



# Release Notes for Cisco UCS Software, Release 1.4

**First Published:** December 19, 2010  
**Last Updated:** January 08, 2016  
**Part Number:** OL-24086-01

This document describes the new features, system requirements, and caveats for Cisco UCS Manager, Release 1.4(1i), 1.4(1j), 1.4(1m), 1.4(2b), 1.4(3i), 1.4(3l), 1.4(3m), 1.4(3q), 1.4(3s), 1.4(3u), 1.4(3y), 1.4(4f), 1.4(4g), 1.4(4i), 1.4(4j), 1.4(4k), 1.4(4l) and all related firmware and BIOSes on blade servers and other Unified Computing System components associated with that release. Use this document with the documents listed in the [“Related Documentation” section on page 78](#).



## Note

We sometimes update the documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates. Documentation updates and errata are also in these release notes. The documentation roadmap for this product is available at: <http://www.cisco.com/go/unifiedcomputing/b-series-doc>

[Table 1](#) shows the online change history for this document.

**Table 1** Online History Change

Part Number	Revision	Date	Description
OL-24086-01	A0	December 19, 2010	Created release notes for Release 1.4(1i). <sup>1</sup>
	B0	January 7, 2011	Updated release notes for Release 1.4(1j).
	C0	March 1, 2011	Updated release notes for Release 1.4(1m).
	D0	April 27, 2011	Updated release notes for Release 1.4(2b). <sup>2</sup>
	E0	June 20, 2011	Updated release notes for Release 1.4(3i).
	F0	July 5, 2011	Updated release notes for Release 1.4(3l).
	G0	August 5, 2011	Updated release notes for Release 1.4(3m).
	H0	September 2, 2011	Updated release notes for Release 1.4(3q).
	I0	October 20, 2011	Updated release notes for Release 1.4(3s).



**Table 1 Online History Change (continued)**

Part Number	Revision	Date	Description
OL-24086-01	J0	December 15, 2011	Updated release notes for catalog release 1.0.52.T.
	K0	December 21, 2011	Updated release notes for Release 1.4(3u).
	L0	February 24, 2012	Updated release notes for Release 1.4(3y).
	M0	May 11, 2012	Updated release notes for Release 1.4(4f).
	N0	June 4, 2012	Updated release notes for Release 1.4(4g).
	O0	June 20, 2012	Updated release notes for Release 1.4(4i).
	P0	July 12, 2012	Updated release notes for Catalog Release 1.0.60.T.
	Q0	August 10, 2012	Updated release notes for Release 1.4(4j).
	R0	September 27, 2012	Updated release notes for Catalog Release 1.0.63.T.
	S0	December 6, 2012	Updated release notes for Catalog Release 1.0.64.T.
	T0	January 11, 2013	Updated release notes for Release 1.4(4k).
	U0	February 18, 2013	Updated release notes for Catalog Release 1.0.66.T.
	V0	May 8, 2013	Updated release notes for Catalog Release 1.0.67.T.
	W0	October 8, 2013	Updated release notes for Catalog Release 1.0.71.T.
	X0	January 14, 2014	Updated release notes for Release 1.4(4l).
	Y0	February 19, 2014	Updated release notes for Catalog Release 1.0.73.T.
	Z0	April 2, 2014	Updated release notes for Catalog Release 1.0.74.T
	A1	May 16, 2014	Added CSCuo78883 in Open Caveats for 1.4(4l).
	B1	May 30, 2014	Removed CSCua02797 from Resolved Caveats; applies only to VIC Driver release notes.
	C1	June 13, 2014	Updated release notes for Catalog Release 1.0.75.T
D1	August 19, 2014	Updated release notes for Catalog Release 1.0.76.T	
E1	December 4, 2014	Updated release notes for Catalog Release 1.0.77.T	
F1	June 30, 2015	Updated release notes for Catalog Release 1.0.78.T	
G1	January 08, 2016	Updated release notes for Catalog Release 1.0.79.T	

1. This release was removed from the download area due to CSCt122248. See the [software deferral notice](#).
2. This release was removed from the download area due to CSCtq03411. See the [software deferral notice](#).

# Contents

This document includes the following sections:

- [“Introduction” section on page 3](#)
- [“System Requirements” section on page 3](#)
- [“Updating Cisco UCS Versions” section on page 3](#)
- [“Hardware and Software Interoperability” section on page 6](#)
- [“Known Limitations and Behaviors” section on page 10](#)

- [“Resolved Caveats” section on page 13](#)
- [“Open Caveats” section on page 23](#)
- [“New Hardware Features in Release 1.4” section on page 70](#)
- [“New Software Features in Release 1.4” section on page 71](#)
- [“Bundle Images” section on page 73](#)
- [“Related Documentation” section on page 78](#)
- [“Obtaining Documentation and Submitting a Service Request” section on page 79](#)

## Introduction

The Cisco Unified Computing System is a next-generation data center platform that unites compute, network, storage access, and virtualization into a cohesive system designed to reduce total cost of ownership (TCO) and increase business agility. The system integrates a low-latency, lossless 10-Gigabit Ethernet unified network fabric with enterprise-class, x86-architecture servers. The system is an integrated, scalable, multi-chassis platform in which all resources participate in a unified management domain.

## System Requirements

Cisco UCS Manager must meet or exceed the following minimum system requirements:



Caution

---

The Cisco UCS Manager GUI is a Java-based application, and is only supported on Sun JRE 1.6.

---

- UCS Manager uses web start and supports the following web browsers:
  - Microsoft Internet Explorer 6.0 or higher
  - Mozilla Firefox 3.0 or higher

Adobe Flash Player 10 or higher is required for some features

- UCS Manager is supported on the following operating systems:
  - Microsoft Windows XP
  - Microsoft Windows Vista
  - Red Hat Enterprise Linux 5.0 or higher

## Updating Cisco UCS Versions

To update the Cisco UCS software and firmware, see the appropriate [Upgrading Cisco UCS](#) document for your installation. All A, B, and C bundles must be at the exact same version and patch level.



Tip

---

The upgrade process from 1.4(1) to 1.4(2) or 1.4(3) or 1.4(4) is identical to upgrading from 1.3 versions to 1.4 versions.

---

Use the **scope firmware** and **show package filename expand** CLI commands to view the contents of a given release package. Filenames are accurate for the initial patch release in each table. Expect small changes for subsequent patch releases.

Table 2 shows the software files in Release 1.4(4).

**Table 2** Files in Release 1.4(4)

Release Version	CCO Software Type	File name(s)	Comment
1.4(4l) Bundle Images	SWT Unified Computing System (UCS) Infrastructure Software and Server Software Bundles for 1.4(4l).	—	—
	SWT Unified Computing System (UCS) Manager Capability Catalog	ucs-catalog.1.0.71.T.bin	UCS Manager capability catalog image
	SWT Unified Computing System (UCS) Drivers	ucs-b2xx-drivers-1.4.2.iso	ISO image of UCS drivers
	SWT Unified Computing System (UCS) Utilities	ucs-b2xx-utils-1.4.1-linux.iso ucs-b2xx-utils-1.4.1-vmware.iso ucs-b2xx-utils-1.4.1-windows.iso	ISO images of UCS utilities
1.4(4k) Bundle Images	SWT Unified Computing System (UCS) Infrastructure Software and Server Software Bundles for 1.4(4k).	—	—
	SWT Unified Computing System (UCS) Manager Capability Catalog	ucs-catalog.1.0.65.T.bin	UCS Manager capability catalog image
1.4(4j) Bundle Images	SWT Unified Computing System (UCS) Infrastructure Software and Server Software Bundles for 1.4(4j).	—	—
	SWT Unified Computing System (UCS) Manager Capability Catalog	ucs-catalog.1.0.60.T.bin	UCS Manager capability catalog image
	SWT Unified Computing System (UCS) Infrastructure Software Bundle	ucs-k9-bundle-infra.1.4.4i.A.bin	Switch software, CMC/IOM software, and UCS Manager
	SWT Unified Computing System (UCS) Server Software	ucs-k9-bundle-b-series.1.4.4i.B.bin ucs-k9-bundle-c-series.1.4.4i.C.bin	Server-side BIOS, CIMC, and other firmware images for blades (B) and rack servers (C)
	SWT Unified Computing System (UCS) Manager Capability Catalog	ucs-catalog.1.0.57.T.bin	UCS Manager capability catalog image

Table 3 shows the software files in Release 1.4(3).

**Table 3** Files in Release 1.4(3)

CCO Software Type	File name(s)	Comment
SWT Unified Computing System (UCS) Infrastructure Software Bundle	ucs-k9-bundle-infra.1.4.3m.A.bin	Switch software, CMC/IOM software, and UCS Manager
SWT Unified Computing System (UCS) Server Software	ucs-k9-bundle-b-series.1.4.3m.B.bin ucs-k9-bundle-c-series.1.4.3m.C.bin	Server-side BIOS, CIMC, and other firmware images for blades (B) and rack servers (C)

**Table 3** Files in Release 1.4(3) (continued)

CCO Software Type	File name(s)	Comment
SWT Unified Computing System (UCS) Manager Capability Catalog	ucs-catalog.1.0.42.T.bin	UCS Manager capability catalog image
SWT Unified Computing System (UCS) Drivers	ucs-b2xx-drivers-1.4.2.iso	ISO image of UCS drivers
SWT Unified Computing System (UCS) Utilities	ucs-b2xx-utils-1.4.1-linux.iso ucs-b2xx-utils-1.4.1-vmware.iso ucs-b2xx-utils-1.4.1-windows.iso	ISO images of UCS utilities

Table 4 shows the software files in Release 1.4(2).

**Table 4** Files in Release 1.4(2)

CCO Software Type	File name(s)	Comment
SWT Unified Computing System (UCS) Infrastructure Software Bundle	ucs-k9-bundle-infra.1.4.2b.A.bin	Switch software, CMC/IOM software, and UCS Manager
SWT Unified Computing System (UCS) Server Software	ucs-k9-bundle-b-series.1.4.2b.B.bin ucs-k9-bundle-c-series.1.4.2b.C.bin	Server-side BIOS, CIMC, and other firmware images for blades (B) and rack servers (C)
SWT Unified Computing System (UCS) Manager Capability Catalog	ucs-catalog.1.0.42.T.bin	UCS Manager capability catalog image
SWT Unified Computing System (UCS) Drivers	ucs-b2xx-drivers-1.4.2.iso	ISO image of UCS drivers
SWT Unified Computing System (UCS) Utilities	ucs-b2xx-utils-1.4.1-linux.iso ucs-b2xx-utils-1.4.1-vmware.iso ucs-b2xx-utils-1.4.1-windows.iso	ISO images of UCS utilities

Table 5 shows the software files in Release 1.4(1).

**Table 5** Files in Release 1.4(1)

CCO Software Type	File name(s)	Comment
SWT Unified Computing System (UCS) Infrastructure Software Bundle	ucs-k9-bundle-infra.1.4.1m.A.bin	Switch software, CMC/IOM software, and UCS Manager
SWT Unified Computing System (UCS) Server Software	ucs-k9-bundle-b-series.1.4.1m.B.bin ucs-k9-bundle-c-series.1.4.1m.C.bin	Server-side BIOS, CIMC, and other firmware images for blades (B) and rack servers (C)
SWT Unified Computing System (UCS) Manager Capability Catalog	ucs-catalog.1.0.42.T.bin	UCS Manager capability catalog image
SWT Unified Computing System (UCS) Drivers	ucs-b2xx-drivers-1.4.2.iso	ISO image of UCS drivers
SWT Unified Computing System (UCS) Utilities	ucs-b2xx-utils-1.4.1-linux.iso ucs-b2xx-utils-1.4.1-vmware.iso ucs-b2xx-utils-1.4.1-windows.iso	ISO images of UCS utilities

# Hardware and Software Interoperability

- “Internal Dependencies” section on page 6
- “Capability Catalog” section on page 8

For detailed information about storage switch, operating system, adapter, adapter utility, and storage array interoperability, see the *Hardware and Software Interoperability Matrix* for this release, located at: <http://www.cisco.com/c/en/us/support/servers-unified-computing/unified-computing-system/products-technical-reference-list.html>



## Note

VMware ESX and ESXi 3.5 Update 4, and ESX and ESXi 4.0 are not compatible with Intel 56xx processors. 55xx processors are not affected by this limitation. See the interoperability matrix for this release for OS and other support questions.

## Internal Dependencies

Table 6 shows interdependencies between UCS hardware and versions of Cisco UCS Manager. Server FRU items like DIMMs are dependent on their server type, and chassis items like fans and power supplies work with all versions of UCS Manager.



## Caution

You cannot mix component software versions (for example, you cannot have a B200 using the 1.0(1) BIOS with a UCS M81KR adapter running 1.0(2) firmware managed by UCS Manager 1.3(1)). Compare the minimum software version for all your components and use at least the latest of all the versions, or use the most current version of software for all components. Mixing M1 and M2 hardware versions is not an issue if they are running software at a version matching the other system components.

**Table 6** Internal Dependencies

Component	Recommended Minimum Software Version	Recommended Software Version
<b>Servers</b>		
B200 M1	1.0(1)	1.4(4)
B230 M1	1.4(1)	1.4(4)
B250 M1	1.1(1)	1.4(4)
B440 M1	1.3(1)	1.4(4)
B200 M2	1.2(1)	1.4(4)
B230 M2	1.4(3)	1.4(4)
B250 M2	1.2(1)	1.4(4)
B440 M2	1.4(3)	1.4(4)
C200 M2	1.4(1)	1.4(4)
C210 M2	1.4(1)	1.4(4)
C250 M2	1.4(1)	1.4(4)

Table 6 Internal Dependencies (continued)

Component	Recommended Minimum Software Version	Recommended Software Version
<b>Adapters</b>		
UCS 82598KR-CI UCS M71KR-E UCS M71KR-Q	1.0(1)	1.4(4)
UCS M81KR	1.0(2)	1.4(4)
UCS NIC M51KR-B UCS CNA M61KR-I <sup>1</sup> UCS CNA M72KR-Q UCS CNA M72KR-E	1.3(1)	1.4(4)
<b>Fabric Interconnect</b>		
UCS 6120XP	1.0(1)	1.4(4)
UCS 6140XP	1.1(1)	1.4(4)
<b>Fabric Extender</b>		
Cisco UCS 2104	1.0(1)	1.4(4)
Cisco Nexus 2248	1.4(1)	1.4(4)
<b>Fabric Interconnect Expansion Modules</b>		
N10-E0440 N10-E0600 N10-E0080	1.0(1)	1.4(4)
N10-E0060	1.1(1)	1.4(4)
<b>10-GB connections</b>		
SFP-10G-SR, SFP-10G-LR SFP-H10GB-CU1M SFP-H10GB-CU3M SFP-H10GB-CU5M	1.0(1)	1.4(4)
FET-10G	1.4(1)	1.4(4)
SFP-H10GB-ACU7M= SFP-H10GB-ACU10M=	1.4(2)	1.4(4)
<b>8-GB connections (FC expansion module N10-E0060)</b>		
DS-SFP-FC8G-SW DS-SFP-FC8G-LW	1.3(1)	1.4(4)
<b>4-GB connections (FC expansion module N10-E0080)</b>		
DS-SFP-FC4G-SW DS-SFP-FC4G-LW	1.0(1)	1.4(4)

**Table 6** Internal Dependencies (continued)

Component	Recommended Minimum Software Version	Recommended Software Version
<b>1-GB connections</b>		
GLC-T (V03 or higher)	1.3(1)	1.4(4)
GLC-SX-MM		
GLC-LH-SM		

1. N20-AI0002, the Cisco UCS 82598KR-CI 10-GB Ethernet Adapter, is not supported on the B440 server but is still available for other models. We suggest you use the Cisco UCS CNA M61KR-I Intel Converged Network Adapter in place of the Cisco UCS 82598KR-CI 10-GB Ethernet Adapter.

## Capability Catalog

Cisco UCS Manager uses the catalog to update the display and configurability of server components such as newly qualified DIMMs and disk drives. The UCS Manager Capability Catalog is a single image, but it is also embedded in UCS Manager. The latest posted 1.x catalog will work with any posted 1.3 or 1.4 release.



### Note

Cisco UCS Manager 1.x releases will work with any 1.x catalog file, but not with any 2.0 or later catalog versions. Release 1.4 is only compatible with a 1.0 catalog file.

If a server component is not dependent on a specific BIOS version, using it and having it recognized by UCS Manager is primarily a function of the catalog version. The catalog is released as single image in some cases for convenience purposes in addition to being bundled with UCS infrastructure releases. See [Table 7](#) for details.

**Table 7** Version Mapping

UCS Release	Catalog File	Adds Support for PID	Additional Parts Qualified for PID
1.4(1i)	ucs-catalog.1.0.16.T.bin	A02-M316GB2-L on B200 M2	
1.4(1j)	ucs-catalog.1.0.17.T.bin	—	
1.4(1k)	ucs-catalog.1.0.17.T.bin	—	
1.4(1m)	ucs-catalog.1.0.24.T.bin	A02-M332GB3-2-L on B440 M1	
—	ucs-catalog.1.0.25.T.bin	—	
1.4(2b)	ucs-catalog.1.0.37.T.bin	N01-M308GB2-L and N01-M308GB2 on B200	
1.4(3i)	ucs-catalog.1.0.39.T.bin	B230 M2 and B440 M2	
1.4(3m)	ucs-catalog.1.0.42.T.bin	—	
1.4(3q)	ucs-catalog.1.0.46.T.bin	UCS-SSD100GI1F105 UCS-MR-1X041RX-A UCS-MR-2X082RX-B	
1.4(3s)	ucs-catalog.1.0.49.T.bin	—	



Table 7 Version Mapping (continued)

UCS Release	Catalog File	Adds Support for PID	Additional Parts Qualified for PID
—	ucs-catalog.1.0.52.T.bin	UCS-CPU-X5687 on B200 M2 UCS-HDD900GI2F106 on C200 and C210 UCS-MR-2X082RX-C	
1.4(4i)	ucs-catalog.1.0.57.T.bin	Fixed incorrect data for the following PIDs: UCS-SD200G0KA2-T UCS-SD300G0KA2-T UCS-SD100G0KA2-E UCS-SD200G0KA2-E UCS-SD300G0KA2-E UCS-HDD900GI2F106	
1.4(4j)	ucs-catalog.1.0.60.T.bin	UCS-MR-2X041RX-B UCS-MR-1X162RY-A UCS-HDD300GI2F105 UCS-MR-2x164RX-C	
—	ucs-catalog.1.0.63.T.bin	UCS-MR-1X162RY-A UCS-SD100G0KA2-G UCS-SD100G0KA2-S UCS-SD400G0KA2-G UCS-SD400G0KA2-S UCS-MR-2x164RX-D	
—	ucs-catalog.1.0.64.T.bin	—	
1.4(4k)	ucs-catalog.1.0.65.T.bin	UCS-CPU-E5-2658	
—	ucs-catalog.1.0.66.T.bin	A03-D300GA2 A03-D600GA2 UCS-HDD900GI2F106	
—	ucs-catalog.1.0.67.T.bin	—	
—	ucs-catalog.1.0.71.T.bin	—	
1.4(4l)	—	—	
—	ucs-catalog.1.0.73.T.bin	UCS-MR-1X041RY-A UCS-MR-1X082RY-A UCS-MR-2X041RX-C UCS-MR-2X162RX-C	
—	ucs-catalog.1.0.74.T.bin	UCS-MR-2X041RY-B UCS-MR-2X082RY-B	
—	ucs-catalog.1.0.75.T.bin	UCS-MR-2X324RX-C	
—	ucs-catalog.1.0.76.T.bin	—	
—	ucs-catalog.1.0.77.T.bin	—	

Table 7 Version Mapping (continued)

UCS Release	Catalog File	Adds Support for PID	Additional Parts Qualified for PID
—	ucs-catalog.1.0.78.T.bin	—	
—	ucs-catalog.1.0.79.T.bin	<b>Drives</b> <ul style="list-style-type: none"> <li>• UCS-HD300G10K12G</li> <li>• UCS-HD300G15K12G</li> <li>• UCS-HD450G15K12G</li> <li>• UCS-HD600G10K12G</li> <li>• UCS-HD600G15K12G</li> <li>• UCS-HD900G10K12G</li> </ul>	<b>Memory</b> <ul style="list-style-type: none"> <li>• UCS-MR-1X162RY-A</li> <li>• UCS-MR-2X162RX-C</li> </ul>

For more details, see the [UCS Manager GUI Configuration Guide](#).

