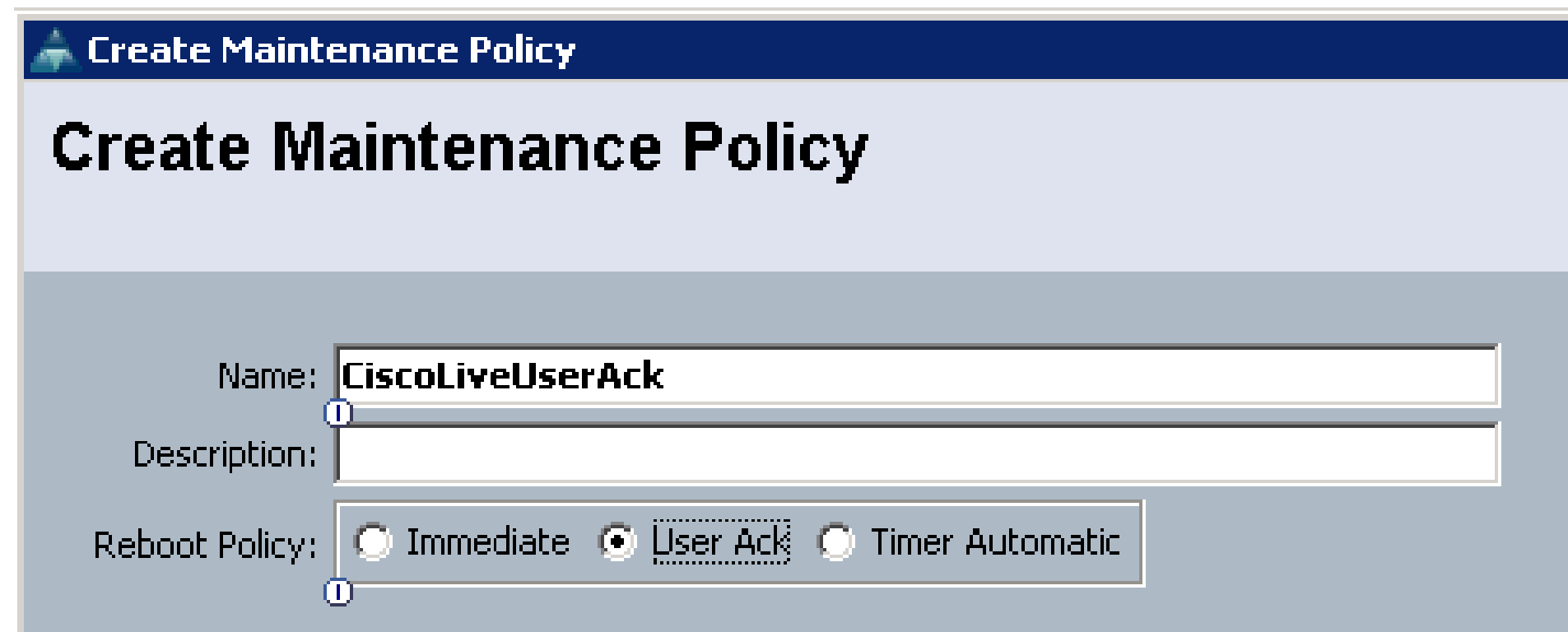
Blade Package Version:

Rack Package Version:

Firmware Steps

Maintenance Policies

- Used to defer Service Profile state changes
- 3 Policies for reboot behaviours
- Create a maintenance policy
 - User Acknowledged



The screenshot shows a web-based configuration interface for creating a maintenance policy. The page title is "Create Maintenance Policy". The form contains the following fields and options:

- Name:** CiscoLiveUserAck
- Description:** (empty text box)
- Reboot Policy:** Three radio button options: Immediate, User Ack, and Timer Automatic.

Firmware Steps

Create Service Profile Template

- Templates provide standardisation
- Create service profile template
- Configure Host firmware package policy
- Associate Policy to the Template

Identify Service Profile Template

You must enter a name for the service profile template and specify the template type assigned to this template and enter a description.

Name:

The template will be created in the following organization. Its name must be unique within this organization.

Where: **org-root**

The template will be created in the following organization. Its name must be unique within this organization.

Type: Initial Template Updating Template

Firmware Management (BIOS, Disk Controller, Adapter)

If you select a host firmware policy for this service profile template, the profile will update the firmware on the server that it is associated with. Otherwise the system uses the firmware already installed on the associated server. Management firmware policy is deprecated and so it is recommended to use host firmware policy to set CIMC versions.