## Known Limitations and Behaviors

The following known limitations found in Release 1.4(x) are not otherwise documented:

- Unable to vMotion after blade firmware upgrade from 1.4(3m) to any later release due to AES-NI bit difference. Reboot the server, and disable OEM AESNI Control in BIOS. After you boot to ESXi, vMotion will proceed between the two hosts without any issues.
- Prior to Release 1.4(1) all backplane ports show up in UCS Manager regardless of blade connectivity status. In Release 1.4(1) and later, backplane ports are only created when UCS Manager detects an adapter in the connected blade server. Connected blade servers without an adapter will not create any backplane ports. This issue only applies to blade servers.
- In Release 1.4(1), fabric interconnects introduced support for FC direct topologies, though local zoning is not configurable in the UCS software and is inherited from upstream Cisco MDS or Nexus 5000 switches. For SAN environments with no FC zoning, expect scaling and security issues not seen in an environment with zoning configured. This issue is not UCS specific behavior but common to any default zoned environment. Default zoned configurations are not recommended for production deployments, which should always use direct connect FC topologies with upstream Cisco MDS or Nexus 5000 switches. If no SAN network presently exists upstream, a pair of redundant Cisco MDS 9124 or 9148 switches that are not in the data path will be able to provide zoning configuration. If redundancy is not critical, a single SAN switch is sufficient to provide zoning, however, you will not be able to make zone configuration changes when the SAN switch incurs a failure. Alternately, FCoE licenses on an existing pair of upstream Cisco Nexus 5000 switches would be sufficient to configure zoning.
- In Release 1.4(1i) and later releases, when the monitored DIMM Correctable ECC error rate exceeds the threshold for a given time interval, memory DIMM operability is marked as “Degraded” and minor faults are seen even though the overall status is marked “Operable.” Once marked as “Degraded,” DIMM operability will not get reevaluated unless the DIMM is replaced, even if a BMC or host CPU reset occurs, and DIMM operability will not change. Affected DIMMs will continue to be operational (when Operability status is marked as “Operable”) so correcting the marking is optional. You can force DIMM operability to be reevaluated with the “reset memory error” action in the GUI DIMM window or with the following CLI command sequence: **scope server x/y -> scope memory-array <x> -> scope dimm <y> -> reset-errors -> commit-buffer.**

- The VLAN virtual port limit in Release 1.4(1) is 6000 or 14000 in 1.4(3q) if you do not turn on port security and use private VLANs. When this system-wide limit is reached, if you try to add more VLANs through service profiles, the service profile association will fail. In a Layer 2 topology, logical instances of a VLAN are created on each interface for each active VLAN. These instances are referred to as spanning-tree active logical ports or virtual ports. For example, if you define 900 VLANs and 2 uplinks, this configuration would consume 1800 of these virtual VLAN ports.
- When you configure a SPAN, you create a named monitoring session, specify a destination port, and specify one or more sources to monitor. In the GUI, this configuration is all done in one place. In the CLI, you create the session and enter its configuration mode. There, you can only specify the destination session. Next, you have to navigate to the scope of the desired source interface, and tell that interface that it is a source for the particular monitoring session. This behavior is correct according to the way the system is designed.
- Adding a VSAN or VLAN as a SPAN source could fail if another VLAN or VSAN is already a source for a SPAN. When UCS Manager creates a VSAN, it associates an FCoE VLAN to it. Only one UCS Manager-created VSAN and its FCoE VLAN, can be put into a monitor session (SPAN). If both are set as a SPAN source, one monitor session will fail with a fault message. To avoid this, remove either the VSAN or the VLAN as a SPAN source.
- If you are unable to install ESXi 4.x on systems with Generation 2 Intel M61KR-I, Emulex M72KR-E, Broadcom M51KR-B or Qlogic M72KR-Q CNA Adapters, be advised that ESXi 4.0 U1, U2, or ESXi 4.1 does not have the updated drivers needed for the Generation 2 CNA from Intel M61KR-I, Emulex M72KR-E, Broadcom M51KR-B, or Qlogic M72KR-Q so it will fail installation before trying to select an installation disk. The reason is that ESXi needs to load a network driver in order to install properly. The only CNA that is currently supported in ESXi versions prior to ESXi 4.0 U1, U2, and ESXi 4.1 is the Cisco M81KR.
- In a RHEL 5.5 installation (either new or an update to UCS 1.4(1)) using the default 1.4.0.98 fnic driver, a command issued to reset a LUN or rescan the LUNs of a SCSI host causes the OS to freeze. If you are using this driver, upgrade to the 1.4.0.145 release of the fnic driver that is available as an RPM or as a driver update disk (DUD). The former can be used to replace the in-box driver with the 1.4.0.145 fnic driver after RHEL 5.5 installation, and the latter can be used to replace the in-box driver with the 1.4.0.145 fnic driver during installation itself. The 1.4.0.145 fnic driver is also available in UCS Release 1.4(1), in the ucs-b2xx-drivers-1.4.1.iso image file. See the README accompanying the fnic rpm and DUD for specific instructions on how to use either. This bug was tracked with RedHat as bugzilla bug number 578328 ([https://bugzilla.redhat.com/show\\_bug.cgi?id=578328](https://bugzilla.redhat.com/show_bug.cgi?id=578328)).
- The LSI 1064E RAID controller in the B200 and B250 runs at 1.5-GB link speed instead of 3-GB with all 6-GB disks using UCS 1.4 and earlier releases.
- If a RAID cluster is migrated, if during the reassociation process the service profile is shown as “Any Configuration” instead of a specific RAID level, the RAID LUN will remain in an “Inactive” state, and will not boot. To avoid this issue, reassociate the server using exactly the same Policy setting instead of “Any Configuration”.
- We recommend that you follow the industry standard practice of using drives of the same capacity when creating RAID volumes. If drives of different capacities are used, the usable portion of the smallest drive will be used on all drives that make up the RAID volume.
- When installing ESXi 4.0 U2 or 4.1 to a local SSD on a B230, do not use the standard install package. There are driver compatibility issues that require installing a customized ISO image. The image is available by going to [http://downloads.vmware.com/d/info/datacenter\\_downloads/vmware\\_vsphere\\_hypervisor\\_esxi/4\\_0#drivers\\_tools](http://downloads.vmware.com/d/info/datacenter_downloads/vmware_vsphere_hypervisor_esxi/4_0#drivers_tools) and then selecting **OEM Customized Installer CDs** and the Custom Cisco ISO for the ESXi version you wish to install.

- After upgrading from a 1.3(1) to a 1.4(x) or a later release, you might see the service profile configuration disappears from an organization. To confirm that this problem has occurred, use a CLI command that begins with show service-profile. A NULL CLI output confirms the problem. This problem is most likely to occur if you created an organization with a space in its name while running a Cisco UCS Manager 1.0 release and then later upgraded Cisco UCS Manager to a 1.3(1) release. In the 1.3(1) release, spaces are not allowed in organization names and are automatically replaced with an underscore. If the system is subsequently upgraded to a 1.4(x) or later release, the old organization name with a space reappears without the space to underscore conversion and all of its children (which includes service profiles, policies, and templates) are deleted. Note: An organization that was created in a Cisco UCS 1.3(1) release or with a name that does not contain a space character will not have this problem.

To avoid this problem, do the following before upgrading from a 1.3(1) release to a 1.4(x) or a later release:

1. Change the description field of the organizations that have underscores in their names, by removing the underscores and any spaces to help keep the orgs in the database.
  2. Create a backup using the All Configuration option before upgrading. If a problem occurs after the upgrade, restore the configuration using the backup file. After importing the configuration file, reacknowledge all blades to restore their VIF status.
- When you are upgrading an Emulex adapter while you have a Cisco UCS Manager Release 1.4(4h) or an earlier release installed, the firmware upgrade fails. The failure is not dependent on the version of the Emulex adapter itself.

When performing an Emulex adapter upgrade while you are on Release 1.4, upgrade the Cisco UCS Manager firmware to at least 1.4(4i) release before upgrading the Emulex adapter. When performing a downgrade from a release higher than Release 1.4(4i) to a release lower than Release 1.4(4i), perform the Emulex downgrade first prior to performing the Cisco UCS Manager downgrade

**The following known limitations found in Release 1.3(1) are not otherwise documented:**

- With the B-250 blade server, the displayed ESX and Linux OS HDD Boot Device Order is the reverse of the BIOS HDD Boot Order. To rectify this issue, review both the disks (and drive labels as applicable), during installations of ESX and Linux versions and choose the correct disk for installation.
- Only ports 1/1 through 1/8 on the UCS 6120 Fabric Interconnect and 1/1 to 1/16 on the UCS 6140 Fabric Interconnect can be configured to use 1-GB transceivers (GLC-T, GLC-SX-MM, and GLC-LH-SM). Auto-negotiation is not supported for this change; you will need to set the speed manually in UCS Manager. All member ports of a port channel must use these ports running at the same speed, so if you need to have one member port using a 1-GB port, all other members will have to change as well.
- Even with the Protect Configuration Flag set to Enabled, user data may not be protected during a UCS upgrade from release 1.2(1) or earlier builds to release 1.3(1i) for unassociated servers, the first time the servers get associated under 1.3(1i), the ProtectConfig Property (even if ProtectConfig=YES) will not protect the user data as the association will proceed without the configuration errors. Note that the subsequent associations would be blocked if the ProtectConfig = YES and the Local Disk Configuration Policy mismatches. Associated servers will not reboot and no configuration errors will be reported.
- The Protect Configuration Flag was introduced in 1.3(1c) and so after the upgrade, this flag is Enabled in the Local Disk Policy as the default. If there is no mismatch between the Local Disk Policy of the previous SP to the incoming SP, the association should go through. Make sure that there is no mismatch; otherwise, a configuration error will be reported and association will fail.

To manually disable the Protect Config Flag (only do this if you do not care about the data in the disk) to prevent the configuration errors and allow the service profile association to go through, follow these steps:

- a. Select the service profile that you will be using to associate to the Server.
  - b. Select the Storage Tab on the right hand side pane of the service profile.
  - c. Select Change Local Disk Configuration Policy under the Storage Tab.
  - d. Disable or Enable the Protect Configuration Flag (property) as desired and save the settings.
- The Disk Fault/Error Codes, Disk Status, Alarms, and the failures forwarded by the SAS Controller are not received by Cisco UCS Manager.
  - Before you delete a VLAN from a fabric interconnect, ensure that the VLAN has been removed from all vNICs and vNIC templates. If you delete a VLAN that is assigned to a vNIC or vNIC template, the vNIC could allow that VLAN to flap.

## Resolved Caveats

The following caveats are resolved in 1.4(4l) release:

- A memory leak in the bmcd and thermal processes no longer causes the IOM to reboot due to lack of memory. (CSCtz27298)
- Transient faults related to UCS Manager chassis SEEPROM usage and power capping no longer occur. (CSCue49366)
- IOM process bmcd no longer fails to discover blades after reboot. (CSCuf34701)
- IOMs no longer crash due to a memory leak in the baseboard management controller (BMC). (CSCuf61116)

The following caveats are resolved in the 1.4(4k) release:

- The snmpd and ldapd processes no longer crash and restart when new bundle images are activated during the UCS Manager upgrade process. (CSCty33146)
- FIs no longer crash after ports are changed from fabric port to SPAN destination port and the SPAN configuration is removed. (CSCuc11474)
- Polling of SNMP objects no longer causes an eth\_port\_sec process crash. (CSCub36000)
- The following critical fault, '[FSM:FAILED]: communication service configuration (FSM:sam:dme:CommSvcEpUpdateSvcEp)' is no longer seen after disabling SNMP, or after restoring the SAM configuration when SNMP is disabled. (CSCuc53591)
- The IOM upgrade no longer fails and gets into a continuous reboot after the IOM is activated by the fabric interconnect. (CSCuc15009)
- You will no longer see random errors such as thermal-problem, performance-problem, and equipment-degraded false alarm. (CSCua96703)
- When polling ipAdEntIfIndex, you will no longer see the following error: .1.3.6.1.2.1.4.20.1.2 = No Such Instance currently exists at this OID to the MDS boxes. (CSCub84958)
- Cisco UCS Manager is no longer truncating the last digit of the license file id from the license. (CSCuc32555)
- SNMP no longer fails to return the management IP address. (CSCub90031)

- When downgrading to Release 1.4.4, the license count displayed and available is no longer greater than the licenses you have obtained. (CSCuc82895)

**The following caveats are resolved in the 1.0(63).T catalog:**

- The Cisco UCS B230 M2 and B440 M2 servers now recognize the UCS-MR-2X164RX-D DIMMs. (CSCua71178) (CSCuc32844)

**The following caveats are resolved in the 1.4(4j) release:**

- Fan module amber LED blinking and/or fans running at high speeds for no apparent reason will no longer be seen. (CSCtx49686, CSCtx52556)
- IOM with memory parity issue will no longer unexpectedly crash/hang. IOM will automatically reboot and recover without any intervention. (CSCtz15594)
- User with server-profile role and one assigned Locale can reset/shutdown/boot the server from KVM window. (CSCua54788)
- Cisco UCS Manager will show correct PSU slots for C200 Cisco UCS rack-Mount Server. (CSCua38633)

**The following caveats are resolved in the 1.4(4i) release:**

- Upon server reboot, the FCoE interfaces on Cisco UCS N20-AE0002 will always be operationally up. (CSCua37003)
- Cisco UCS 1.4(4i) release contains a fix for the adapter firmware upgrade. When you are upgrading an Emulex adapter while you have a Cisco UCS Manager Release 1.4(4h) or an earlier release installed, the firmware upgrade fails. The failure is not dependent on the version of the Emulex adapter itself.

When performing an Emulex adapter upgrade while you are on Release 1.4, upgrade the Cisco UCS Manager firmware to at least 1.4(4i) release before upgrading the Emulex adapter. When performing a downgrade from a release higher than Release 1.4(4i) to a release lower than Release 1.4(4i), perform the Emulex downgrade first prior to performing the Cisco UCS Manager downgrade. (CSCtq36461)

**The following caveats are resolved in the 1.4(4g) release:**

- The Cisco B200 M2 Blade discovery will no longer get stuck in a throttled state in a scaled setup. (CSCtx49569)
- The read-only users can no longer create any log files at the /var/home/ directory and the operation performed by the read-only users will no longer fill the "/" partition using the CLI show command. As a result, there will no longer be any remote authentication failure on the Cisco UCS Manager. (CSCua07619)
- The Fibre Channel firmware issue will no longer disrupt the SAN connectivity for the server. (CSCtz87024)
- Phase 3.0 Emulex Tigershark firmware is added to the UCS 1.4.4 release. (CSCua26726)

The following caveats are resolved in the 1.4(4f) release:

#### BIOS

- When interrupt remapping is enabled in the BIOS, the virtual Host Bus Adapters (vHBAs) and the other PCI devices respond in ESX/ESXi 4.1. (CSCth36989)
- While upgrading from the 2.0(1q) to 2.0(1s) release and from the 1.4.3 to 1.4.4 release, the host performance will no longer be affected after activating the subordinate Fabric Interconnect. (CSCtw97157)
- The interrupt remapping issue on VMware ESX is now fixed. (CSCty98534)

#### Cisco UCS Manager

- Cisco UCS Fabric Interconnect now reboots properly and no configuration files are missing. (CSCto51594)
- The CIMC activate process no longer gets stuck in the "activating" state. (CSCty56181)
- While attempting to upgrade the B230 M1/M2 CIMC firmware, the blade discovery no longer fails. (CSCtt08673)
- The HTTP version is upgraded to 2.2.21 and the OpenSSL library version is upgraded to 0.9.8q. (CSCtw88264)
- Creating a local user account will no longer fail when the password is set. (CSCtx53713)
- Cisco UCS Fabric Interconnect devices no longer restart after receiving a malformed SNMP request. (CSCts32452) (CSCts32463)
- The I2C communication issues are fixed now and the ASIC port failure message will no longer be seen. (CSCtr18730)
- FET detection algorithm version 3 is now supported in the 1.4(4f) release. (CSCty83695)
- The board temperature sensors TEMP\_SENS\_FRONT and TEMP\_SENS\_REAR are now moved to the Minor faults category in the Cisco UCS Manager. (CSCtj26813)
- Any actions on the service profile that involve a change, no longer trigger a reboot on the server. (CSCty10870)
- When a service profile is in the config-failed state and some of the previously allocated VLANs are deleted, the deleted VLANs now get counted in the access port VLAN count. When a service profile comes out of the config-failed state upon reducing the border port VLANs, the access VLAN port count is consistent with the actual number of the access port VLANs. (CSCty37323)
- The DME process on one Fabric Interconnect no longer crashes after a peer Fabric Interconnect is in an inoperable state. (CSCty90643)
- The PNUOS image now gets updated during the Cisco UCS build upgrade process as expected and the HDD/SSD operability is now reported correctly. (CSCtq45199)
- The permissions on the /dev/null directory on a primary Fabric Interconnect are now corrected, and the Fabric Interconnect can now join as a secondary device. (CSCto94998)
- When the Cisco UCS Manager is upgraded from 1.3(x) release to either 1.4(x) or 2.x release before upgrading the Fabric Interconnects, an internal process no longer crashes and both the Fabric Interconnects receive the Cisco NX-OS firmware. (CSCty19988)
- The Cisco UCS Manager cluster election process is now improved in case of the chassis and the Fabric Interconnect failure. Primary election now happens automatically after a power failure. (CSCtx66751)

**Fabric Interconnect**

- Fabric B connected to the Cisco Nexus 5000 series platforms no longer fails in the NPIV process during a stable state. (CSCts53457)
- An internal process no longer crashes on a Fabric Interconnect running the Cisco UCS Manager 1.4.3l release and the Fabric Interconnect does not reboot unexpectedly. (CSCtx41463)
- The Ethernet Port Channel service on the Cisco UCS 6200 Series Fabric Interconnect no longer crashes when the system is in a steady state. (CSCtx79272)
- The Fibre Channel span port now works for the Port Analyzer Adapter (PAA) on the 8-GB expansion module with the Cisco UCS Manager 1.4.3 release. (CSCty05262)

**Security**

- Cisco UCS Fabric Interconnect devices no longer write sensitive SSL key material to the system log when a new CSR request is generated. (CSCtq86508)
- An internal service account can no longer authenticate to the Cisco UCS Fabric Interconnect from an isolated internal network. (CSCtq86534)
- While attempting to access the system using the vKVM, the “Login Failed” message is no longer seen. (CSCtq94963)
- With the ls-config-policy or the ls-server-policy privileges, you can now add or modify the contents of a firmware package. (CSCty43432)
- The Apache Web Server ETag HTTP response header will no longer display the static file attributes. (CSCty45689)

**The following caveats are resolved in the 1.4(3y) release:**

- A denial of service vulnerability was found in the way the multiple overlapping ranges are handled by the Apache HTTPD server as described in <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110830-apache>. The vulnerability has been resolved. (CSCts33291)
- When activating a blade controller image, only images appropriate for that blade are presented. (CSCtw73436)
- A board controller firmware upgrade of a B230-M1 or B230-M2 blade no longer gets stuck when updating it after a system upgrade. (CSCtx96515)

**The following caveats are resolved in the 1.4(3u) release:**

- When a third party Converged Network Adapter which does not support IO Virtualization (or VNTag) is used but experiences a failure, instead of bringing down the IOM backplane interface the uplink port it is pinned to, the user is allowed to control the behavior and the configuration in the network control policy is honored. This will occur even when the network control policy has the uplink failure action set to bring the link down. Note that the default uplink failure action is to bring the IOM backplane/host facing port down. So users who upgrade to this version will see a change in the default behavior if they had non-network managed adapters in their system. (CSCtq00634)
- When upgrading UCS Manager from 1.3(1) to 1.4(3u) the servers no longer reboot on UCS Manager activation. (CSCtu17091)
- Board controller firmware upgrade on the B250 server will now complete as expected. (CSCtw70911)



- If you notice an installation or deletion of license files hung in an "installing" or "deleting" state, a subsequent installation and deletion operation will recover the failure for this license file. (CSCtq59732)
- When SNMP is enabled and the HA policy is set to "reboot," an unexpected reboot of both Fabric Interconnects with an SNMP crash and a reload reason provided as "Service: snmpd hap reset" no longer occurs, and the system will simply failover to the standby interconnect as expected. (CSCtt99770)
- PVLAN traffic will now flow for an isolated host with a UCS M71KR or UCS M81KR adaptor. The isolated host MAC is now learned on both the isolated VLAN and the primary VLAN. (CSCts53607)
- After upgrade from 1.3 to 1.4, all SAN connectivity is lost when an invalid OUI is used. The 1.4 release now non-disruptively enforces the proper OUI format when using Cisco OUI in the nWWN and pWWN. (CSCtv21887)
- B250 servers with a DDR3 voltage regulator no longer see uncorrectable ECC errors in logs with no DIMMs mapped out on reboot. (CSCtu01217)
- As seen from fabric interconnect, an HIF port on a UCS M71KR no longer goes down for few seconds and comes back up due to a crash and restart of adapter firmware. (CSCts86550)
- Multiple chassis decommission/recommission operations no longer result in incorrect computation of the Access port VLAN count. (CSCtu22407)

**The following caveat is resolved in the 1.4(3s) release:**

- Updating a maintenance policy on a vNIC no longer causes VIF connectivity flaps. (CSCts60501)

**The following caveats are resolved in the 1.4(3q) release:**

- EVC mode on B230 servers using Intel Xeon processors and VMware Virtual Center is now fully supported. (CSCtr63210)
- The DIMM bus speed is no longer restricted to 1067 MHz in DDR performance mode on B250 blade servers. (CSCtr13077)
- The BIOS will correctly initialize Intel Westmere-EP CPUs on a B200-M2 or B250-M2 providing the performance expected. (CSCtq84985)
- When updating a Service Template there is now a clear warning that changing a server pool assignment will result in a server reboot and association state change.
- DME will no longer crash when disassociating or associating service profile when an incorrect value of AssignToDN is detected. (CSCtr65550)
- UCS Manager debug log files will persist after a fabric interconnect reboot. (CSCtq10224)
- IO Module ambient temperature sensors are accurate. (CSCtq13905)
- False positive chassis thermal issues, power redundancy failures, PSU or fan module presence state changes due to I2C bus locking are no longer seen. (CSCtr65585)
- The default LV DDR BIOS setting now defaults to power saving mode on B250 servers. (CSCts07534)

**The following caveats are resolved in the 1.4(3m) release:**

- UCS Manager "named-policy-unresolved" faults will now be cleared when a policy is deleted and a new policy is assigned to a service profile or service/vnic template. (CSCtq15342)

- Restarting some UCS Manager processes no longer causes a race condition in which a service profile is reported as operable even when the associated physical server is powered off and reported as unassociated. (CSCtr44885)
- While upgrading to UCS software release 1.4 with specific vSAN config values, DME no longer crashes. (CSCtr16422)
- The fabric interconnect no longer reboots giving a reset reason of "fwm hap reset" indicating the fwm process has core dumped. (CSCtq07287)
- The fabric interconnect can no longer be elected as the spanning tree root bridge resulting in sub-optimal network paths or topologies. (CSCstr09796)
- VNICs not actively carrying traffic on some of the VLANs no longer unnecessarily consume MAC table entries. (CSCto91833)
- In a 1 CPU B230 or 2 CPUs B440, a critical thermal fault saying "Temperature on chassis x is upper-non-recoverable" is no longer raised due to missing sensor readings for the uninstalled CPUs. (CSCtr29409)
- 100GB SSD discovery will no longer fail in the blade and rack servers. (CSCtq98495)

**The following caveats are resolved in the 1.4(3i) release:**

- A protection algorithm was implemented to prevent damage in case of a power transistor failure. (CSCtr05373)

**The following caveats are resolved in the 1.4(3i) release:**

- Background processes no longer cause clogging of the MTS queue. (CSCtq03411)
- Power supplies no longer show up as functioning when they are failing to provide DC power to servers. (CSCto48803 and CSCto76305)
- Connectivity problems in slot 3 of a UCS 5108 chassis causing I/O failures to I2C devices are no longer seen. (CSCtq10987 and CSCto68535)
- ESXi boot up no longer hangs when initializing the scheduler. (CSCtj19224)
- B200 servers no longer hang around the 6 minute mark hang while executing Memtest86+. (CSCto49133)
- A Nehalem-EX based blade running the VMware hypervisor no longer sees lower VM efficiency than expected when compared to other blades using a different Intel architecture. (CSCtq00382)
- DIMMs in a B250 blade no longer display random uncorrectable ECC errors. (CSCtq08997)
- After changing the VLAN list for an Appliance port via the 'Configure VLAN' option, the window closes as expected. (CSCto81948)
- The BIOS default value for the Processor C6 Report no longer causes performance or power related issues. (CSCtq11300)
- Using a DNS server without dynamic DNS capabilities no longer causes a failure to associate a service profile or discover a blade. (CSCtq11608)

**The following caveats are resolved in the 1.4(2b) release:**

**UCS Manager**

- Blade and Rack Servers that include unequal sized HDDs or SSDs can be used. (CSCtk55618)

- BIOS files no longer go missing during an upgrade to 1.4(2) from a release prior to 1.4(1). (CSCt148689)
- UCS Manager-Vcenter communication now functions as expected, and does not produce an error message. (CSCt198317)
- Custom pointers to default or custom certificate files function as expected. (CSCtn46746)
- Fiber channel ports will now auto-negotiate to speeds greater than 2Gbps, even if a SPAN session is deleted prior to removing any FC interfaces, defined as destination ports, from the FC SPAN session. If this fault is still seen in a system running release 1.4(2), check the running configuration of NX-OS to see if the speed has been hard set to 2Gbps. (CSCtn82207)
- A chassis with three power supplies whose policy is set to n+1 shows the expected status in the status window. (CSCt192106)
- If you create a Service Profile and do not specify a solPolicyName, a usable default will now be applied. (CSCt188314)
- When you use the **show cli history** command to view the commands executed in that shell, the time stamp field is correct. (CSCtg97581)
- Attempting to delete a VLAN or modify an Appliance Port/Port Channel works as expected. (CSCt107693)
- When an associated blade is removed or re-inserted, BIOS tokens are now automatically re-deployed from UCS Manager. (CSCtk82286)
- If a post on error token is set, and the BIOS later encounters an error during boot, the boot will not be halted. (CSCtk96784)
- When the primary interconnect is using an authentication mode other than local, the software behaves as expected. (CSCtj50268)
- Cisco UCS Manager no longer experiences http service failing or unexpectedly restarting. (CSCto56777)
- System Inventory Callhome messages no longer fail when the number of chassis exceeds 12. (CSCtk84080)
- The primary fabric interconnect will complete the reboot sequence as expected. (CSCt105535)
- After a downgrade from 1.4(2) to release 1.1, a chassis or blade no longer fails discovery. (CSCtk68545)
- During upgrade from 1.3(1n) to 1.4(2b) blades are no longer unexpectedly rebooted. (CSCtn31824)
- A UCS system with B200-M2 no longer produces numerous false positive over-voltage messages. (CSCtj87747)
- When assigning a blade to a UUID pool (such as the default UUID pool) that doesn't have available resources, reboot warnings and config failure preventing a blade reboot no longer occurs. (CSCt146139)
- When attempting to upgrade the Capability Catalog, synchronizing the upgrade with the subordinate fabric interconnect now functions correctly. (CSCt109603)
- A **capture show tech-support chassis all** detail with a file size of zero is no longer unexpectedly generated. (CSCt151633)
- HDD Fault Detection, Monitoring functionality, and the 'Operability' field for the local HDDs on a UCS no longer produce false positive indications of a hardware issue, and instead will in most cases read "n/a" (CSCtn12666)

- A blade server status LED blinking due to a faulty DIMM will be accompanied by a fault generated in UCS Manager. (CSCto54541)
- The UCS Manager core file tftp exporter now correctly transfers core files as binary. (CSCtl45687)
- You will no longer see excessive chassis fan speed due to fan controller status read or write errors. (CSCtl74710)

#### Fabric Interconnect

- Fabric failover functions correctly for all servers even if the interface list is not properly processed by an interface card. (CSCtn06862)
- Faulty SNMP traps with agent-addr set to 0.0.0.0 are no longer sent and no longer affect integration with third party management systems. (CSCtn27661)
- The Fabric Interconnect no longer reboots during creation of a large number of VHBAs. (CSCtn11656)
- A Fabric Interconnect will no longer reboot generating an Ethpm core file due to a missing heartbeat event. (CSCtn11671)
- Fabric interconnects no longer reboot during an SNMP walk operation. (CSCtl92511)

#### BIOS

- The operating memory speed and operating memory voltage no longer shows up as “N/A” in discovered state, both in the GUI and CLI. (CSCth93460)
- B200 servers no longer hang while executing Memtest86+. (CSCto49133)

#### CMC

- False SEL events are no longer generated for CPU temperature sensors. (CSCtl04398)
- UCS Manager no longer gives false critical temperature warnings. (CSCti08803)
- Fans operating normally or at maximum speed no longer falsely show up in UCS Manager as inoperable. (CSCtl43716)
- A B230 with one CPU no longer fails discovery. (CSCtl72727)

#### Adapter Cards

- When the DHCP server is using option 67 (RFC 2132) to report the bootfile name to the PXE client, a UCS server with an M81KR adapter, the server will PXE boot correctly. (CSCtl91488)

### The following caveats are resolved in the 1.4(1m) release:

- After upgrading to 1.4(x) from 1.3(1), licensing information for ports under the default 8/16 count on fixed modules are as expected. (CSCtl22487)
- If the UCS system domain name is invalid according to the standard for 1.4(1), you will still be able to log in to the GUI after the upgrade. (CSCtl22245)
- Upon detecting memory errors, error counts get updated as expected. (CSCtl53748)
- Having a B440 server with two CPUs no longer causes misleading faults that trigger 100% fan speed to cool CPUs that are in fact at a normal temperature. (CSCtl71804)
- Upgrade to UCS Manager 1.4(1m) now completes as expected. the “Failed login info: Maximum sessions reached” is no longer seen. (CSCtl85717)
- Random corruptions of the license file with characters like ^M during download no longer occurs. (CSCtl87477)

**The following caveat is resolved in the 1.4(1j) release:**

- After activating the UCS Manger Software during upgrade from releases prior to 1.3(1p) you no longer lose the ability to log into the UCS Manager GUI. Upgrading to release 1.3(1p) before continuing to release 1.4(1j) is not necessary. (CSCt122248)

**The following caveats are resolved in the 1.4(1i) release:**

**TFTP**

- When downloading an image or bundle using TFTP or FTP, the download task no longer appears to be stuck at 2% or fails completely. (CSCt66646 and CSCt99193)
- Fault messages are correctly logged if the UCS Manager is unable to complete a TFTP copy of the core files. (CSCt42855)

**Adapters**

- For both rack and blade servers, if unsupported adapters are installed, discovery of the server will fail. If an unsupported adapter is found in a server, an appropriate error message will appear. (CSCt59558)
- The link between the Fabric interconnect and the Adapter no longer flaps when a large number of VMs (30) are “Powered On” simultaneously. (CSCt73499)

**Cisco UCS Manager**

- A fabric extender can now report the reason for a reset if the reset is caused by the power level going out of tolerance. (CSCt13227)
- UCS Manager allows 17 characters in the callhome phone number. (CSCt08699)
- Remote authentication no longer fails when there are simultaneous logins. (CSCt46727)
- UCS Manager now allows the ~!@#%&\*()\_+|:~[-];,.characters for Datacenter, Folder and DVS names. However due to the XML parser limitations, the ^ = < > / \ " ' special character are still not allowed: (CSCt93987)
- The Call Home example for a phone number now conforms to user input constraints. (CSCt06380)
- Before creating a service profile clone, UCS Manager checks for existing service profile names. (CSCt63284)
- Manually triggered adapter activation functions as expected. (CSCt89868)
- The assignment of servers to dynamic pools is now an automatic process. (CSCt06882)
- 82598KR-I adapter firmware running version and startup version displays correctly after adapter FW upgrade. (CSCt40158)
- The administrator is able to log in as expected after a domain name change followed by a reboot. (CSCt46930)
- When the time-based UUID generation method is used in the UUIDgen tool, the system no longer reports duplicate UUIDs. (CSCt40790)
- Users will no longer get an error indicating that a UUID is in use when it is not. (CSCt59481)
- A service profile will no longer associate even if the VLAN-Port instances count is reached. (CSCt41935)
- The system now initializes more quickly when a large number of virtual interfaces is configured. (CSCt59681)

- Removing blades that have not been previously decommissioned no longer leads to undefined or missing slots if a new blade is subsequently inserted. (CSCtd86292)

#### UCS Manager GUI

- The “Gracefully shutdown OS” option in the GUI functions as expected. (CSCtc77623)
- When the “Cleared” check box in the fault table is de-selected and someone clears SEL logs or any such log, the table no longer displays that fault entry. (CSCte05392)
- The UCS Manager GUI no longer shows Admin Speed (gbps) 1 and 10 for UCS 6120 fabric interconnect ports beyond 1/8. (CSCtg48718)

#### Fabric Interconnect

- When you set a TFTP core exporter IP address through Cisco UCS Manager, the fabric interconnect will no longer accept the address if it is malformed. (CSCsz75747)
- System messages are shown on the terminal monitor when logging on a terminal monitor is enabled globally and on a particular session. (CSCta31689)

#### Fabric Extender

- After upgrading Cisco UCS 2104XP Fabric Extender firmware, IOM Status LED no longer stays amber without UCS Manager failing to detect errors on the fabric extender. (CSCtk00601)

#### C-series Integration

- Rack Server association no longer fails with an “Error Configuring Local Disk Controller” error if the RAID-1 is configured in the Intel ICH10R On-board Controller environment. (CSCti97414)

#### RAID Controller

- UCS Manager is now properly reporting a bad drive with a defective SAS interface as inoperable. (CSCtg42960)

#### KVM

- Keyboard strokes pressed during the boot sequence are no longer ignored by the KVM Application because the KVM Tab has lost focus. (CSCte36910)

#### BIOS

- If the CPUID of the installed CPU is 206C2, a system hang, reboot or memory ECC errors will no longer occur when exiting the package C6 state after updating the BIOS to the 1.4(1) version. (CSCtj38908)
- Some installed DIMMs will now be correctly enabled following a reset. (CSCtk63217)
- A UCS B250-M2 with all low voltage DIMMs can now use performance mode as expected. (CSCtj80122)
- Misleading error messages are no longer sent from a B200 M2 with LV DIMMs installed. (CSCth93217)
- When a NIC is not present in the system, or is not part of the boot order, the BIOS no longer produces the prompt “Press F12 to boot from the Network”. (CSCsz44683)
- If a single DIMM in a channel is marked faulty during BIOS POST, the channel is no longer marked faulty and empty DIMM slots are distinguished from faulty DIMMs. (CSCsz73464)

- After clearing the CMOS, Service Profile disassociation no longer takes up to 20 FSM iterations to finish, the virtual media KVM interface no longer incorrectly indicates it will boot to the EFI Shell, and the BIOS boot-order table no longer contains only the EFI-shell as a boot option. (CSCtc44331)
- ESXi boot up no longer intermittently hangs at the initializing scheduler. (CSCtj19224)

#### CIMC

- When the IO Module not controlling fan speed is unable to communicate with a fan for more than 10 minutes its health LED no longer turns amber unexpectedly. (CSCtg85906)

## Open Caveats

Caveats opened in earlier builds of a release are still open unless noted otherwise in the bug record.

### The following bugs were found in Release 1.4(4I):

**Symptom** ‘Application Blocked by Security Settings’ error when starting the Cisco UCS Manager GUI or KVM Console application. (CSCUo78883)

Because the Java Code Signing Certificate expired, users on Java 7 update 40 or higher might see the following message:

```
Application Blocked by Security Settings
Your security settings have blocked an application signed with an expired or
not-yet-valid certificate from running.
```

**Workaround** To fix this issue, you can either temporarily lower your Java security settings to add Cisco UCS Manager as an exception, or if you are using Java 7 update 51 or higher, you can add the Cisco UCS Manager host IP address to the Exception Site list.

To temporarily lower your security settings:

1. Start your Java Control Panel. The location may vary depending on your operating system and browser preferences.
2. Lower the Security level to Medium.
3. Start Cisco UCS Manager.
4. At the warning message, check the “I accept the risk and want to run this application” checkbox and click **Run**.
5. Return to the Java Control Panel and reset your security level.

To add the IP address to the exception site list (for Java 7 version 51 and higher):

1. Start your Java Control Panel. The location may vary depending on your operating system and browser preferences.
2. In the Security area, click the Edit Site button to add the IP address to the list.  
If you use HTTPS to access Cisco UCS Manager, ensure that you have the correct prefix.
3. Click **OK**.

**Symptom** When the Fibre Channel Forwarder (FCF) MAC is learned dynamically, it is treated as a MAC move. SAN traffic stops working and the FI loses the data path. This affects devices configured in either NPV or FCoE (FCoE Forwarder). (CSCug14669)

**Workaround** Do the following:

- Remove the device source that injects the duplicate MAC address into the L2 infrastructure.
- Flap the FC/FCoE link that initially owned this MAC address.

**Symptom** The FIs reset with the following error message, usually after 780 days of uptime:

```
%SYSMGR-2-SERVICE_CRASHED: Service "monitor" (PID XXXX) hasn't
caught signal 6 (core will be saved).
%KERN-0-SYSTEM_MSG: writing reset reason 16, monitor hap reset -
kernel
```

**Workaround** Do the following:

- Configure a SPAN and do not enable it for Ethernet SPAN session.
- Reset the FI during a maintenance window after around 770 days of uptime. (CSCug20103)

**Symptom** Adding VLAN to VNIC triggers reboot notification. (CSCue52164)

**Workaround** Upgrade UCS Manager to release 2.1.1a.

**Symptom** If you have Java 1.6, update 45 installed, when you launch KVM console from Cisco UCS Manager, you will get the following error:

```
"Cannot run program "C:\\Program": CreateProcess error=2, The system cannot find the file
specified"
```

**Workaround** Do one of the following:

- Downgrade Java to 1.6 Update 43 or lower. If you cannot downgrade Java, you can access the KVM from the KVM Manager.
- Uninstall Java, and reinstall in a different location with no spaces in the path. For example, "C:\Java\jre6".
- Launch KVM through `http://<UCSM-IP>/ucsm/kvm.jnlp`, which prompts for the username/password and the server's KVM IP. (CSCug40752)

**Symptom** Cisco UCS Manager displays sporadic `error accessing shared-storage` errors. Transient Call Home fan alerts or IOM boot-up errors might also be seen. (CSCui41165)

**Workaround** There is no known workaround for this issue.



**The following bugs were found in Release 1.4(4k):**

**Symptom** If you have installed unsupported DIMMs in the blade server, and upgrade to a new catalog version that supports those DIMMs, not all of the DIMM information is displayed when the DIMMs are discovered. (CSCuj63448)

**Workaround** This is a cosmetic issue. You can reacknowledge the blade server to fix the issue, but that is disruptive.

**Symptom** On some Cisco UCS B200 M2 blades running bare metal Windows 2008 R2 SP1, the Onboard Failure Logging (OBFL) fills up with OS IPMI information related to the the Windows Power Meter. (CSCud51076)

**Workaround** There is no known workaround for this issue.

**Symptom** An SNMP trap with a blank cucsFaultDescription is being sent for FAN fault. (CSCud65983)

**Workaround** Confirm the FAN status with Cisco UCS Manager.

**Symptom** The Cisco UCS P81E VIC VMware driver 2.1.2.38 cannot be installed. Upgrading via VUM displays an error stating that the package is invalid. Installing the driver manually using the CLI displays an error stating that the driver is not signed. (CSCud64349)

**Workaround** There is no known workaround for this issue.

**The following bugs were found in Release 1.4(4j):**

**Symptom** In some cases, after upgrading and activating Cisco UCS Manager, SNMP crash reboots both FIs. (CSCub34939)

**Workaround** There is no known workaround for this issue.

**The following bugs were found in the 1.0(57).T catalog:**

**Symptom** The Cisco UCS B230 M2 and B440 M2 servers fail to recognize the UCS-MR-2X164RX-D DIMMs.

**Workaround** Upgrade to the 1.0(63).T catalog (ucs-catalog.1.0.63.T.bin). (CSCua71178) (CSCuc32844)

**The following bugs were found in Release 1.4(4f):**

**Symptom** On the Cisco UCS B230 and B440 systems, the temperature sensors for the memory buffer return a false value that is higher than the upper non-recoverable value. The system event logs are generated for the temperature sensors. (CSCty85611)

**Workaround** This issue is likely to occur when the system runs a memory intensive application, for example, a memory stress test. This is not a hardware issue. The system event logs that are generated for the temperature sensors can be safely ignored.

**Symptom** The Java download link on the GUI login page currently directs the user to a latest version of Java for download. In Cisco UCS Manager 1.4, only Java version 1.6 is supported. (CSCtz78507)

**Workaround** Download the correct version of Java 1.6 from Oracle Website.

**Symptom** When running the Cisco UCS Manager from a Cisco UCS 2.0 release and running the system image from a Cisco UCS pre-2.0 release, there may be an additional delay of approximately 2-4 minutes before the Cisco UCS Manager system starts to process the configuration. This issue happens because of a known issue in one of the Cisco UCS Manager application gateways. (CSCtz56680)

**Workaround** There is no known workaround for this issue. Apart from the delay, there is no functional impact on the Cisco UCS Manager.