Host Firmware:

Firmware Update Approx Times in Minutes

Function	Update	Activate
Upgrade CIMC	5-6	1-2
Upgrade UCSM	--	1-2
Upgrade I/O module	12-16	3-6sec
Upgrade FI pair and I/O modules	--	24-38
Upgrade Host server	1-2	4
TOTAL Minutes	24	46



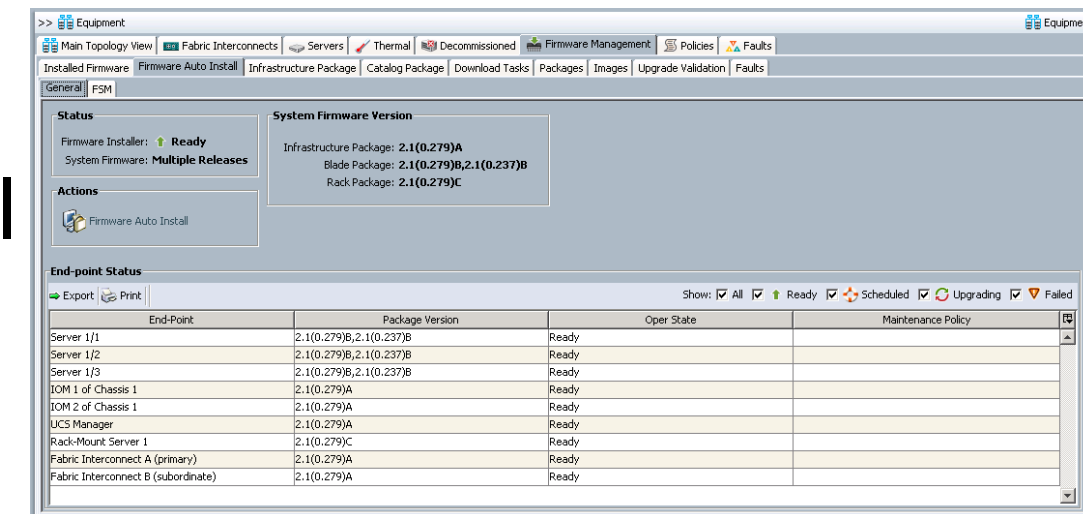
Firmware Automation



Firmware Auto Install

Automation for Firmware Deployment

- New Automated firmware deployment engine integrated into UCSM
- Can automate the update the firmware of all UCS components
- Multiple modes of operation
 - Auto Install firmware on Infrastructure components
 - Auto Install firmware on UCS Managed servers
- Managed from Local UCSM or from UCS Central
- Validates firmware dependencies automatically
- Update firmware in correct order
- All firmware components in the UCS domain can be updated



Firmware Auto Install

Automation for Firmware Deployment

- Infrastructure package
 - Contains UCS Manager, FI kernel and system, IOM
 - Allows user to choose the version to update infrastructure to
 - Default pack is created and used by Auto Install
- Host Firmware Package
 - Same as existing host firmware package now includes CIMC
 - deprecating management firmware pack
- Current direct updates and firmware packs will continue to work with no changes
- A schedule can be applied to infrastructure pack to control firmware deployment time frame
- Server update can be controlled by maintenance policy on Service profile (Existing mechanism)

Firmware Auto Install

For a New UCS System

- Use for brand new UCS domain pre-deployment
 - Install all infrastructure
 - Install all B and C series servers
- Select Equipment → Firmware Auto Install → Actions Install Infrastructure then Servers

The screenshot shows the 'Properties' dialog for a firmware installation. The 'Name' is 'default' and the 'Description' is 'Infrastructure Pack'. The 'Version' is set to '2.1(0.279)A'. The 'Infrastructure Schedule' section shows 'Admin State: Untriggered', 'Overall Status: Triggered', and 'Policy Owner: Local'. The 'Start Time' is '1970-01-01T00:00:00'. There is a 'One Time Occurrence Properties' button. On the left, the 'Firmware System Status' shows 'Firmware Installer: Ready' and 'System Firmware: Multiple Releases'. Below that, the 'Actions' section has a 'Cancel Infrastructure Upgrade' button. At the bottom, there is a table with columns for Vendor, Model, PID, Presence, and Version. The table contains one row: Cisco Systems, CAM-NSK, Present, 2.1(0.279). Buttons for OK, Apply, Cancel, and Help are at the bottom right.

Vendor	Model	PID	Presence	Version
Cisco Systems		CAM-NSK	Present	2.1(0.279)

The screenshot shows the 'Unified Computing System Manager' interface. The main title is 'Unified Computing System Manager'. On the left, there is a list of steps for 'Install Servers': 1. Prerequisites (checked), 2. Select Package Versions (selected), 3. Select Host Firmware Packages, and 4. Summary. The main area is titled 'Select Package Versions' and contains two sections: 'B-Series Blade Server Software' and 'C-Series Rack-Mount Server Software'. Each section shows 'Current Version' and 'New Version' dropdown menus. The B-Series section shows 'Current Version: 2.1(0.283)B, 2.1(0.237)B' and 'New Version: <not set>'. The C-Series section shows 'Current Version: 2.1(0.283)C' and 'New Version: <not set>'. At the bottom, there is a note: 'If the desired packages are not found then click [here](#) to go to the download firmware screen.'