**Symptom** After upgrading the CIMC/board controller firmware images using the host firmware package and the management firmware package, the blades reboot on performing a configuration change on the service profile. (CSCty83359)

**Workaround** If the current CIMC firmware version is between 1.4.0 and 1.4.3s or 2.0 and 2.0.1t, first upgrade the CIMC firmware to a version that supports the board controller firmware upgrade. Once the CIMC firmware is upgraded, upgrade the board controller. Note that performing this action will reboot the blade.

**The following bugs were found in Release 1.4(3m):**

**Symptom** If a hot spare is added in a B200 or B250 server by replacing the bad disk in the RAID array, the Auto Rebuild will fail.

**Workaround** The rebuild must be started manually. (CSCtr66115)

**The following bugs were found in Release 1.4(3i):**

**Symptom** A failure has been observed where a MOSFET power transistor failed in a manner that caused it to overheat and emit a flash before failing. There is no indication of a systemic issue with the MOSFET components, and the observed failure in the field is considered to be a random component failure.

**Workaround** UCS B440 users are strongly encouraged to install UCS Blade Management Controller software version 1.3(1w) or 1.4(3L) in order to mitigate potential for overheating. The software can be downloaded from Cisco.com. See FN-63430 for more information. (CSCtr05373)

**The following bugs were found in Release 1.4(2b):****UCS Manager**

**Symptom** Failed discovery of blade servers, disassociation of service profiles and I/O module link failure faults which could be caused by a message queue getting filled and not getting drained.

**Workaround** Upgrade software to release 1.4(3i) (CSCtq03411. See the [software deferral notice](#).)

**Symptom** Associated or discovered rack servers do not come up after downgrading only UCS Manager from 1.4 release to lower releases, then returning to 1.4 from lower releases.

**Workaround** Always decommission rack servers and fabric extender before downgrading to releases lower than 1.4. Alternately, do not downgrade UCS Manager alone, instead downgrade all the three images (kernel, system and UCS Manager). On upgrade again upgrade all three images. Both downgrade and upgrade will reboot the fabric interconnect. After coming back to 1.4, unconfigure then reconfigure the switch ports connected to rack servers. If you forgot to decommission the rack servers and fabric extender before downgrade and downgraded only the UCS Manager, then after upgrading back to the 1.4 release reboot the switch and unconfigure then reconfigure the switch ports connected to rack unit adapters. (CSCtn84605)

**Symptom** Nexus 2248 Fabric Extenders show up as a chassis after a downgrade from a 1.4 release. Fabric Extenders are only supported from release 1.4 onwards. If you must downgrade from 1.4 to a previous release, the fabric extender should be decommissioned while in the supported 1.4 release. If the extender (which shows up as a chassis) is decommissioned in the pre 1.4 release, it will not be discovered upon re-upgrading back to 1.4.

**Workaround** If downgrading to pre-1.4 releases, then decommission the fabric extender prior to downgrade. If the downgrade was done without decommissioning the fabric extender, then do not decommission the fabric extender in the downgraded release. Instead upgrade back to 1.4 and decommission in 1.4. (CSCtl91937)

## BIOS

**Symptom** If the installed DIMMs do not have thermal sensors (the most likely cause as this warning is logged during initial system memory initialization) or the installed DIMMs exceeded the thermal threshold values programmed in either the memory controller or the Memory buffer, then the RankMargintest file in the BMC shows the following warning code:

```
MRC - Warning Code:0x9 on Socket#1 Br#0 Ch#00, Ddr#00, Dimm#00, Rank#FF (if applicable)
MRC - Warning Code:0x9 on Socket#1 Br#0 Ch#00, Ddr#01, Dimm#00, Rank#FF (if applicable)
```

**Workaround** None. The message is informational, and can be ignored. (CSCtn09020)

### The following bug was found in Release 1.4(1j):

**Symptom** If the UCS system is running UCS Manager firmware prior to release 1.4.1 and a new firmware bundle for Release 1.4.(1i) or (1.4.1j) for B or C series are downloaded then a total of four BIOS files will go missing. This issue is caused by internal BIOS image format change in the 1.4.1 release which was not previously known.

The 4 files will show as deleted under the **Equipment** -> **Firmware Management** -> **Packages** screen.

The files which will show as deleted in B-series are  
ucs-b230-m1-bios.B230M1.1.4.1c.0.120820101441.bin and  
ucs-b440-m1-bios.B440M1.1.4.1b.0.120820101442.bin

The files which will show as deleted in C-series are: ucs-c200-bios.C200.1.2.2f.0.112720102041.bin  
and ucs-c250-bios.C250.1.2.2f.0.112820100448.bin

**Workaround** Remove the downloaded C and B-Series firmware bundle and repeat the download when the new 1.4.1 UCS Manager code is activated. (CSCtl48689)

### The following bugs were found in Release 1.4(1i):

#### Upgrade

**Symptom** Under certain conditions, the VIC adapter fails after upgrade due to FRU corruption.

**Workaround** Contact Cisco customer support.

**Symptom** If the UCS system domain name is invalid, you will not be able to log in to the GUI after the upgrade. A blank name is allowed. Prior to UCS Manager 1.4(1i) invalid characters were allowed in the UCS system domain name. Allowable characters are upper and lower case a through z, numbers 0 through 9, and hyphens except as the first character of the name. A period is allowed for the extension (such as .com) but no other punctuation or spaces are allowed.

**Workaround** Using the UCS Manager GUI or CLI (use the **set domain** command), set a valid UCS system domain name before upgrading to this release. (CSCtl22245)

**Symptom** When trying to log into the GUI you experience a java error: “Login Error: java.net.SocketTimeoutException: Read timed out”. This may happen after upgrade to version 1.4(1i) from version 1.2(1) or earlier. After activating the UCS Manger Software you lose the ability to log into the UCS Manager GUI.

**Workaround** Upgrade to version 1.4(1j) instead. (CSCt122248. See the [software deferral notice](#).)

## ESX

**Symptom** ESXi installation fails on RAID clusters with two SSDs on the B230 server. This is an LSI driver packaging issue in a particular ESXi distribution.

**Workaround** Be sure to use ESXi 4.0u2 or ESX-COS. (CSCtj63157)

**Symptom** Unable to install ESXi 4.x on systems with Intel M61KR-I, Emulex M72KR-E, Broadcom M51KR-B or Qlogic M72KR-Q CNA Adapters.

**Workaround** ESXi 4.0 U1, U2 or ESXi 4.1 does not have the updated drivers needed for these adapters so it will fail installation before trying to select an installation disk. The reason is that ESXi needs to load a network driver in order to install properly. The only adapter that is currently supported in ESXi versions prior to ESXi 4.0 U1, U2 and ESXi 4.1 is the Cisco M81KR. (CSCtj98207)

## High Availability

**Symptom** High Availability does not become ready until all 3 selected HA devices (chassis/rack-unit) have been discovered. The condition that triggers this problem is the fact that a previously functioning and fully discovered device (either chassis or rack mount server) has failed. This may be due to connectivity problems or faulty behavior. In this case the system remains in HA NOT READY state.

**Workaround** The root of the problem is a failed device. Fixing the problem in the device is the first step. If the failure is persistent the faulty device can be decommissioned to resolve the problem. (CSCth17136)

**Symptom** When UCS Manager is operated in High Availability mode, SNMP traps stop arriving as expected if the SNMP trap IP header source address field is set to the cluster virtual IP address.

**Workaround** SNMP trap recipients must not use the SNMP trap IP header source address, or be prepared for it to contain the management IP address of the currently primary fabric interconnect. (CSCth69032)

## BIOS

**Symptom** On B440 and B230 blades with a certain DIMM population, when a single DIMM is found faulty by the BIOS, other DIMMs will be marked faulty, and there is a potential for a BIOS POST failure. On the EX CPUs, the channels are grouped into “branches”. Each branch covers two adjacent channels. When a faulty DIMM is found on one channel, the other channel on the same branch will also be affected.

**Workaround** Replace all DIMMs on both channels affected. (CSCti46985)

**Symptom** The operating memory speed and operating memory voltage show up as “N/A” in discovered state, both in the GUI and CLI. These are new properties added in UCS 1.4(1) release. Also, UCSM will not be able to distinguish a BIOS-detected failed DIMM from a BIOS-detected ignored DIMM, on B440 and B230 servers. This should happen only for B440 and B230 servers, and should not happen for B200, B250, C200 and C250 servers, all of which provide SMBIOS table 203 support.

**Workaround** None available in the UCS 1.4(1) release. Upgrading to a BIOS version for B440 or B230 with 203 support is the only solution. (CSCth93460)

**Symptom** Blade and Rack Servers that include unequal sized HDDs or SSDs have encountered various failures intermittently. UCS Manager reports “Error Configuring Local Disk Controller” in most cases during these failures, though other errors are also seen.

**Workaround** Verify that the servers use equal sized disks from the same vendor. This ensures that all of the disks are of identical disk capacity. (CSCtk55618)

**Symptom** The blade appears to hang when pressing “Ctrl +C” multiple times during POST with “silent mode” enabled.

**Workaround** Disable “silent mode” or do not press “Ctrl + C” or keys that are not instructed during POST. (CSCtj61949)

**Symptom** The BIOS Setup shows less memory size and some DIMMs disabled on a B230. The SMBIOS table does not report memory info in Type 17 structure for the disabled DIMMs. The UCSM reports less memory size and some DIMMS disabled. This happens when the BIOS disables some DIMMs incorrectly when DIMMs on certain slots do not have the corresponding lockstep pairs installed. For example, configurations that can cause this failure include:

1. DIMM on slot C2 is not installed and slot C3 is installed - Causes DDR training failure that results in DIMM failure on slots C0,C1,C3,D0,D1,D2,D3.
2. DIMM on slot A1 is not installed - Disables DIMMs on slots A0, A2, A3. The NHM-EX CPU requires the DIMM0 in each DDR channel populated first before populating DIMM1 on that channel. This is an invalid configuration.
3. DIMM on slot B0 is not installed - Disables DIMMs on slots B1, B2, B3. The NHM-EX CPU requires the DIMM0 in each DDR channel populated first before populating DIMM1 on that channel. This is an invalid configuration.

**Workaround** Always populate the DIMMs in lockstep pairs, as described in the user documentation. The lockstep-ed DIMM slot pairs are A0 & A1, A2 & A3, B0 & B1, B2 & B3, C0 & C1, C2 & C3, D0 & D1, and D2 & D3. Also, it is recommended to populate the DIMMs in the following order. Blue slot pairs, White slot pairs, Yellow slot pairs, Black slot pairs. (CSCtj67835)

## CIMC

**Symptom** Network connection to CIMC is lost. There must be at least 400 host reboots or power-ons for this issue to be seen. And even with that many host reboots or power-ons, the issue may still not happen.

**Symptom** Reseat the blade. (CSCtk63908)

**Symptom** When using mirroring mode, if a UCE error happens, there is a Redundancy SEL event and also a UCE SEL event. No other details are available for the Data Parity error.

**Workaround** None. (CSCti94391)

**Symptom** For a B200-M2 when a blade is configured in Low Voltage mode, and a LPC reset is asserted it is possible for the 1.5V DDR3 sensors to cause threshold crossing SEL events. The LPC reset causes the DIMM voltage level to return to High Voltage Mode (Hardware Caused). This causes a race condition between IPMI code and the Voltage Mode monitor code. Given this race condition it is possible for IPMI to assert the threshold crossing before the monitor code notifies the IPMI stack of the Voltage Mode change. This can be identified by the fact you have a Upper Critical Voltage crossing right after a LPC reset when in LV mode.

**Workaround** 1.5V SEL entries at the time of reset can be ignored when the manual reading is not asserting past a threshold. (CSCti68905)

## Adapters

**Symptom** When rack-server have mixed adapter vendor types, behavior is unpredictable.

**Workaround** None. Do not mix adapter vendors in rack-servers. (CSCti94883)

**Symptom** If the Windows SAN boot device is an EMC Clarion array and the adapter is a M72KR-E, SAN boot can fail with a blue screen. The frequency of the failure can go up if the storage is directly connected to the Fabric Interconnect.

**Workaround** None at this time. (CSCtk69120)

**Symptom** The link from the Rack server adapter to the fabric interconnect port remains down if the SFP type is FET (Fabric extender transceiver). Currently the FET type is supported only between a fabric extender and a fabric interconnect. If the SFP used for the link between the IOM and the rack server adapter is an FET, the link will remain down.

**Workaround** Replace the SFP with one of the supported SFPs for rack server adapters. (CSCtj89468)

**Symptom** CRC errors reported on an M81KR network interface on SLES 11 SP1. This is seen under High TX and RX traffic on SLES 11 SP1. The FIFO is not cleared as fast as it should because of some delays in the PCI path. An M81KR firmware devcmd storm from the host is also investigated to be one reason for the PCI stalls. These CRC errors are actually caused by FIFO overruns on the M81KR which are in turn caused by PCI stalls. They are not real CRC errors but truncated packets (due to FIFO overrun) flagged as CRC errors.

**Workaround** Reduce the traffic load to reduce the reported CRC errors. This assumes that the CRC errors in question are generated on M81KR and that there are no bad packets entering the adapter. (CSCtj82445)

### UCS Manager

**Symptom** System detects a temporary version difference between primary and secondary switch during upgrade process from previous release to 1.4. As a result, DME process may generate a core file. The event does not impact system functionality in any way.

**Workaround** None. (CSCtl05066)

**Symptom** UCS Manager takes a long time to push configurations containing large number of port-profiles to the VMware Virtual Center (VC). This happens when large number of hosts and virtual machines (VMs) are configured (tested with 500 VMs on 60 hosts managed by same VC) and a large number of port-profiles assigned to multiple DVSEs in the VCenter.

**Symptom** Wait until the operations complete. Configuration FSM could take more than 30 minutes. Then, configure a smaller number of port-profiles (we've measured up to 92 profiles to successfully configure in around 5 minutes in above large number of hosts and VMs situation). (CSCtk97755)

**Symptom** If a post on error token is set, and the BIOS later encounters an error during boot, the boot will be halted. Subsequent re-discovery or re-association would also halt during boot.

**Workaround** Connect to KVM and manually unset the token, and then unset the token from the BIOS policy. Or, unset the token from the BIOS policy and then decommission and recommission the server. (CSCtk96784)



**Symptom** When an associated blade is removed or re-inserted, BIOS tokens are not automatically re-deployed from UCS Manager. Previous BIOS settings will remain, but the BIOS screen will not be locked.

**Workaround** Re-acknowledge the blade. (CSCtk82286)

**Symptom** When 15 or more chassis are configured in Release 1.4(1) and the system is downgraded to release 1.3(1), chassis beyond 14 are still there. This may cause some issues as the max chassis support enabled with the 1.3(1) release is 14.

**Workaround** Manually decommission chassis in the system to keep the total number of chassis to 14 before downgrading to release 1.3(1) from 1.4(1). (CSCtk69231)

**Symptom** After a downgrade to version 1.1, a chassis or blade fails discovery. The system may not respond to connection requests on a virtual IP address. This was seen when a system was downgraded from version 1.4 to version 1.1 while some chassis or blade FSM were running. The condition is not handled properly by 1.1 code.

**Workaround** Clean up the objects (chassis or blades) that have scheduled FSMs by decommissioning them and re acknowledging them. If the virtual IP address has not been programmed, connect directly to the primary switch IP address. After chassis/blades have been recommissioned, reboot the primary switch. The subordinate takes over and the VIP is reprogrammed. After the Fabric extender finishes rebooting, it can be made primary again by forcing failover (to do this, connect to local-mgmt and use the “cluster lead X” command). (CSCtk68545)

**Symptom** Attempting to delete a VLAN or modify an Appliance Port/Port Channel triggers the error message “Config for Ethernet Port P doesn’t exist for switch S.” When two or more VLANs (in global or local scope) that share the same ID are added to an Appliance Port/Port Channel and then when an Appliance Port/Port Channel is deleted or the port type of the Appliance port is changed to be different from an Appliance Port, without the corresponding VLAN association being removed, this condition will occur.

**Workaround** If the condition occurs, recreate the Appliance Port/Port Channel, delete all VLAN associations and then delete the Appliance Port/Port Channel. If the VLAN associations are deleted prior to deleting the Appliance Port/Port Channel, this condition will not occur. (CSCtl07693)

**Symptom** In order to speed up route convergence when a server (VNIC) is not reachable through one of the fabric paths (either A or B) the MAC sync feature was introduced in the 1.4.1 release of UCS which keeps the VNIC MAC address in sync between the Fabric Interconnects. This feature is not automatically enabled for service profiles that were associated and active before upgrade to the 1.4 version of UCS Manager and Fabric Interconnect software.

**Workaround** Disassociating and re-associating the service profile will automatically turn on this feature. For service profiles that are associated after upgrading to 1.4.1 version, this feature will be automatically turned on. (CSCtl05696)

**Symptom** The primary fabric interconnect fails to complete the reboot sequence, UCS Manager is not available, and Virtual IP does not respond. This can happen in an HA setup with two fabric interconnects, but one is permanently down and the other one is alive and it is primary, and the primary is rebooted. The problem occurs in one of the following configurations:

- The system contains only rack mount servers (no chassis).
- The system contains at least one rack mount server (in addition to chassis) and that rack mount server was selected as a repository for HA information. UCS Manager picks a total of 3 repositories so mixed configurations with less than 3 chassis are always affected.

**Workaround** Use the “cluster force lead” command on the primary node from the CLI. This will allow UCS Manager to finish initialization and enable the VIP for GUI access. (CSCti05535)

**Symptom** When a rack server has a local disk installed, it does not report real-time disk operability status (disk operability is reported as “N/A”).

**Workaround** None. (CSCtj18969)

**Symptom** When the UCS Manager shell mode is set to s either management or local-management mode, the CLI command **terminal monitor** is not available.

**Workaround** Use the **terminal** command in NXOS mode. (CSCtj82918)

**Symptom** The minimum power cap that can currently be set is 3400W. The chassis power cap has a lower limit of 3778 W (AC), which is internally converted to 3400 W (DC).

**Workaround** Do not enter a cap below this requirement. This requirement was derived from the need to safely allow a chassis to simultaneously boot all blades in a chassis. (CSCtj62296)

**Symptom** The UCS Manager shell does not support redirection of **show** command output to a remote file system.

**Workaround** Redirect the output to a local file in either *workspace:* or *volatile:* and then transfer the file to the remote system using the **cp** command in local-mgmt mode. (CSCti87891)

**Symptom** A DIMM which is detected by the BMC as present but SMBIOS table 203 shows it as either failed or ignored, the DIMM will show up with location information but with an incorrect and random value for the speed property. As the DIMM is already detected as failed/ignored, the incorrect speed value may be ignored.

**Workaround** Replace the failed/ignored DIMM. (CSCtj96263)

**Symptom** In UCS Manager there is no option to change the port speed of the SPAN destination port.

**Workaround** Un-configure the SPAN destination port and make it an “uplink”. Change the port speed on the uplink port, then reconfigure the port as a SPAN destination port. The port speed will be at the value that user set for the “uplink” port. (CSCti86217)

**Symptom** UCS Manager reports an unsupported DIMM as missing but does not raise a fault.

**Workaround** Verify that the DIMM is a Cisco DIMM supported on that server model. (CSCtj51582)

**Symptom** Dynamic vNIC creation fails with a message saying the port profile is not available in NPPM. This will happen if you are trying to provision more than 180 port profiles, the maximum in Release 1.4(1).

**Workaround** Delete extra port profiles and retry. (CSCtj17237)

**Symptom** If you delete existing VMware data center objects & VCenter in the VM configuration tab, then create a new VCenter with the same IP address as previous VC server. UCS Manager sends an error stating “deletion of vCenter object is still in progress” and will not allow creation of new VCenter. The deletion of the previous VCenter had not succeeded and UCS Manager keeps retrying the deletion. Since 2 VCenters with same IP cannot exist in the system, UCS Manager disallows the second VC creation.

**Workaround** Manually delete the deletion task. In the CLI, use the **show pending-deletion** command to see pending deletion tasks then delete the appropriate task using the **delete pending-deletion** and **commit-buffer** commands. Using the GUI, the task can be deleted by going to VM tab, then clicking VMware on left hand side, then going to the Deletion Tasks tab. (CSCtj03776)

### UCS Manager GUI

**Symptom** Non-disruptive pending changes may not be shown on a service profile. When a service profile has a maintenance policy that defers the application of disrupting changes to the server, user can see what changes are pending and make further changes. Disruptive pending changes are always visible on the service profile, whereas non-disruptive changes may not be shown. Non-disruptive pending changes are only shown for user convenience. This defect has no functional impact.

**Workaround** None. (CSCtj57838)

### UCS Manager CLI

**Symptom** When VIF creation doesn't follow V-motion, NPPM doesn't move the VIF to a new dynamic and the stale VIF doesn't carry the traffic any more. This would cause the SPAN to stop monitoring the traffic from the original VM.

**Workaround** Re-discover the AM's and re-create the SPAN. (CSCtj78998)

**Symptom** When you use the **show Cali history** command to view the commands executed in that shell, the time stamp field associated with each command is incorrect and shows up as 00:00:00.

**Workaround** None. (CSCtj97581)

## UCS Manager Capability Catalog

**Symptom** The following DIMM is missing from the Capability Catalog in UCS Manager, including information about the product name, PID, and VID:

Product Name: 2x4GB Kit DDR3-1333MHz RDIMM/PC3-10600

PID: A02-M308GB3-2

VID: V01

Vendor: 0x80CE

Vendor Description: Samsung Electronics, Inc.

Vendor Part Number: M393B5170FH0-YH9

Vendor Serial (SN): 0x4247988F.

This issue is cosmetic and has no impact on functionality.

**Workaround** Customers who purchased this DIMM should download the following UCS Manager Capability Catalog update from Cisco.com: ucs-catalog.1.0.16.T.bin. For information on how to activate this Capability Catalog update in UCS Manager, follow the steps in the Cisco UCS Manager CLI Configuration Guide or the Cisco UCS Manager GUI Configuration Guide. (CSCt107941)

## Fabric Interconnect

**Symptom** Fabric interconnect activation during a downgrade from 1.4(1) to 1.3(1) will fail if the setup has an active Nexus 2248 fabric extender.

**Workaround** Decommission all fabric extenders and rack-servers and completely decommission the FSM before downgrading the fabric interconnect image. (CSCtk35213)

**Symptom** The show port-security NXOS CLI command returns a negative value for the Max Addresses. This will occur when a system is configured with more than 8192 Port VLAN instances and port security is enabled on all interfaces such that more than 8192 MACs are secured.

**Workaround** Do not configure port-security such that secured Port VLAN instances is more than 8192. (CSCtj10809)

**Symptom** When an N2XX-ACPCI01 adapter port on a C-series server is connected to an uplink port on a UCS 6100 fabric interconnect, a fault message should appear because this connection is not supported, but there is no such fault message for this situation in this release.

**Workaround** None. (CSCti85875)

## CIMC

**Symptom** False SEL events are generated for CPU temperature sensors. These SEL events can occur shortly after power on of the host. A deassertion SEL event will be generated shortly after the assertion of the critical threshold crossing (1-10s after). On power on of the host, readings from the PECCI bus to the processor sometimes returns zero. This is zero reading causes the thermal SEL event.

**Symptom** If the thermal assertion is quickly followed by a thermal deassertion, the original assertion should be ignored. (CSCtl04398)

**Symptom** Rack server does not show up in GUI or CLI within reasonable delay after a recommission. This happens when a rack server is recommissioned within a very short time of its decommissioning. The server has a DHCP lease expiration time from when it was decommissioned, which is a few minutes.

**Workaround** After decommissioning, wait a few minutes before recommissioning a rack server. (CSCtj55009)

**Symptom** The Blade CIMC static management IP address assignment is not included in backups.

**Workaround** Manually record the blade CIMC static management IP address assignments, and re-enter them if necessary. (CSCtj93577)

**Symptom** The Disk Fault/Error Codes, Disk Status, Alarms and the failures forwarded by the SAS Controller are not received by UCS Manager.

**Workaround** None. (CSCsy76853)

## RAID/Local Disk

**Symptom** UCS Manager fails to report the Local Disk Failures, Faults, Alarms, Status and Disk Errors/Error Codes from the MegaRAID Controller on the B440 server.

**Workaround** None. (CSCtf73879)

**Symptom** For the B200 and B250 blade servers, the Local Disks 'Operability' field is reported as "N/A". The 'Operability' field of the Local Disks in B200 and B250 is expected to have a correct value and should not be reporting 'N/A'.

**Workaround** None. (CSCtj03021)

**Symptom** For the MegaRAID Controller on the B440 blade server, UCS Manager fails to report BBU Status, Properties and Errors.

**Workaround** None. (CSCtf84982)

**Symptom** If one or more conditions are met, UCS Manager fails to capture certain Local Disk errors. Conditions include: Mixing the SAS and SATA Local Disks in the same server; Disk spin-up or disks present but not reaching 'Ready' state; Missing Disks.

**Workaround** None. (CSCtj48519)

**Symptom** UCS Manager does not include the implementation for the Write Through, Write Back, and Write back with BBU MegaRAID Battery (BBU) Write Policies for the B440 server.

**Workaround** None. (CSCtf17708)

**Symptom** C210 and C250 rack servers are missing RAID 50 and RAID 60 support.

**Workaround** None. (CSCti39470)

**Symptom** For B200 and B250 blade servers. The Local Disks 'Operability' field is reported as "N/A".

**Workaround** None. (CSCti39470)

**Symptom** UCS Manager fails to create a single disk striped RAID config in the Storage Controller 1064E environment.

**Workaround** None. (CSCtj89447)

## Caveats from Previous Releases

### Release 1.3(1)

The following caveats were opened in Release 1.3(1i):

**Symptom** During Server Association, the following configuration error is reported - "Missing or Incompatible BIOS Image".

**Workaround** None. (CSCth84003)

**Symptom** FSM gets stuck in an Error Configuring the Local Disk Controller state due to various underlying conditions. Those can include but are not limited to the following:

- The Local Disks not getting discovered correctly or are "available/presence-Equipped" but not in a Ready state.
- Failures that can't be correctly communicated to Cisco UCS Manager can get reported as this type of error.

**Workaround** Remove and insert all of the local disks from the failing server, then re-acknowledge the server. (CSCta45805)

**Symptom** CIMC or BIOS fails to confirm that a board is running in low voltage mode before setting threshold. When threshold is set for low voltage and the board runs at high voltage, a SEL event occurs and causes amber lights to display.

For example, here is an error message for a B200-M2 with a low voltage DIMM and CPU. Voltage levels (column 2) are similar to the boards with high voltage components. The threshold is set for LV (columns 5 and 6, 9 and 10).

```
1V5_DDR3_P2 | 1.523 | Volts | nr | 1.213 | 1.290 | na | na | 1.407 | 1.494
P1V5_DDR3_P1 | 1.513 | Volts | nr | 1.213 | 1.290 | na | na | 1.407 | 1.494

P0V75_DDR3_P1 | 0.757 | Volts | nr | 0.601 | 0.640 | na | na | 0.708 | 0.747
P0V75_DDR3_P2 | 0.757 | Volts | nr | 0.601 | 0.640 | na | na | 0.708 | 0.747
```

**Workaround** None. Resolved in 1.3(1n). (CSCth93217)

The following caveats were opened in Release 1.3(1c), if they are resolved in later builds it is mentioned:

**Symptom** The UCS Manager GUI fails to provide the Local Disk Configuration Policy details if you make global policy changes and then select the Local Disk Configuration Policy after selecting the service profile.

**Workaround** Select a different service profile or a different GUI pane window and then return back to the service profile which was showing this issue. (CSCth95564)

**Symptom** When using M2 processors and Low Voltage DIMMs, the following error log messages may be seen for P0V75\_DDR3\_P1 and P1V5\_DDR3\_P1:

```
Line 503: 1f7 | 07/06/2010 10:33:44 | BMC | Voltage
P0V75_DDR3_P2 #0x14 | Lower critical - going low | Asserted | Reading 0.64 < Threshold
0.64 Volts

Line 418: 1a2 | 12/31/1969 19:00:36 | BMC | Voltage P1V5_DDR3_P2 #0x09 | Lower critical
- going low | Asserted | Reading 1.33 < Threshold 1.44 Volts
```

**Workaround** None. Resolved in 1.3(1i). (CSCth70776)

### UCS Manager

**Symptom** SNMP authentication fails when using user details configured from a third party authentication server like RADIUS and subsequently all SNMPv3 requests fail. Network management tools like Device Manager (DM), Fabric Manager (FM) will not be able to retrieve information from the UCS through SNP and are unable to display important information. SNMP only recognizes two roles "network-operator" or "vdc-admin". User accounts created on a RADIUS server who do not have these roles will not be authorized to access SNMP details.

**Workaround** Add "network-operator" or "vdc-admin" as roles to the user accounts in the RADIUS server. (CSCtg94770)

**Symptom** A standard attempt to execute Update Firmware ALL fails with a dependency on a deployed FW pack.

**Workaround** Follow the error message to execute Update All, i.e., Modify the policy to execute the update. (CSCtc69186)

### Red Hat Linux

**Symptom** When installing ESX 4.0 or ESX 4.0 Update 1 on a server with more than 190GB of physical memory, booting the ESX host fails and opens the recovery shell

**Workaround** For ESX 4.0 and ESX 4.0 Update 1, reduce the low reserved memory by setting the boot option “memLowReservedMaxMB” to 384MB. In the bootloader console, append the following to the command line: vmkopts=memLowReservedMaxMB:384. Depending on the types of devices in your network, you may have to increase the amount of low reserved-memory to achieve a better performance. For more detail, refer to: <http://kb.vmware.com/kb/1016239> (CSCtf61345)

**Symptom** Loading multiple driver disks during a RHEL 5.x installation fails.

**Workaround** Refer to the article at <http://kbase.redhat.com/faq/docs/DOC-17753> (CSCte73015)

**Symptom** When a vNIC is not in failover mode and a link down event occurs, the network traffic on the blades is disrupted with a system running RHEL 5.3.

**Workaround** This is a known issue with the ixgbe driver in RHEL 5.3 and because RHEL 5.4 is the latest release, Red Hat recommends upgrading the systems to the RHEL 5.4. If you cannot upgrade to RHEL 5.4, below are a few suggestions that has been found to work.

1. Restart the network.

```
service network restart
```

or

```
ifdown ethx
```

```
ifup ethx
```

2. Run your system with nomsi.
  - Edit /etc/grub.conf
  - Add pci=nomsi to the kernel line
  - Restart the system with this kernel



#### Note

---

Network performance may be affected since the system is running in legacy mode. (CSCte44548)

---

**Symptom** Pass-through DMA Support selection is not available in the BIOS if it was Disabled prior to the BIOS upgrade. If you had this option Disabled in previous version, the selection is hidden in the updated BIOS.

**Workaround** When you are in the BIOS Setup utility, press F9 to Load the BIOS defaults (CSCtb96792)



## Local Disk/RAID

**Symptom** After the removal or insertion of one or more local disks, their full discovery fails.

**Workaround** Re-acknowledge the server to complete the full discovery. (CSCsy80888)

**Symptom** The disk scrub policy does not meet DoD compliance.

**Workaround** None. (CSCsy20036)

## BIOS

**Symptom** Hubs that only use USB 1.0 may not properly present an attached USB device to the UCS server.

**Workaround** Avoid using USB hubs that are exclusively USB 1.0 capable. Virtually all USB hubs sold today are USB 1.0/2.0 capable. (CSCtb20301)

**Symptom** With the B-250 blade server, the displayed ESX and Linux OS HDD Boot Device Order is the reverse of the BIOS HDD Boot Order.

**Workaround** Review both the disks (and drive labels as applicable) during installations of ESX and Linux versions and choose the correct disk for installation. (CSCtd90695)

**Symptom** When memory mirroring configuration is disabled by removing a DIMM, the BIOS will switch to the Performance mode, and will not log a SEL that mirroring was disabled.

**Workaround** Check the status of the memory mirroring in **BIOS Setup->Advanced -> Memory Configuration -> Memory RAS and Performance Configuration**. (CSCsy54097)

**Symptom** When a faulty DIMM is detected in early BIOS POST (e.g. the blade was powered on with a faulty DIMM), two SEL entries will be sent to the CIMC. One entry will be logged for each DIMM.

**Workaround** Enter BIOS Setup and navigate to **Advanced -> Memory Configuration**. This menu will help to distinguish a faulty DIMM from its neighbor. (CSCsy97698)

**Symptom** When hot plugging or removing USB devices at a BIOS Setup -> Advanced -> USB screen, the Setup Utility may freeze.

**Workaround** Reboot the server. (CSCsz41907)

**Symptom** Installing EFI Native SLES 11 is not supported in this release.

**Workaround** Currently, there is no workaround. (CSCsz99666)

**Symptom** Disabling USB 2.0 through **Advanced->USB** could result in inconsistent information on that particular page. Some devices may not show up as expected. This does not results in functional degradation during POST.

**Workaround** Either don't disable USB 2.0, or ignore the resulting artifacts in the BIOS setup. (CSCta21849)

**Symptom** After resetting the CMOS the system date needs to be reset to current.

**Workaround** None. (CSCtb12390)

### Adapters

**Symptom** Failure to PXE boot a UCS server with an M81KR adapter, and there is an indication that a boot file is not found. This is seen when the DHCP server is using option 67 (RFC 2132) to report the bootfile name to the PXE client.

**Workaround** Use the DHCP “filename” setting instead of the “option file-name” setting for ISC DHCP servers or the equivalent for other DHCP servers. (CSCt191488)

**Symptom** With a server booting from SAN, a server crash may occur when an FC HBA is reset, or when a WWPN is zoned in or out on a core fabric switch, or a link flap event occurs either between the NPV switch and the host, or between the NPV switch and the core switch, or the core switch and storage. The symptoms of this problem include server hangs during normal operation, whether or not I/Os happen. It may either remain hung, or may panic and reboot. Upon a reboot, a vmcore file may or may not be present in /var/crash/ depending on whether sync to disk succeeded or not. Alternatively, the server may not crash or hang but can encounter a journal commit I/O error and the boot partition (located on a SAN LUN) will become a read-only file system. The server stays up, but nothing can be written to the necessary partition.

**Workaround** There is no workaround other than not booting from SAN. If the OS is RHEL, the fix for this issue will be in RHEL 5.5.z, and upgrading to that kernel is recommended when it releases. (CSCtf81596)

**Symptom** When a DCBXP peer on a physical interface sends two different unique identifiers in the Protocol data unit in the same session, a DCBXP process error disables the port.

**Workaround** Issue the following commands to enable the port:

```
scope chassis <Chassis Id>
scope server <Server Id>
scope adapter <Adapter Id>
scope ext-eth-if <Id>
set adminstate reset-connectivity
commit-buffer
```

Wait for a minute, the port will come up.(CSCsx42435)

## KVM

**Symptom** During the Server Power-State Management, the KVM session may be aborted with a message displaying “Network Connection Dropped”.

**Workaround** Close the KVM session(s) that have been aborted and open a new KVM session. (CSCtc53253)

## Cisco UCS Manager

**Symptom** Information about the number of CPU cores enabled is unavailable. Along with the other processor information, the UCS manager GUI and CLI don't show this info.

**Workaround** None. (CSCte12172)

**Symptom** A SMASH Command with an incorrect option should result in an “INVALID OPTION” error.

**Workaround** No work-around required. The message displayed is “COMMAND SYNTAX ERROR”. (CSCsv87256)

**Symptom** The PCIe Address for the Cisco UCS M81KR Virtual Interface Card is not seen in the GUI (or CLI). It causes no functional impact.

**Workaround** The only work around is to boot some host OS onto the blade and then determine the PCI address and map it to the MAC address (and subsequently to the VNIC). In a 2.6 kernel based Linux for instance, the /sys/class/net/<device> directory has relevant information. (CSCte58483)

**Symptom** Modification of trusted CoS policy in Service Profile does not get immediately applied to the server. If you modify the trusted CoS policy of an adapter profile in a service profile that is currently attached to a physical server, a server reboot is needed. Since it is unsafe to automatically reboot an associated server, UCSM currently does not.

**Workaround** Manually reboot the server or disassociate and reassociate the server to get the CoS policy to be applied. (CSCte44668)

**Symptom** Environment statistics for IO Module 1 are not shown.

**Workaround** None. (CSCtd14585)

**Symptom** For each Cisco UCS 82598KR-CI 10 Gigabit Ethernet Adapter, 2 interfaces show up in the OS and ethtool reports Link Detected = yes for both of them. This is only seen on Cisco UCS B250 servers.

**Workaround** Use the MAC that has the value provisioned in the service profile. (CSCtd14055)

**Symptom** One vNIC defined in the service profile boot order results in two BIOS vNICs.

**Workaround** Avoid defining two different pxelinux.cfg/<MAC> files that have different boot/install instructions. When booted, both vNICs should execute the same PXE configuration. (CSCsz41107)

**Symptom** After a full restore of the primary fabric interconnect, the subordinate fabric interconnect installation may temporarily fail with the following message:

```
Enter the admin password of the peer switch:
Connecting to peer switch... unable to connect! Password could be wrong.
Hit enter to try again or type 'restart' to start setup from beginning...
```

**Workaround** Retry the fabric interconnect installation. (CSCsz85876)

**Symptom** For a given port profile with existing VIFs, if the “Max-Ports” setting is reduced from the currently configured value to a value less than the “Used-Ports” value reported for that port profile by VMware vCenter, this is a mis-configuration. The new value for “Max-Ports” for that port profile will only be updated in Cisco UCS Manager and its update in VMware Center will fail, causing a inconsistency between Cisco UCS Manager and VMware Center Server.

**Workaround** If the need arises to reduce the value of “Max-Ports” of a given port profile, the new value should be at least the value of “Used-Ports” reported by the VMware Center for all the DVSEs for that port profile (not lower than maximum of all the “Used-Ports” values). This constraint has to be ensured manually. (CSCte12163)

**Symptom** When a service profile containing 2 vNICs and having failover enabled is applied to some adapters, the fail back timeout specified in the adapter policy for the second vNIC has no effect. The fail back timeout specified in the adapter policy and applied to the first vNIC is applied to the whole adapter and effective for both vNICs.

**Workaround** Specify the desired timeout in the adapter policy and apply to the first vNIC. (CSCsz68887)

**Symptom** Cisco UCS Manager reports incorrect v NICs or VIFs associated with a given Virtual Machine if and only if the Virtual Machine is deployed from VMware Center in Fault-Tolerance (Active-Standby) mode and the Virtual Machine happens to be the standby or FT Virtual Machine.

**Workaround** None. (CSCte45010)

**Symptom** When firmware is updated, UCSM accepts another firmware update before the completion of the current update. The new request will fail silently and lock out the selected firmware package for the next update.

**Workaround** Create a new host firmware package with a different name from the one that gets locked out which points to the same BIOS package. The new package with a different name, using the same BIOS will not be locked out. (CSCtc26149)

## Cisco UCS Manager GUI

**Symptom** When upgrading from releases prior to 1.1.1, OS-specific default adapter policies will not have the current recommended default values.

**Workaround** After an upgrade from a release prior to 1.1.1, we recommend manually changing the adapter policy parameters to the following values:

```
Eth VMWare->RSS: Disabled
Eth VMWarePassThru->RSS: Enabled
Eth default->RSS: Enabled

FC (all)->FCP Error Recovery: Disabled
FC (all)->Flogi Retries: 8
FC (all)->Flogi Timeout: 4000
FC (all)->Plogi Timeout: 20000
FC (all)->IO Throttle Count: 16
FC (all)->Max LUNs Per Target: 256
(CSCte58155)
```

**Symptom** The UCSM GUI could show all DIMMs to be in array 1, and maximum memory for a blade of 192GB for a B200.

**Workaround** This is a display-only issue, and does not affect functionality. DIMMs may be physically located in array 1 or array 2. (CSCta56527)

**Symptom** Hardware revision numbers for fabric interconnect components are not populated in the Cisco UCS Manager.

**Workaround** Enter the **connect nxos** command to connect to the native NX-OS CLI, then issue the appropriate **show sprom component** command and look for **H/W Version:** field in the command output. (CSCta12005)

**Symptom** In the Cisco UCS Manager GUI, you can only select port channels and individual uplink ports as pin targets, but the Cisco UCS Manager CLI allows you to also select port channel member ports as pin targets.

**Workaround** Port channel member ports should not be selected as pin targets, even if the Cisco UCS Manager CLI allows you to. (CSCta60495)

**Symptom** Even though there are no POST failures in the chassis, Cisco UCS Manager may sometimes display the overall status of the chassis as POST-failure.

**Workaround** Check the chassis POST messages for errors, and if there are none, ignore the Cisco UCS Manager status message. (CSCsz01878)

**Symptom** Statistics counters cannot be cleared using Cisco UCS Manager CLI.

**Workaround** Clear the counters using the Cisco UCS Manager GUI. (CSCsz47512)

**Symptom** When a cluster configuration is set up such that I/O module 1 is cabled to fabric interconnect B and I/O module 2 is cabled to fabric interconnect A, then the Ethernet devices are given ports 1 and 0. However if the setup is straight, with I/O Module 1 connected to fabric interconnect A and I/O Module 2 to fabric interconnect B, then the devices are assigned ports 0 and 1.