Firmware Auto Install

For an Existing UCS System

- Use for production UCS domain and leverage host firmware policies for support of multiple host code levels
- Select Equipment → Firmware Auto Install → Actions Install Infrastructure
- Infrastructure updates: UCSM, both FIs, and I/O modules

Properties

Name: **default**
Description:
Version:
Infrastructure Schedule
Admin State: **Untriggered**
Overall Status: **Triggered**
Policy Owner: **Local**
Start Time:
One Time Occurrence Properties

Firmware System Status
Firmware Installer: **Ready**
System Firmware: **Multiple Releases**

Actions

UCSM | Fabric Interconnect Kernel | Fabric Interconnect Software | IO Modules

Filter | Export | Print

Vendor	Model	PID	Presence	Version
Cisco Systems		CAM-N5K	Present	2.1(0.279)

OK Apply Cancel Help

Firmware Auto Install

For an Existing UCS System

- Single screen for UCS Domain status
- Summary and logs
- View impact of end points



The screenshot shows the 'Equipment' page in the UCS Management interface, specifically the 'Firmware Management' section. The 'Firmware Auto Install' tab is active. The 'Status' section shows 'Firmware Installer: In Progress' and 'System Firmware: Multiple Releases'. The 'Firmware Package Version' section shows: Infrastructure: 2.1(0.279)A, 2.1(0.283)A; Blade: 2.1(0.283)B, 2.1(0.237)B; Rack: 2.1(0.283)C. The 'End-point Status' table is shown below.

End-Point	Package Version	Oper State	Maintenance Policy
Server 1/1	2.1(0.283)B, 2.1(0.237)B	Ready	
Server 1/2	2.1(0.283)B, 2.1(0.237)B	Ready	
Server 1/3	2.1(0.283)B, 2.1(0.237)B	Ready	
IOM 1 of Chassis 1	2.1(0.279)A	Upgrading	
IOM 2 of Chassis 1	2.1(0.279)A	Upgrading	
UCS Manager	2.1(0.283)A	Ready	
Rack-Mount Server 1	2.1(0.283)C	Ready	
Fabric Interconnect A (primary)	2.1(0.279)A	Ready	
Fabric Interconnect B (subordinate)	2.1(0.279)A	Upgrading	

Server Firmware Auto Install

For an Existing UCS System

- FOLLOW the instructions on the last screen
- Create a Backup of the configuration
- Check all maintenance policies for host service profiles
- Once started the process must finish to completion

Prerequisites

This wizard will enable you to perform a bulk firmware upgrade of servers. You may specify whether to upgrade the Blade server and/or Rack-Mount server firmware package. You can only upgrade by specifying a package, not a specific equipment end-point.

Before undertaking a system wide firmware upgrade you should consider the following activities and implications.

- 1) A full system backup so that you may restore the system configuration if any errors occur during the upgrade process.
Click [here](#) to launch backup tool.
- 2) Understanding the potential consequences of disruptive service impact by cross referencing the impacted end-points with any service they may be supporting.
- 3) This wizard will update host firmware packages potentially impacting service profiles that reference them.
Click [here](#) to view maintenance policies.

Firmware Auto Install

For an Existing UCS System

- Host firmware updates use existing Host Firmware Package Policies if selected
- By default Auto Install will honor Maintenance Policy settings for the service profiles
- By default Auto Install will change the contents of the host firmware package policy selected for update

Select Host Firmware Packages

Warning

You have selected version **2.1(0.323)B** of B-Series Blade Server Software.
You have selected version **2.1(0.323)C** of C-Series Rack-Mount Server Software.
All selected host packs below will be **modified** with images from the above mentioned package(s).

Host Firmware Packages

- root
 - CiscoLive_2.1.323 [2.1(0.323)B, 2.1(0.323)C]
 - CiscoLive_Blades [2.1(0.283)B, 2.1(0.283)C]
 - default [2.1(0.283)B]

PowerShell

Firmware Automation

- Powerful and flexible object oriented scripting tool
- Most UCS commands and functions have PowerShell cmdlets
- Run commands against one or multiple UCS Domains
- Run commands manually in powertool
- Build your own scripts and automation methods
- Large open community to freely share scripts
- Demo

DEMO/VIDEO



Cisco UCS Firmware Simplicity Summary

Firmware Management Simplified vs. Legacy

- Reduced number of infrastructure endpoints
- Reduced firmware management complexity
- Centralised firmware management for entire UCS domains
 - 160 servers and endpoints under one UCSM instance
 - 800 servers and endpoints under UCS Central instance
- Single tool and interface used for all firmware tasks
- Built in firmware deployment automation

Q & A



Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2013 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site www.ciscoliveaustralia.com/mobile
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 8 March 12:00pm-2:00pm



Cisco *live!* 365

Don't forget to activate your Cisco Live 365 account for access to all session material,

communities, and on-demand and live activities throughout the year. Log into your Cisco Live portal and click the "Enter Cisco Live 365" button.

www.ciscoliveaustralia.com/portal/login.wv

Cisco *live!*