**Workaround** Connect IOM1 to fabric-interconnect A, and IOM2 to fabric-interconnect B. (CSCtb35660)

**Symptom** Logon access is denied for user accounts where the password field was left blank during user account creation.

**Workaround** When creating a user account, ensure that a secure password for the account is specified. (CSCta21326)

**Symptom** When more than 10 Cisco UCS Manager GUI sessions are open at the same time with remote authentication for a long time (typically for a few hours), one of the Cisco UCS Manager GUI sessions may fail to re-authenticate. This causes the session that fails the re-authentication to close. The problem does not happen when local authentication is in use.

**Workaround** Re-login to the Cisco UCS Manager GUI session when it closes. (CSCtb05260)

**Symptom** If you move from subnet A to subnet B then do a cluster failover and move back to subnet A, a Virtual IP is no longer pingable.

**Workaround** Set the VIP to a different VIP by using the following CLI commands to set it back to the original address:

```
scope system
set set virtual-ip <new address>
commit
(CSCtc55636)
```

### UCS Manager CLI

**Symptom** The UUID of the VM changes in VMware vCenter. After a VM restarts, the virtual machine node on the VM tab shows multiple instances of the same VM with one online and one offline.

**Workaround** After the VM retention period configured in the VM life cycle policy has passed, Cisco UCS Manager deletes the offline instance automatically. (CSCtc86297)

**Symptom** If multiple vHBA initiators are configured in the same zone so that they are visible to each other and can login to each other, and storage multipathing is not configured with active and standby paths through the Cisco UCS fabric interconnects (There is only one path through the primary fabric interconnect), and the primary fabric interconnect is rebooted, the vHBA driver can be exposed to a situation in which two initiators can try to login to each other at the same time, and cause a host crash.

**Workaround** Do not configure multiple vHBA initiators in the same zone, to ensure that they are not visible to each other. (CSCte36784)

**Symptom** ESX Read and Write commands sent on a vHBA keep timing out and being aborted even if the target device is logged into the network. This can happen if the link flaps very fast from up to down to up and memory allocation for the link event fails. The vHBA driver misses the link down event and it does not re-login to the fabric interconnect. The fabric interconnect, however, has no login state for the vHBA and so drops all packets from the vHBA.

**Workaround** Disable and re-enable the port on the UCS fabric interconnect that corresponds to the vHBA. (CSCte08092)

### Fabric Interconnect

**Symptom** Without pin group configuration, server interfaces are pinned to uplink interfaces of the fabric interconnect dynamically and the pinning is redistributed as uplink interfaces go up or down. In some situations, the distribution of server interfaces across uplink interfaces is not balanced. Potential impact is some uplinks are under utilized.

**Workaround** None. (CSCsv92356)

**Symptom** At bootup of the fabric interconnect, the following message will be displayed on the console: "The startup-config won't be used until the next reboot."

**Workaround** None, just ignore the message. (CSCsx13134)

**Symptom** Console login is treating the admin and ADMIN account as the same. Console login name on the fabric interconnect is not case sensitive, so there is no differentiation between e.g. 'admin' and 'ADMIN'.

**Workaround** Implement usernames that are not case sensitive. (CSCsy15489)

**Symptom** Under high stress on the system with repeated port flapping and a default or native VLAN changing simultaneously, a process may cause the fabric interconnect to reload.

**Workaround** None. (CSCta09325)

**Symptom** The **show cdp neighbor** command does not display information for CDP neighbors seen from the management interface, nor does it display the fabric interconnect CDP information corresponding to the management interface.

**Workaround** None. (CSCta25287)

**Symptom** With FM/DM version 5.0(0.295) and UCS 1.1 release, a security user defined in Cisco UCS Manager does not get displayed on FM/DM.

**Workaround** None. Verify user security from Cisco UCS Manager. (CSCte25876)

## Release 1.2(1)

The following caveats were opened in Release 1.2(1):

### Red Hat Linux

**Symptom** Loading multiple driver disks during a RHEL 5.x installation fails.

**Workaround** Refer to the article at <http://kbase.redhat.com/faq/docs/DOC-17753> (CSCte73015)

**Symptom** When a vNIC is not in failover mode and a link down event occurs, the network traffic on the blades is disrupted with a system running RHEL 5.3.

**Workaround** This is a known issue with the ixgbe driver in RHEL 5.3 and because RHEL 5.4 is the latest release, Red Hat recommends upgrading the systems to the RHEL 5.4. If you cannot upgrade to RHEL 5.4, below are a few suggestions that has been found to work.

1. Restart the network.

```
service network restart
or
```

```
ifdown ethx
ifup ethx
```

2. Run your system with nomsi.
  - Edit /etc/grub.conf
  - Add pci=nomsi to the kernel line
  - Restart the system with this kernel



### Note

Network performance may be affected since the system is running in legacy mode. (CSCte44548)



**Symptom** Pass-through DMA Support selection is not available in the BIOS if it was Disabled prior to the BIOS upgrade. If you had this option Disabled in previous version, the selection is hidden in the updated BIOS.

**Workaround** When you are in the BIOS Setup utility, press F9 to Load the BIOS defaults (CSCtb96792)

### Local Disk/RAID

**Symptom** After the removal or insertion of one or more local disks, their full discovery fails.

**Workaround** Re-acknowledge the server to complete the full discovery. (CSCsy80888)

**Symptom** The Disk Fault/Error Codes, Disk Status, Alarms and the failures forwarded by the SAS Controller are not received by Cisco UCS Manager.

**Workaround** None. (CSCsy76853)

**Symptom** FSM gets stuck in an Error Configuring the Local Disk Controller state due to various underlying conditions. Those can include but are not limited to the following:

- The Local Disks not getting discovered correctly or are “available/presence-Equipped” but not in a Ready state.
- Failures that can't be correctly communicated to Cisco UCS Manager can get reported as this type of error.

**Workaround** Remove and insert all of the local disks from the failing server, then re-acknowledge the server. (CSCta45805)

**Symptom** The disk scrub policy does not meet DoD compliance.

**Workaround** None. (CSCsy20036)

### BIOS

**Symptom** Hubs that only use USB 1.0 may not properly present an attached USB device to the UCS server.

**Workaround** Avoid using USB hubs that are exclusively USB 1.0 capable. Virtually all USB hubs sold today are USB 1.0/2.0 capable. (CSCtb20301)

**Symptom** With the B-250 blade server, the displayed ESX and Linux OS HDD Boot Device Order is the reverse of the BIOS HDD Boot Order.

**Workaround** Review both the disks (and drive labels as applicable) during installations of ESX and Linux versions and choose the correct disk for installation. (CSCtd90695)

**Symptom** When memory mirroring configuration is disabled by removing a DIMM, the BIOS will switch to the Performance mode, and will not log a SEL that mirroring was disabled.

**Workaround** Check the status of the memory mirroring in **BIOS Setup->Advanced -> Memory Configuration -> Memory RAS and Performance Configuration**. (CSCsy54097)

**Symptom** When a faulty DIMM is detected in early BIOS POST (e.g. the blade was powered on with a faulty DIMM), two SEL entries will be sent to the CIMC. One entry will be logged for each DIMM.

**Workaround** Enter BIOS Setup and navigate to **Advanced -> Memory Configuration**. This menu will help to distinguish a faulty DIMM from its neighbor. (CSCsy97698)

**Symptom** When hot plugging or removing USB devices at a BIOS Setup -> Advanced -> USB screen, the Setup Utility may freeze.

**Workaround** Reboot the server. (CSCsz41907)

**Symptom** Installing EFI Native SLES 11 is not supported in this release.

**Workaround** Currently, there is no workaround. (CSCsz99666)

**Symptom** Disabling USB 2.0 through **Advanced->USB** could result in inconsistent information on that particular page. Some devices may not show up as expected. This does not result in functional degradation during POST.

**Workaround** Either don't disable USB 2.0 (we are not aware of any need to disable it), or ignore the resulting artifacts in the BIOS setup. (CSCta21849)

**Symptom** After resetting the CMOS the system date needs to be reset to current.

**Workaround** None. (CSCtb12390)

## Red Hat Linux

### Adapters

**Symptom** With a server booting from SAN, a server crash may occur when an FC HBA is reset, or when a WWPN is zoned in or out on a core fabric switch, or a link flap event occurs either between the NPV switch and the host, or between the NPV switch and the core switch, or the core switch and storage. The symptoms of this problem include server hangs during normal operation, whether or not I/Os happen. It may either remain hung, or may panic and reboot. Upon a reboot, a vmcore file may or may not be present in /var/crash/ depending on whether sync to disk succeeded or not. Alternatively, the server may

not crash or hang but can encounter a journal commit I/O error and the boot partition (located on a SAN LUN) will become a read-only file system. The server stays up, but nothing can be written to the necessary partition.

**Workaround** There is no workaround other than not booting from SAN. If the OS is RHEL, the fix for this issue will be in RHEL 5.5.z, and upgrading to that kernel is recommended when it releases. (CSCtf81596)

**Symptom** When a DCBXP peer on a physical interface sends two different unique identifiers in the Protocol data unit in the same session, a DCBXP process error disables the port.

**Workaround** Issue the following commands to enable the port:

```
scope chassis <Chassis Id>
scope server <Server Id>
scope adapter <Adapter Id>
scope ext-eth-if <Id>
set adminstate reset-connectivity
commit-buffer
```

Wait for a minute, the port will come up.(CSCsx42435)

## KVM

**Symptom** During the Server Power-State Management, the KVM session may be aborted with a message displaying “Network Connection Dropped”.

**Workaround** Close the KVM session(s) that have been aborted and open a new KVM session. (CSCtc53253)

## Cisco UCS Manager

**Symptom** Information about the number of CPU cores enabled is unavailable. Along with the other processor information, the UCS manager GUI and CLI don't show this info.

**Workaround** None (CSCte12172)

**Symptom** A SMASH Command with an incorrect option should result in an “INVALID OPTION” error.

**Workaround** No work-around required. The message displayed is “COMMAND SYNTAX ERROR”. (CSCsv87256)

**Symptom** The PCIe Address for the Cisco UCS M81KR Virtual Interface Card is not seen in the GUI (or CLI). It causes no functional impact.

**Workaround** The only work around is to boot some host OS onto the blade and then determine the PCI address and map it to the MAC address (and subsequently to the VNIC). In a 2.6 kernel based Linux for instance, the /sys/class/net/<device> directory has relevant information. (CSCte58483)

**Symptom** Modification of trusted CoS policy in Service Profile does not get immediately applied to the server. If you modify the trusted CoS policy of an adapter profile in a service profile that is currently attached to a physical server, a server reboot is needed. Since it is unsafe to automatically reboot an associated server, UCSM currently does not.

**Workaround** Manually reboot the server or disassociate and reassociate the server to get the CoS policy to be applied. (CSCte44668)

**Symptom** Environment statistics for IO Module 1 are not shown.

**Workaround** None. (CSCtd14585)

**Symptom** For each Cisco UCS 82598KR-CI 10 Gigabit Ethernet Adapter, 2 interfaces show up in the OS and ethtool reports Link Detected = yes for both of them. This is only seen on Cisco UCS B250 servers.

**Workaround** Use the MAC that has the value provisioned in the service profile. (CSCtd14055)

**Symptom** One vNIC defined in the service profile boot order results in two BIOS vNICs.

**Workaround** Avoid defining two different pxelinux.cfg/<MAC> files that have different boot/install instructions. When booted, both vNICs should execute the same PXE configuration. (CSCsz41107)

**Symptom** After a full restore of the primary fabric interconnect, the subordinate fabric interconnect installation may temporarily fail with the following message:

```
Enter the admin password of the peer switch:
  Connecting to peer switch... unable to connect! Password could be wrong.
  Hit enter to try again or type 'restart' to start setup from beginning...
```

**Workaround** Retry the fabric interconnect installation. (CSCsz85876)

**Symptom** For a given port profile with existing VIFs, if the “Max-Ports” setting is reduced from the currently configured value to a value less than the “Used-Ports” value reported for that port profile by VMware vCenter, this is a mis-configuration. The new value for “Max-Ports” for that port profile will only be updated in Cisco UCS Manager and its update in VMware Center will fail, causing a inconsistency between Cisco UCS Manager and VMware Center Server.

**Workaround** If the need arises to reduce the value of “Max-Ports” of a given port profile, the new value should be at least the value of “Used-Ports” reported by the VMware Center for all the DVSEs for that port profile (not lower than maximum of all the “Used-Ports” values). This constraint has to be ensured manually. (CSCte12163)

**Symptom** When a service profile containing 2 vNICs and having failover enabled is applied to some adapters, the fail back timeout specified in the adapter policy for the second vNIC has no effect. The fail back timeout specified in the adapter policy and applied to the first vNIC is applied to the whole adapter and effective for both vNICs.

**Workaround** Specify the desired timeout in the adapter policy and apply to the first vNIC. (CSCsz68887)

**Symptom** Cisco UCS Manager reports incorrect v NICs or VIFs associated with a given Virtual Machine if and only if the Virtual Machine is deployed from VMware Center in Fault-Tolerance (Active-Standby) mode and the Virtual Machine happens to be the standby or FT Virtual Machine.

**Workaround** None. (CSCte45010)

**Symptom** When firmware is updated, UCSM accepts another firmware update before the completion of the current update. The new request will fail silently and lock out the selected firmware package for the next update.

**Workaround** Create a new host firmware package with a different name from the one that gets locked out which points to the same BIOS package. The new package with a different name, using the same BIOS will not be locked out. (CSCtc26149)

### Cisco UCS Manager GUI

**Symptom** When upgrading from releases prior to 1.1.1, OS-specific default adapter policies will not have the current recommended default values.

**Workaround** After an upgrade from a release prior to 1.1.1, we recommend manually changing the adapter policy parameters to the following values:

```
Eth VMWare->RSS: Disabled
Eth VMWarePassThru->RSS: Enabled
Eth default->RSS: Enabled

FC (all)->FCP Error Recovery: Disabled
FC (all)->Flogi Retries: 8
FC (all)->Flogi Timeout: 4000
FC (all)->Plogi Timeout: 20000
FC (all)->IO Throttle Count: 16
FC (all)->Max LUNs Per Target: 256
(CSCte58155)
```

**Symptom** All DIMMs are reported to be in array 1, and the max memory for a blade is reported as 192GB.

**Workaround** DIMMs may be physically located in array 1 or array 2. This is a display-only issue, and does not affect functionality. Ignore the incorrect report. (CSCta56527)

**Symptom** The UCSM GUI could show all DIMMs to be in array 1, and maximum memory for a blade of 192GB for a B200.

**Workaround** This is a display-only issue, and does not affect functionality. DIMMs may be physically located in array 1 or array 2. (CSCta56527)

**Symptom** Hardware revision numbers for fabric interconnect components are not populated in the Cisco UCS Manager.

**Workaround** Enter the **connect nxos** command to connect to the native NX-OS CLI, then issue the appropriate **show sprom component** command and look for **H/W Version:** field in the command output. (CSCta12005)

**Symptom** In the Cisco UCS Manager GUI, you can only select port channels and individual uplink ports as pin targets, but the Cisco UCS Manager CLI allows you to also select port channel member ports as pin targets.

**Workaround** Port channel member ports should not be selected as pin targets, even if the Cisco UCS Manager CLI allows you to. (CSCta60495)

**Symptom** Even though there are no POST failures in the chassis, Cisco UCS Manager may sometimes display the overall status of the chassis as POST-failure.

**Workaround** Check the chassis POST messages for errors, and if there are none, ignore the Cisco UCS Manager status message. (CSCsz01878)

**Symptom** Statistics counters cannot be cleared using Cisco UCS Manager CLI.

**Workaround** Clear the counters using the Cisco UCS Manager GUI. (CSCsz47512)

**Symptom** When a cluster configuration is set up such that I/O module 1 is cabled to fabric interconnect B and I/O module 2 is cabled to fabric interconnect A, then the Ethernet devices are given ports 1 and 0. However if the setup is straight, with I/O Module 1 connected to fabric interconnect A and I/O Module 2 to fabric interconnect B, then the devices are assigned ports 0 and 1.

**Workaround** Connect IOM1 to fabric-interconnect A, and IOM2 to fabric-interconnect B. (CSCtb35660)

**Symptom** Logon access is denied for user accounts where the password field was left blank during user account creation.

**Workaround** When creating a user account, ensure that a secure password for the account is specified. (CSCta21326)

**Symptom** When more than 10 Cisco UCS Manager GUI sessions are open at the same time with remote authentication for a long time (typically for a few hours), one of the Cisco UCS Manager GUI sessions may fail to re-authenticate. This causes the session that fails the re-authentication to close. The problem does not happen when local authentication is in use.

**Workaround** Re-login to the Cisco UCS Manager GUI session when it closes. (CSCtb05260)

**Symptom** If you move from subnet A to subnet B then do a cluster failover and move back to subnet A, a Virtual IP is no longer pingable.

**Workaround** Set the VIP to a different VIP by using the following CLI commands to set it back to the original address:

```
scope system
set set virtual-ip <new address>
commit
(CSCtc55636)
```

### Fabric Interconnect

**Symptom** Without pin group configuration, server interfaces are pinned to uplink interfaces of the fabric interconnect dynamically and the pinning is redistributed as uplink interfaces go up or down. In some situations, the distribution of server interfaces across uplink interfaces is not balanced. Potential impact is some uplinks are under utilized.

**Workaround** None. (CSCsv92356)

**Symptom** At bootup of the fabric interconnect, the following message will be displayed on the console: “The startup-config won't be used until the next reboot.”

**Workaround** None, just ignore the message. (CSCsx13134)

**Symptom** Console login is treating the admin and ADMIN account as the same. Console login name on the fabric interconnect is not case sensitive, so there is no differentiation between e.g. 'admin' and 'ADMIN'.

**Workaround** Implement usernames that are not case sensitive. (CSCsy15489)

**Symptom** Under high stress on the system with repeated port flapping and a default or native VLAN changing simultaneously, a process may cause the fabric interconnect to reload.

**Workaround** None. (CSCta09325)

**Symptom** The **show cdp neighbor** command does not display information for CDP neighbors seen from the management interface, nor does it display the fabric interconnect CDP information corresponding to the management interface.

**Workaround** None. (CSCta25287)

**Symptom** With FM/DM version 5.0(0.295) and UCS 1.1 release, a security user defined in Cisco UCS Manager does not get displayed on FM/DM.

**Workaround** None. Verify user security from Cisco UCS Manager. (CSCte25876)

#### UCS Manager CLI

**Symptom** The UUID of the VM changes in VMware vCenter. After a VM restarts, the virtual machine node on the VM tab shows multiple instances of the same VM with one online and one offline.

**Workaround** After the VM retention period configured in the VM life cycle policy has passed, Cisco UCS Manager deletes the offline instance automatically. (CSCtc86297)

**Symptom** If multiple vHBA initiators are configured in the same zone so that they are visible to each other and can login to each other, and storage multipathing is not configured with active and standby paths through the Cisco UCS fabric interconnects (There is only one path through the primary fabric interconnect), and the primary fabric interconnect is rebooted, the vHBA driver can be exposed to a situation in which two initiators can try to login to each other at the same time, and cause a host crash.

**Workaround** Do not configure multiple vHBA initiators in the same zone, to ensure that they are not visible to each other. (CSCte36784)

**Symptom** ESX Read and Write commands sent on a vHBA keep timing out and being aborted even if the target device is logged into the network. This can happen if the link flaps very fast from up to down to up and memory allocation for the link event fails. The vHBA driver misses the link down event and it does not re-login to the fabric interconnect. The fabric interconnect, however, has no login state for the vHBA and so drops all packets from the vHBA.

**Workaround** Disable and reenab the port on the UCS fabric interconnect that corresponds to the vHBA. (CSCte08092)



## Release 1.1(1)

The following caveat is open for Release 1.1(1i), most Release 1.1(1j) caveats also apply unless they are listed as resolved for Release 1.1(1i):

**Symptom** Pass-through DMA Support selection is not available in the BIOS if it was Disabled prior to the BIOS upgrade. If you had this option Disabled in previous version, the selection is hidden in the updated BIOS.

**Workaround** When you are in the BIOS Setup utility, press F9 to Load the BIOS defaults (CSCtb96792)

This section lists the open caveats in Release 1.1(1j).

### BIOS

**Symptom** Low Voltage DIMMs marked as Identity Not Established and are not included in the PID catalog.

**Workaround** None. Disregard the message, the DIMMs are fully functional and the error state is a false positive. Closed in 1.1(1m). (CSCtg86520)

**Symptom** With the B-250 blade server, the displayed ESX and Linux OS HDD Boot Device Order is the reverse of the BIOS HDD Boot Order.

**Workaround** Review both the disks (and drive labels as applicable) during installations of ESX and Linux versions and choose the correct disk for installation. (CSCtd90695)

**Symptom** When memory mirroring configuration is disabled by removing a DIMM, BIOS will switch to the Performance mode, and will not log a SEL that mirroring was disabled.

**Workaround** Check the status of the memory mirroring in **BIOS Setup->Advanced -> Memory Configuration -> Memory RAS and Performance Configuration**. (CSCsy54097)

**Symptom** When a faulty DIMM is detected in early BIOS POST (e.g. the blade was powered on with a faulty DIMM), two SEL entries will be sent to the BMC. One entry will be logged for each DIMM.

**Workaround** Enter BIOS Setup and navigate to **Advanced -> Memory Configuration**. This menu will help to distinguish a faulty DIMM from its neighbor. (CSCsy97698)

**Symptom** When hot plugging or removing USB devices at a BIOS Setup -> Advanced -> USB screen, the Setup Utility may freeze.

**Workaround** Reboot the server. (CSCsz41907)

**Symptom** Installing EFI Native SLES 11 is not supported in this release.

**Workaround** Currently, there is no workaround. (CSCsz99666)

**Symptom** Disabling USB 2.0 through **Advanced->USB** could result in inconsistent information on that particular page. Some devices may not show up as expected. This does not results in functional degradation during POST.

**Workaround** Either don't disable USB 2.0 (we are not aware of any need to disable it), or ignore the resulting artifacts in the BIOS setup. (CSCta21849)

**Symptom** FSM gets stuck in an Error Configuring the Local Disk Controller state due to various underlying conditions. Those can include but are not limited to the following:

- The Local Disks not getting discovered correctly or are “available/presence-Equipped” but not in a Ready state.
- Failures that can't be correctly communicated to Cisco UCS Manager can get reported as this type of error.

**Workaround** Remove and insert all of the local disks from the failing server, then re-acknowledge the server. (CSCta45805)

**Symptom** The Disk Fault/Error Codes, Disk Status, Alarms and the failures forwarded by the SAS Controller are not received by Cisco UCS Manager.

**Workaround** None. (CSCsy76853)

**Symptom** After resetting the CMOS the system date needs to be reset to current.

**Workaround** None. (CSCtb12390)

## Red Hat Linux

**Symptom** When a vNIC is not in failover mode and a link down event occurs, the network traffic on the blades is disrupted with a system running RHEL 5.3.

**Workaround** This is a known issue with the ixgbe driver in RHEL 5.3 and because RHEL 5.4 is the latest release, Redhat recommends upgrading the systems to the RHEL 5.4. If you cannot upgrade to RHEL 5.4, below are a few suggestions that has been found to work.

1. Restart the network.

```
service network restart  
or
```

```
ifdown ethx  
ifup ethx
```

2. Run your system with nomsi.

- Edit /etc/grub.conf
- Add pci=noms to the kernel line
- Restart the system with this kernel



Note

Network performance may be affected since the system is running in legacy mode. (CSCte44548)

## Adapters

**Symptom** When a DCBXP peer on a physical interface sends two different unique identifiers in the Protocol data unit in the same session, a DCBXP process error disables the port.

**Workaround** Issue the following commands to enable the port:

```
scope chassis <Chassis Id>
scope server <Server Id>
scope adapter <Adapter Id>
scope ext-eth-if <Id>
set adminstate reset-connectivity
commit-buffer
```

Wait for a minute, the port will come up.(CSCsx42435)

## KVM

**Symptom** During the Server Power-State Management, the KVM session may be aborted with a message displaying “Network Connection Dropped”.

**Workaround** Close the KVM session(s) that have been aborted and open a new KVM session. (CSCtc53253)

## Cisco UCS Manager

**Symptom** UCSM 1.1.(1j) firmware activation during UCS firmware upgrade will result in a server reboot. Customers upgrading their systems from the 1.0.1 or 1.0.2 release to the 1.1(1j) release will experience an unexpected server reboot upon UCSM component activation. This is a result of an incorrect setting of the internal VNIC/VHBA property called lifecycle, that makes the system believe that reconfiguration of these objects is required. This reconfiguration triggers a server reboot.

**Workaround** No workaround currently exists. Customers can install the 1.1.(1j) release if a server reboot is acceptable for their firmware upgrade scenario and a maintenance window is scheduled. Customers that do not consider a server reboot as an acceptable condition during UCSM FW activation, should install release 1.1(1m). (CSCtf02353)



Note

BIOS and interface card firmware upgrade still require a server reboot. Customers are expected to continue their operations after UCS firmware upgrade with a new BIOS and Interface Card firmware. Therefore the server reboot described in CSCtf02353 is an unexpected condition on UCSM activation, but still fits in the current firmware upgrade completion requirements.

**Note**


---

CSCtf02353 will not be a problem on newly purchased systems that ship with Release 1.1.(1j).

---

**Symptom** The disk scrub policy does not meet DoD compliance.

**Workaround** None. (CSCsy20036)

**Symptom** After the removal or insertion of one or more local disks, their full discovery fails.

**Workaround** Re-acknowledge the server to complete the full discovery. (CSCsy80888)

**Symptom** One vNIC defined in the service profile boot order results in two BIOS vNICs.

**Workaround** Avoid defining two different pxelinux.cfg/<MAC> files that have different boot/install instructions. When booted, both vNICs should execute the same PXE configuration. (CSCsz41107)

**Symptom** After a full restore of the primary fabric interconnect, the subordinate fabric interconnect installation may temporarily fail with the following message:

```
Enter the admin password of the peer switch:
Connecting to peer switch... unable to connect! Password could be wrong.
Hit enter to try again or type 'restart' to start setup from beginning...
```

**Workaround** Retry the fabric interconnect installation. (CSCsz85876)

**Symptom** For a given port profile with existing VIFs, if the “Max-Ports” setting is reduced from the currently configured value to a value less than the “Used-Ports” value reported for that port profile by VMware vCenter, this is a mis-configuration. The new value for “Max-Ports” for that port profile will only be updated in Cisco UCS Manager and its update in VMware Center will fail, causing an inconsistency between Cisco UCS Manager and VMware Center Server.

**Workaround** If the need arises to reduce the value of “Max-Ports” of a given port profile, the new value should be at least the value of “Used-Ports” reported by the VMware Center for all the DVSEs for that port profile (not lower than maximum of all the “Used-Ports” values). This constraint has to be ensured manually. (CSCte12163)

**Symptom** When a service profile containing 2 vNICs and having failover enabled is applied to some adapters, the fail back timeout specified in the adapter policy for the second vNIC has no effect. The fail back timeout specified in the adapter policy and applied to the first vNIC is applied to the whole adapter and effective for both vNICs.

**Workaround** Specify the desired timeout in the adapter policy and apply to the first vNIC. (CSCsz68887)

**Symptom** Cisco UCS Manager reports incorrect v NICs or VIFs associated with a given Virtual Machine if and only if the Virtual Machine is deployed from VMware Center in Fault-Tolerance (Active-Standby) mode and the Virtual Machine happens to be the standby or FT Virtual Machine.

**Workaround** None. (CSCte45010)

### Cisco UCS Manager GUI

**Symptom** The UCSM GUI could show all DIMMs to be in array 1, and maximum memory for a blade of 192GB for a B200.

**Workaround** This is a display-only issue, and does not affect functionality. DIMMs may be physically located in array 1 or array 2. (CSCta56527)

**Symptom** Hardware revision numbers for fabric interconnect components are not populated in the Cisco UCS Manager.

**Workaround** Enter the **connect nxos** command to connect to the native NX-OS CLI, then issue the appropriate **show sprom component** command and look for **H/W Version:** field in the command output. (CSCta12005)

**Symptom** In the Cisco UCS Manager GUI, you can only select port channels and individual uplink ports as pin targets, but the Cisco UCS Manager CLI allows you to also select port channel member ports as pin targets.

**Workaround** Port channel member ports should not be selected as pin targets, even if the Cisco UCS Manager CLI allows you to. (CSCta60495)

**Symptom** Even though there are no POST failures in the chassis, Cisco UCS Manager may sometimes display the overall status of the chassis as POST-failure.

**Workaround** Check the chassis POST messages for errors, and if there are none, ignore the Cisco UCS Manager status message. (CSCsz01878)

**Symptom** Statistics counters cannot be cleared using Cisco UCS Manager CLI.

**Workaround** Clear the counters using the Cisco UCS Manager GUI. (CSCsz47512)

**Symptom** In Cisco UCS Manager GUI, if the **Reboot on boot Order Change** checkbox is checked for a boot policy, and if CD-ROM or Floppy is the last device in the boot order, then deleting or adding the device does not directly affect the boot order and the server does not reboot.

**Workaround** None. (CSCta54895)

**Symptom** When a cluster configuration is set up such that I/O module 1 goes to fabric interconnect B and I/O module 2 goes to fabric interconnect A, then the Ethernet devices are given ports 1 and 0. However if the setup is straight, with I/O Module 1 connected to fabric interconnect A and I/O Module 2 to fabric interconnect B, then the devices are assigned ports 0 and 1.

**Workaround** Connect IOM1 to fabric-interconnect A, and IOM2 to fabric-interconnect B. (CSCtb35660)

**Symptom** Logon access is denied for user accounts where the password field was left blank during user account creation.

**Workaround** When creating a user account, ensure that a secure password for the account is specified. (CSCta21326)

**Symptom** When more than 10 Cisco UCS Manager GUI sessions are open at the same time with remote authentication for a long time (typically for a few hours), one of the Cisco UCS Manager GUI sessions may fail to re-authenticate. This causes the session that fails the re-authentication to close. The problem does not happen when local authentication is in use.

**Workaround** Re-login to the Cisco UCS Manager GUI session when it closes. (CSCtb05260)

#### Fabric Interconnect

**Symptom** Without pin group configuration, server interfaces are pinned to uplink interfaces of the fabric interconnect dynamically and the pinning is redistributed as uplink interfaces go up or down. In some situations, the distribution of server interfaces across uplink interfaces is not balanced. Potential impact is some uplinks are under utilized.

**Workaround** None. (CSCsv92356)

**Symptom** At bootup of the fabric interconnect, the following message will be displayed on the console: "The startup-config won't be used until the next reboot."

**Workaround** None, just ignore the message. (CSCsx13134)

**Symptom** Console login is treating the admin and ADMIN account as the same. Console login name on the fabric interconnect is not case sensitive, so there is no differentiation between e.g. 'admin' and 'ADMIN'.

**Workaround** Implement usernames that are not case sensitive. (CSCsy15489)

**Symptom** Under high stress on the system with repeated port flapping and a default or native VLAN changing simultaneously, a process may cause the fabric interconnect to reload.

**Workaround** None. (CSCta09325)

**Symptom** The **show cdp neighbor** command does not display information for CDP neighbors seen from the management interface, nor does it display the fabric interconnect CDP information corresponding to the management interface.

**Workaround** None. (CSCta25287)

**Symptom** With FM/DM version 5.0(0.295) and UCS 1.1 release, a security user defined in Cisco UCS Manager does not get displayed on FM/DM.

**Workaround** None. Verify user security from Cisco UCS Manager. (CSCte25876)

#### UCS Manager CLI

**Symptom** The UUID of the VM changes in VMware vCenter. After a VM restarts, the virtual machine node on the VM tab shows multiple instances of the same VM with one online and one offline.

**Workaround** After the VM retention period configured in the VM lifecycle policy has passed, Cisco UCS Manager deletes the offline instance automatically. (CSCtc86297)

**Symptom** If multiple vHBA initiators are configured in the same zone so that they are visible to each other and can login to each other, and storage multipathing is not configured with active and standby paths through the Cisco UCS fabric interconnects (There is only one path through the primary fabric interconnect), and the primary fabric interconnect is rebooted, the vHBA driver can be exposed to a situation in which two initiators can try to login to each other at the same time, and cause a host crash.

**Workaround** Do not configure multiple vHBA initiators in the same zone, to ensure that they are not visible to each other. (CSCte36784)

**Symptom** ESX Read and Write commands sent on a vHBA keep timing out and being aborted even if the target device is logged into the network. This can happen if the link flaps very fast from up to down to up and memory allocation for the link event fails. The vHBA driver misses the link down event and it does not re-login to the fabric interconnect. The fabric interconnect, however, has no login state for the vHBA and so drops all packets from the vHBA.

**Workaround** Disable and reenabte the port on the UCS fabric interconnect that corresponds to the vHBA. (CSCte08092)

## Release 1.0(2)

The following caveats were opened in UCS software release 1.0(2) and are still unresolved.

### Adapters

**Symptom** If default adapter policies are used, windows OS can take a long time to boot due to non-ideal VHBA related settings.

**Workaround** Create an adapter policy with optimal values and use that in the service profile. (CSCtb99003)

### BIOS

**Symptom** With various Local Disk Configurations, the LSI SAS Configuration Utility fails to launch while in BIOS.

**Workaround** The LSI SAS Controller Utility should not be used and all of the Local Disk Policy and Service Profile operations must be executed using UCSM.(CSCtc21336)

**Symptom** Disabling USB 2.0 is disabled through Advanced->USB, results in various artifacts on that particular page. Some devices may not show up as expected. This results in no functional degradation during POST.

**Workaround** Either do not disable USB 2.0 (we are currently are not aware of any need to disable it), or ignore the resulting artifacts in the BIOS setup. (CSCta21849)

**Symptom** When the memory mirroring configuration is destroyed by removing a DIMM, the BIOS will switch to the Performance mode, and will not log a message that mirroring was disabled.

**Workaround** Check the status of the memory mirroring in **BIOS Setup->Advanced -> Memory Configuration -> Memory RAS and Performance Configuration**. (CSCsy54097)

**Symptom** When plugging or removing USB devices at **BIOS Setup -> Advanced -> USB**, the Setup Utility may hang.

**Workaround** Reboot the server. (CSCsz41907)

### Fabric Interconnect

#### HTTP

**Symptom** HTTPD process crashed, with the following event log:

Process crashed. Core file 1253640662\_SAM\_ucs-6120-1-A\_httpd\_log.3114.tar.gz (SAM/Switch Core Dump) detected on fabric interconnect A.



**Workaround** None. (CSCtc13234)

## Pinning

### UCS Manager GUI

**Symptom** When more than 10 GUI sessions are open at the same time with remote authentication for a long time (typically for few hours), it has been observed that one of the GUI sessions fails to re-authenticate. This causes the session that fails re-authentication to close. Problem does not happen when local authentication is in use.

**Workaround** Re-login to the GUI session when it closes. (CSCtb05260)

**Symptom** When waking up from sleep, the UCS Manager GUI will detect an event sequencing error and display the error: “Event Sequencing is skewed” because the JRE doesn't have a sleep detection mechanism.

**Workaround** Always shut down the UCSM GUI before putting your computer to sleep. (CSCta94641)

**Symptom** Downloads may be slow if TFTP is used.

**Workaround** If TFTP performance is slow, use SCP or another protocol. (CSCtb45761)

## Release 1.0(1)

The following caveats were opened in UCS software release 1.0(1e) and are still present.

### AAA

**Symptom** Local user passwords can not contain “\$” character.

**Workaround** Do not include the “\$” character in local user passwords. (CSCsz44814)

**Symptom** When using a fully qualified domain name (FQDN) of an LDAP provider, the FQDN is not resolved with DNS, and user authentication using the LDAP provider does not work.

**Workaround** Use an IP address instead of an FQDN when creating LDAP providers. (CSCta09972)

**Symptom** The IPMI user database is not backed up in the UCS Manager when you export a configuration backup.

**Workaround** After the configuration import is done, manually configure the IPMI user profile. (CSCta48483)

## Adapters

**Symptom** When a service profile containing two vNICs and having failover enabled is applied to QLogic or Emulex CNAs, the failback timeout specified in the adapter policy for the second vNIC has no effect. The failback timeout specified in the adapter policy and applied to the first vNIC is applied to the whole adapter and is effective for both vNICs.

**Workaround** Specify the desired failback timeout in the adapter policy and apply to the first vNIC. (CSCsz68887)

**Symptom** When a DCBXP peer on a physical interface sends two different unique identifiers in the protocol data unit in the same session, a DCBXP process error disables the port.

**Workaround** Enter the following commands and then wait for a minute for the port to come up:

```
scope chassis chassis-id
scope server server-id
scope adapter adapter-id
scope ext-eth-if ext-eth-if-id
set adminstate reset-connectivity
commit-buffer
```

(CSCsx42435)

## BIOS

**Symptom** When a blade server is powered on with a faulty DIMM, the BIOS POST detects the faulty DIMM and two SEL entries are sent to the BMC. One entry is logged for each DIMM.

**Workaround** Enter the BIOS setup and navigate to the Advanced > Memory Configuration menu to distinguish the faulty DIMM from its neighbor. (CSCsy97698)

**Symptom Symptom** Installing EFI Native SLES 11 is currently not supported in this release.

**Workaround** None. (CSCsz99666)

**Symptom** One vNIC defined in the UCS Manager service profile boot order results in two BIOS vNICs.

**Workaround** Avoid defining two different pxelinux.cfg/<MAC> files that have different boot/install instructions. When booted, both vNICs should execute the same PXE configuration. (CSCsz41107)

## Fabric Interconnect

**Symptom** Without pin-group configuration, server interfaces are dynamically pinned to fabric interconnect uplink interfaces, and the pinning is redistributed as uplink interfaces go up or down. In some situations, the distribution of server interfaces across uplink interfaces is not even.

**Workaround** None. (CSCsv92356)

**Symptom** When a fabric interconnect boots, the “The startup-config won't be used until the next reboot” message appears on the console. Fabric interconnect configuration is controlled by the UCS Manager, so this message has no meaning on the fabric interconnect configuration and has no functional impact.

**Workaround** None. (CSCsx13134)

**Symptom** Console logon user names on the fabric interconnect are not case sensitive. For example, there is no differentiation between admin and ADMIN.

**Workaround** Use case insensitive user names. (CSCsy15489)

**Symptom** When the system is under high stress, with repeated port flapping (ports rapidly going up and down) and default (native) VLAN change, the FWM process may core and cause the fabric interconnect to reload.

**Workaround** None. (CSCta09325)

**Symptom** The **show cdp neighbor** CLI command does not display information for CDP neighbors seen from the management interface, nor does it display the fabric interconnect CDP information corresponding to the management interface.

**Workaround** None. (CSCta25287)

## Faults and Alerts

**Symptom** Even though there are no POST failures in the chassis, the UCS Manager sometimes displays the overall status of the chassis as POST-failure.

**Workaround** Check the chassis POST messages for errors, and if there are none, ignore the UCS Manager status message. (CSCsz01878)

**Symptom** In rare cases the UCS Manager reports the link absence fault between the fabric interconnect server port and the fabric extender during the internal inventory collection. The following is an example of such a fault:

```
*****
Severity: Cleared
Code: F0367
Last Transition Time: 2009-07-15T11:47:49
ID: 646445
Status: None
Description: No link between fabric extender port 2/1/1 and switch A:1/9
Affected Object: sys/chassis-2/slot-1/fabric/port-1
Name: Ether Switch Intfio Satellite Connection Absent Cause: Satellite Connection Absent
Type: Connectivity
Acknowledged: No
Occurrences: 1
Creation Time: 2009-07-15T11:46:49
Original Severity: Major
Previous Severity: Major
Highest Severity: Major
```

\*\*\*\*\*

**Workaround** Ignore the fault message; it will automatically get cleared after one minute. This will not impact the data path. (CSCta76573)

### High Availability

**Symptom** After a full restore of the primary fabric interconnect, the subordinate fabric interconnect installation may temporarily fail with the following message:

```
Enter the admin password of the peer switch:
Connecting to peer switch... unable to connect! Password could be wrong.
Hit enter to try again or type 'restart' to start setup from beginning...
```

**Workaround** Retry the fabric interconnect installation. (CSCsz85876)

### Inventory

**Symptom** Hardware revision numbers for fabric interconnect components are not populated in the UCS Manager.

**Workaround** Perform the following steps to determine the revision number for a fabric interconnect component:

1. Enter the **connect nxos** command to connect to the native NX-OS CLI.
2. Enter the appropriate **show sptom component** command and look for **H/W Version:** field in the command output. (CSCta12005)

**Symptom** All DIMMs are reported to be in array 1, and maximum memory for a blade is reported as 192-GB.

**Workaround** DIMMs may be physically located in array 1 or array 2, and the maximum memory is 96-GB. This is a display-only issue, and does not affect functionality. (CSCta56527)

### Pinning

**Symptom** In the UCS Manager GUI, you can only select port channels and individual uplink ports as pin targets, but the UCS Manager CLI allows you to also select port channel member ports as pin targets.

**Workaround** Port channel member ports should not be selected as pin targets, even if the UCS Manager CLI allows you to. (CSCta60495)

## Server

**Symptom** Local disk removal and insertion is not detected.

**Workaround** Select the **Re-Acknowledge Server** option in UCS Manager GUI to discover the server. (CSCsy80888)

**Symptom** The disk scrub policy needs enhancements to meet DOD compliance.

**Workaround** None. (CSCsy20036)

## SNMP

**Symptom** SNMP shows the fabric interconnect name rather than system name.

**Workaround** None. (CSCta22029)

**Symptom** An SNMP user name can not be the same as a local user name.

**Workaround** Select an SNMP user name that does not match any local user name. (CSCta24034)

## SMASH

**Symptom** Any SMASH command entered with wrong option should give “INVALID OPTION” error message.

**Workaround** None. (CSCsv87256)

## UCS Manager CLI

**Symptom** Statistics counters cannot be cleared using the UCS Manager CLI.

**Workaround** Clear the counters using the UCS Manager GUI. (CSCsz47512)

## UCS Manager GUI

**Symptom** When several KVM Consoles are launched, the SUN JRE sometimes reports an error and the KVM Console fails to launch.

**Workaround** Launch the KVM Console again. (CSCta38463)

**Symptom** In the UCS Manager GUI, if the **Reboot on boot Order Change** checkbox is checked for a boot policy, and if CD-ROM or Floppy is the last device in the boot order, then deleting or adding the device does not directly affect the boot order and the server does not reboot.

**Workaround** None. (CSCta54895)

**Symptom** Fibre Channel port and server port events do not appear on the Fibre Channel port and server port **Events** tabs.

**Workaround** Look on the Admin **Events** tab for Fibre Channel port and server port events. (CSCta66375)

## New Hardware Features in Release 1.4

### Release 1.4(3y) adds support for:

- Version 2 of UCS B440 M1 and M2 Blade Servers. This new hardware version is part of a proactive replacement program. See [Field Notice 63430](#) for further details.

### Release 1.4(3) adds support for:

- B440 M2 servers using Westmere EX processors
- B230 M2 servers using Westmere EX processors

### Release 1.4(2) adds support for:

- 7-m and 10-m 10G SFP+ Twinax active cable assemblies

### Release 1.4(1) adds support for:

- UCS B230 server blade
  - UCS Manager now supports the newest blade in the UCS B Series, the UCS B230 which is a 2 socket, 32 DIMM slot half width server with two optional SSDs.
- UCS Manager support for UCS C-Series
  - The UCS C200, C210 and C250 servers can now be managed directly from UCS Manager. Integration details are available in the [C-series server installation guides](#). Contact your Cisco representative for additional information on connectivity and compatibility requirements.
- Fabric Extender Transceiver (FET-10G) between the fabric interconnect and fabric extender.
- 16GB DIMMs (A02-M316GB2-L=) are now qualified on the B200M2 server model when using UCS version 1.4(1i) and UCS capability catalog ucs-catalog.1.0.16.T.bin or greater (this catalog is available separately and included in the version 1.4(1i) software bundle).
- 16GB DIMM pairs (A02-M332GB3-2-L=) are now qualified on the B440M1 server model when using UCS version 1.4(1m). To support new power budget information for the B440 server and updated power numbers for 16GB DIMMs, UCS capability catalog ucs-catalog.1.0.25.T.bin (only available as a standalone download or as part of the UCS version 1.4(1m) bundle) or greater will need to be imported into UCS. The UCS hardware catalog has been modified to increase the B440 system board base power, and increase the power budget for 16GB DIMMs. These values are used to calculate the default Chassis Level Power Cap for the B440 blade with 16GB DIMMs.

**Caution**

Without this catalog update, the calculated default Chassis Power budget may be lower than needed. Certain large configurations (including 16GB DIMMs) of the B440 server, under maximum load, may trigger throttling of the processor with the lower default power budget. If unwanted throttling occurs, a re-acknowledgement of the chassis may be required to include the higher system board base power from the updated catalog, and prevent throttling of the processors. If throttling occurs on a server, an informational fault will be raised in the server faults tab. The fault message is “P-state lowered as consumption hit power cap”.

## New Software Features in Release 1.4

### Release 1.4(3u) adds support for:

- A user label was added to the KVM window.

### Release 1.4(3q) adds support for:

- The maximum number of VLAN Port instances is now 14,000.

### Release 1.4(2) adds support for:

- Chassis renumbering
- LACP support on an appliance port

### Release 1.4(1) adds support for:

- Chassis and multi-chassis power capping for UCS B-Series
  - Power capping has been extended to cover chassis and groups of chassis and includes a policy based workflow using service profiles for setting it up.
- Software packaging with server bundles
  - Support for server and adapter hardware can now be delivered independent of support for the infrastructure components. This allows customers to add support for new server types without having to upgrade their Fabric Interconnect or UCS Manager software.
- Scalability
  - UCS instances now scale to up to 20 UCS 5108 chassis.

### Ethernet and Fibre Channel

- FabricSync
  - The UCS 6100 synchronizes their mac-addresses between them. It works along with FabricFailover feature to provide faster vNIC fail over for Bare metal and brings HA to Hyper-V virtual switch networks. It is always turned on.
- PVLAN support
  - Layer 2 traffic segmentation within a subnet can now be achieved using PVLAN Isolated access in the UCSM. This allows customer to achieve vNIC level isolation which translates to VM level isolation using Cisco Virtual interface card in pass through mode.

- SPAN support on UCS 6100
  - SPAN provides granular visibility in to the Ethernet and FibreChannel flows within UCSM for monitoring and troubleshooting.
- Higher VLAN scalability (>1000)
  - Increased VLAN scalability from 512 in 1.3(1) to 1024 in 1.4(1)
- Direct connect Appliance
  - Specialized IP Appliances such as NAS filers and ISCSI storage can be connected directly to the UCS 6100 in End Host mode. This allows reduction in number of hops and latency for communication between server and IP storage.
- FC Trunking and port channel (in NPV mode)
  - Allows trunking of multiple VSANs using a single FC link and FibreChannel link consolidation when using VSANs,
- Limited Direct Connect FC Storage
  - FibreChannel storage can now be directly connected to the UCS 6100 with default zone policy (No zone configuration allowed in the 6100 but can be inherited from an upstream MDS switch).

### Security

- KVM security enhancements
  - Multi-user KVM access has new controls that allow the first user to allow/deny or control the permissions of subsequent sessions.
- AAA - Active Directory group support
  - Groups defined in active directory can now be mapped into roles within UCS Manager.
- AAA - Multi-authentication support
  - UCS Manager now supports concurrent authentication using different authentication schemes such as Active Directory, TACACS+ or RADIUS. Concurrent authentication with multiple instances of the same scheme, such as multiple Active Directory domains, is also supported.

### Monitoring

- SNMP GET support for all UCS components
  - SNMP support has been extended to provide query (GET) support for all UCS components. The new MIB files can be accessed at <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>. Select UCS Manager under 'Unified Computing'.
- UCS 6100 licensing enforcement/warnings
  - A new GUI based workflow for licensing management is available and licenses are enforced with warning messages.
- Syslog message classification enhancements
  - New UCS labels allow easier filtering of syslog messages.

### Stateless Computing

- Scheduling of service profile changes
  - Through the use of maintenance policies, service profile deployments can be scheduled for a later time. In addition, the number of concurrent profiles that are being applied and the total number of profiles applied during a particular time window can be controlled.



- Impact analysis of configuration changes
  - A simple “pre-flight check” compatibility check allows customers to recognize potential compatibility issues before applying a service profile to a particular server.
- CIMC IP address abstraction
  - In addition to the CIMC IP address for the CIMC on the server an optional management IP is available with the service profile that can move with the service profile when it is moved to a new server.

#### Usability

- User labels for managed objects
  - Service profiles, servers and chassis have custom user labels that can be applied. These user labels can be displayed, sorted and filtered through the UCS Manager GUI.
- Direct upload of firmware image files from UCSM client
  - The need for setting up SCP/SFTP for image file uploads is now optional since a direct upload from the laptop or other UCS Manager client to UCS Manager is now possible.

## Bundle Images

This section includes the following topics:

- [“1.4\(4l\) Bundle Images” section on page 73](#)
- [“1.4\(4k\) Bundle Images” section on page 75](#)
- [“1.4\(4j\) Bundle Images” section on page 77](#)

### 1.4(4l) Bundle Images

This section includes the following topics:

- [SWT Unified Computing System \(UCS\) Infrastructure Software Bundle for 1.4\(4l\)](#)
- [SWT Unified Computing System \(UCS\) Server Software \(B-Series\) for 1.4\(4l\)](#)
- [SWT Unified Computing System \(UCS\) Server Software \(C-Series\) for 1.4\(4l\)](#)

#### SWT Unified Computing System (UCS) Infrastructure Software Bundle for 1.4(4l)

ucs-k9-bundle-infra.1.4.4l.A.bin contains the following images:

- ucs-2100.1.4.4l.bin
- ucs-6100-k9-kickstart.4.2.1.N1.1.44l.bin
- ucs-6100-k9-system.4.2.1.N1.1.44l.bin
- ucs-manager-k9.1.4.4l.bin

#### SWT Unified Computing System (UCS) Server Software (B-Series) for 1.4(4l)

ucs-k9-bundle-b-series.1.4.4l.B.bin contains the following images:

- ucs-b200-m1-bios.S5500.1.4.3b.0.040220121621.bin

- ucs-b200-m1-k9-cimc.1.4.4l.bin
- ucs-b200-m1-sasctrl.01.28.03.00\_06.28.00.00\_03.12.00.00.bin
- ucs-b200-m2-bios.S5500.1.4.3b.0.040220121621.bin
- ucs-b230-m1-bios.B230M1.1.4.1f.0.032920121838.bin
- ucs-b230-m1-k9-cimc.1.4.4l.bin
- ucs-b230-m1-mrsasctrl.20.7.1-0024\_4.18.00\_NA.bin
- ucs-b230-m1-pld.B230100C.bin
- ucs-b230-m2-bios.B230M2.1.4.3e.0.032920121829.bin
- ucs-b230-m2-k9-cimc.1.4.4l.bin
- ucs-b230-m2-pld.B230100C.bin
- ucs-b250-m1-bios.S5500.1.4.3f.0.040320121059.bin
- ucs-b250-m1-k9-cimc.1.4.4l.bin
- ucs-b250-m1-pld.111026-111026.bin
- ucs-b250-m2-bios.S5500.1.4.3f.0.040320121059.bin
- ucs-b440-m1-bios.B440M1.1.4.1e.0.042320121111.bin
- ucs-b440-m1-k9-cimc.1.4.4l.bin
- ucs-b440-m1-mrsasctrl.12.9.0-0050\_3.18.00\_NA.bin
- ucs-b440-m1-pld.B440100C-B4402006.bin
- ucs-b440-m2-bios.B440M2.1.4.3e.0.050320121130.bin
- ucs-b440-m2-k9-cimc.1.4.4l.bin
- ucs-b440-m2-pld.B440100C-B4402008.bin
- ucs-m51kr-b.5.2.7.12.1.bin
- ucs-m61kr-i.2.1.60.1.1.bin
- ucs-m71kr-e-cna.1.4.4l.bin
- ucs-m71kr-e-hba.2.80A4.bin
- ucs-m71kr-e-optionrom.5.03X4.bin
- ucs-m71kr-q-cna.1.4.4l.bin
- ucs-m71kr-q-optionrom.2.02.bin
- ucs-m72kr-e.4.0.467.0.bin
- ucs-m72kr-q.01.02.13.bin
- ucs-m81kr-vic.1.4.4l.bin
- ucs-mgmttext.1.4.4l.bin

## SWT Unified Computing System (UCS) Server Software (C-Series) for 1.4(4l)

ucs-k9-bundle-c-series.1.4.4l.C.bin contains the following images:

- ucs-c-lsi-mezz-1064E.01.30.00.00\_06.30.00.00\_03.12.00.00.bin
- ucs-c-lsi-mrsas-8708EM2.11.0.1-0030.bin

- ucs-c-lsi-mrsas-926x.12.9.0-0050.bin
- ucs-c-lsi-sasctrlr-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.1.2.2j.bin
- ucs-c250-bios.C250.1.2.2f.0.112820100448.bin
- ucs-c250-k9-cimc.1.2.2j.bin
- ucs-mgmttext.1.4.4l.bin
- ucs-p81e-vic.1.4.4l.bin

## 1.4(4k) Bundle Images

This section includes the following topics:

- [SWT Unified Computing System \(UCS\) Infrastructure Software Bundle for 1.4\(4k\)](#)
- [SWT Unified Computing System \(UCS\) Server Software \(B-Series\) for 1.4\(4k\)](#)
- [SWT Unified Computing System \(UCS\) Server Software \(C-Series\) for 1.4\(4k\)](#)

### SWT Unified Computing System (UCS) Infrastructure Software Bundle for 1.4(4k)

ucs-k9-bundle-infra.1.4.4k.A.bin contains the following images:

- ucs-2100.1.4.4k.bin
- ucs-6100-k9-kickstart.4.2.1.N1.1.44k.bin
- ucs-6100-k9-system.4.2.1.N1.1.44k.bin
- ucs-manager-k9.1.4.4k.bin

### SWT Unified Computing System (UCS) Server Software (B-Series) for 1.4(4k)

ucs-k9-bundle-b-series.1.4.4k.B.bin contains the following images:

- ucs-b200-m1-bios.S5500.1.4.3b.0.040220121621.bin
- ucs-b200-m1-k9-cimc.1.4.4k.bin
- ucs-b200-m1-sasctrlr.01.28.03.00\_06.28.00.00\_03.12.00.00.bin
- ucs-b200-m2-bios.S5500.1.4.3b.0.040220121621.bin
- ucs-b230-m1-bios.B230M1.1.4.1f.0.032920121838.bin
- ucs-b230-m1-k9-cimc.1.4.4k.bin
- ucs-b230-m1-mrsasctrlr.20.7.1-0024\_4.18.00\_NA.bin
- ucs-b230-m1-pld.B230100C.bin

- ucs-b230-m2-bios.B230M2.1.4.3e.0.032920121829.bin
- ucs-b230-m2-k9-cimc.1.4.4k.bin
- ucs-b230-m2-pld.B230100C.bin
- ucs-b250-m1-bios.S5500.1.4.3f.0.040320121059.bin
- ucs-b250-m1-k9-cimc.1.4.4k.bin
- ucs-b250-m1-pld.111026-111026.bin
- ucs-b250-m2-bios.S5500.1.4.3f.0.040320121059.bin
- ucs-b440-m1-bios.B440M1.1.4.1e.0.042320121111.bin
- ucs-b440-m1-k9-cimc.1.4.4k.bin
- ucs-b440-m1-mrsasctlr.12.9.0-0050\_3.18.00\_NA.bin
- ucs-b440-m1-pld.B440100C-B4402006.bin
- ucs-b440-m2-bios.B440M2.1.4.3e.0.050320121130.bin
- ucs-b440-m2-k9-cimc.1.4.4k.bin
- ucs-b440-m2-pld.B440100C-B4402008.bin
- ucs-m51kr-b.5.2.7.12.1.bin
- ucs-m61kr-i.2.1.60.1.1.bin
- ucs-m71kr-e-cna.1.4.4k.bin
- ucs-m71kr-e-hba.2.80A4.bin
- ucs-m71kr-e-optionrom.5.03X4.bin
- ucs-m71kr-q-cna.1.4.4k.bin
- ucs-m71kr-q-optionrom.2.02.bin
- ucs-m72kr-e.4.0.467.0.bin
- ucs-m72kr-q.01.02.13.bin
- ucs-m81kr-vic.1.4.4k.bin
- ucs-mgmttext.1.4.4k.bin

## SWT Unified Computing System (UCS) Server Software (C-Series) for 1.4(4k)

ucs-k9-bundle-c-series.1.4.4k.C.bin contains the following images:

- ucs-c-lsi-mezz-1064E.01.30.00.00\_06.30.00.00\_03.12.00.00.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.1.2.2j.bin
- ucs-c250-bios.C250.1.2.2f.0.112820100448.bin
- ucs-c250-k9-cimc.1.2.2j.bin
- ucs-mgmttext.1.4.4k.bin
- ucs-p81e-vic.1.4.4k.bin

## 1.4(4j) Bundle Images

This section includes the following topics:

- [SWT Unified Computing System \(UCS\) Infrastructure Software Bundle for 1.4\(4j\)](#)
- [SWT Unified Computing System \(UCS\) Server Software \(B-Series\) for 1.4\(4j\)](#)
- [SWT Unified Computing System \(UCS\) Server Software \(C-Series\) for 1.4\(4j\)](#)

### SWT Unified Computing System (UCS) Infrastructure Software Bundle for 1.4(4j)

ucs-k9-bundle-infra.1.4.4j.A.bin contains the following images:

- ucs-2100.1.4.4j.bin
- ucs-6100-k9-kickstart.4.2.1.N1.1.44j.bin
- ucs-6100-k9-system.4.2.1.N1.1.44j.bin
- ucs-manager-k9.1.4.4j.bin

### SWT Unified Computing System (UCS) Server Software (B-Series) for 1.4(4j)

ucs-k9-bundle-b-series.1.4.4j.B.bin contains the following images:

- ucs-b200-m1-bios.S5500.1.4.3b.0.040220121621.bin
- ucs-b200-m1-k9-cimc.1.4.4j.bin
- ucs-b200-m1-sasetlr.01.28.03.00\_06.28.00.00\_03.12.00.00.bin
- ucs-b200-m2-bios.S5500.1.4.3b.0.040220121621.bin
- ucs-b230-m1-bios.B230M1.1.4.1f.0.032920121838.bin
- ucs-b230-m1-k9-cimc.1.4.4j.bin
- ucs-b230-m1-mrsasctlr.20.7.1-0024\_4.18.00\_NA.bin
- ucs-b230-m1-pld.B230100C.bin
- ucs-b230-m2-bios.B230M2.1.4.3e.0.032920121829.bin
- ucs-b230-m2-k9-cimc.1.4.4j.bin
- ucs-b230-m2-pld.B230100C.bin
- ucs-b250-m1-bios.S5500.1.4.3f.0.040320121059.bin
- cs-b250-m1-k9-cimc.1.4.4j.bin
- ucs-b250-m1-pld.111026-111026.bin
- ucs-b250-m2-bios.S5500.1.4.3f.0.040320121059.bin
- ucs-b440-m1-bios.B440M1.1.4.1e.0.042320121111.bin

- ucs-b440-m1-k9-cimc.1.4.4j.bin
- ucs-b440-m1-mrsasctrl.12.9.0-0050\_3.18.00\_NA.bin
- ucs-b440-m1-pld.B440100C-B4402006.bin
- ucs-b440-m2-bios.B440M2.1.4.3e.0.050320121130.bin
- ucs-b440-m2-k9-cimc.1.4.4j.bin
- ucs-b440-m2-pld.B440100C-B4402008.bin
- ucs-m51kr-b.5.2.7.12.1.bin
- ucs-m61kr-i.2.1.60.1.1.bin
- ucs-m71kr-e-cna.1.4.4j.bin
- ucs-m71kr-e-hba.2.80A4.bin
- ucs-m71kr-e-optionrom.5.03X4.bin
- ucs-m71kr-q-cna.1.4.4j.bin
- ucs-m71kr-q-optionrom.2.02.bin
- ucs-m72kr-e.4.0.467.0.bin
- ucs-m72kr-q.01.02.13.bin
- ucs-m81kr-vic.1.4.4j.bin
- ucs-mgmttext.1.4.4j.bin

## SWT Unified Computing System (UCS) Server Software (C-Series) for 1.4(4j)

ucs-k9-bundle-c-series.1.4.4j.C.bin contains the following images:

- ucs-c-lsi-mezz-1064E.01.30.00.00\_06.30.00.00\_03.12.00.00.bin
- ucs-c-lsi-mrsas-8708EM2.11.0.1-0030.bin
- ucs-c-lsi-mrsas-926x.12.9.0-0050.bin
- ucs-c-lsi-sasctrl-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.1.2.2j.bin
- ucs-c250-bios.C250.1.2.2f.0.112820100448.bin
- ucs-c250-k9-cimc.1.2.2j.bin
- ucs-mgmttext.1.4.4j.bin
- ucs-p81e-vic.1.4.4j.bin

## Related Documentation

For related documentation, see this document:

- [Cisco UCS Documentation Roadmap](#)

## Cisco UCS C-Series Rack Mount Server Integration with Cisco UCS Manager

For more information, refer to the related documents available at the following links:

- [Cisco UCS C-series Rack Server Integration Guides](#)
- [Cisco UCS C-series Software Release Notes](#)

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: <http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html>.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.

---

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2010–2014 Cisco Systems, Inc. All rights reserved.