



# Release Notes for Cisco UCS Manager, Release 1.0(2)

**First Published: October 29, 2009**

**Latest Revision: March 11, 2010**

**Part Number: OL-20870-01**

This document describes the new features, system requirements, and caveats for Cisco UCS Manager Release 1.0(2d) , Release 1.0(2h), Release 1.0(2j), and Release 1.0(2k) as well as all related firmware on blade servers and other Unified Computing System components associated with those releases. Use this document in conjunction with the documents listed in the [“Related Documentation” section on page 17](#).



**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.



**Note**

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

**Table 1**      **Online History Change**

Part Number	Revision	Date	Description
OL-20870-01	A0	October 29, 2009	Created release notes for Release 1.0(2).
	B0	November 20, 2009	Added CSCtc21336
	C0	December 4, 2009	Added CSCtd32884, CSCta55689, CSC71310, CSCtc54935
	D0	December 23, 2009	Added resolved bugs for 1.0(2h) patch release
	E0	January 19, 2010	Updated for 1.0(2j) patch release
	F0	March 11, 2010	Updated for 1.0(2k) patch release



**Americas Headquarters:**

**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

# Contents

This document includes the following sections:

- [“Introduction” section on page 2](#)
- [“System Requirements” section on page 2](#)
- [“Updating the Cisco UCS Firmware” section on page 3](#)
- [“Hardware and Software Interoperability” section on page 3](#)
- [“Known Limitations and Behaviors” section on page 4](#)
- [“Errata” section on page 4](#)
- [“Open Caveats” section on page 5](#)
- [“Related Documentation” section on page 17](#)
- [“Obtaining Documentation and Submitting a Service Request” section on page 18](#)

## 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, multichassis platform in which all resources participate in a unified management domain.

## System Requirements

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

- The Cisco UCS Manager GUI is a Java-based application that requires Sun JRE 1.6 or later.
- The UCS Manager uses webstart and supports the following web browsers:
  - Microsoft Internet Explorer 6.0 or higher
  - Mozilla Firefox 3.0 or higher
- The UCS Manager is supported on the following operating systems:
  - Microsoft Windows XP
  - Microsoft Windows Vista
  - Red Hat Enterprise Linux 5.0 or higher

# Updating the Cisco UCS Firmware

To update the Cisco UCS firmware, refer to the “Firmware Management” chapter in either of the following documents:

- *Cisco UCS Manager CLI Configuration Guide* located at [http://www.cisco.com/en/US/docs/unified\\_computing/ucs/sw/cli/config/guide/1.0.2/b\\_CLI\\_Config\\_Guide\\_1.0.2.html](http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/cli/config/guide/1.0.2/b_CLI_Config_Guide_1.0.2.html)
- *Cisco UCS Manager GUI Configuration Guide* located at [http://www.cisco.com/en/US/docs/unified\\_computing/ucs/sw/gui/config/guide/1.0.2/b\\_GUI\\_Config\\_Guide.html](http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/gui/config/guide/1.0.2/b_GUI_Config_Guide.html)



## Note

If you have already configured Host Firmware Packs or Management Firmware Packs, then follow the "Updating Firmware Through Service Profiles" section, otherwise use the "Directly Updating Firmware at Endpoints" section.

## Update Sequence

You will need to follow this sequence to upgrade to Release 1.0(.2k) from any earlier 1.0.(2) release.

1. Download the firmware bundle.
2. Upgrade the Interface Cards.
3. Activate the Interface Cards ( use the Set Startup Version Only option).
4. If the upgrade is from release 1.0(2h) or earlier, activate the new UCSM image.
5. Activate the Subordinate FI (Confirm that the HA cluster is up and fully functional)
6. Activate the Primary FI (Confirm that the HA cluster is up and fully functional)
7. Reboot the servers to activate new adapter firmware.

## Hardware and Software Interoperability

For detailed information about storage switch, operating system, adapter, adapter utility, and storage array interoperability, see the *Hardware and Software Interoperability Matrix* located at [http://www.cisco.com/en/US/docs/unified\\_computing/ucs/interoperability/matrix/hw\\_sw\\_interop\\_matrix\\_seriesB\\_102.pdf](http://www.cisco.com/en/US/docs/unified_computing/ucs/interoperability/matrix/hw_sw_interop_matrix_seriesB_102.pdf)

## Feature Changes

Release 1.0(2j) added support for new DIMMs (refer to the interoperability matrix), and increased UCS system scalability from 5 server chassis to 8 server chassis per system.

# Known Limitations and Behaviors

## Adapters

(CSCtd32884 and CSC71310) The type of adapter in a server impacts the maximum MTU supported. Network MTU above the maximums may cause the packet to be dropped for the following adapters:

- The Cisco UCS CNA M71KR adapter supports a maximum MTU of 9216.
- The Cisco UCS 82598KR-CI adapter supports a maximum MTU of 14000.

## Recovering the Corrupt BIOS on a Server

(CSCta55689) Before you attempt to recover a corrupt BIOS, remove all attached or mapped USB storage from a server before you attempt to recover the corrupt BIOS on that server. If an external USB drive is attached or mapped from vMedia to the server, BIOS recovery fails.

## UCSM GUI and Boot Order

(CSCtc54935) The Configured Boot Order tab shows the boot order assigned to the server. The Actual Boot Order tab shows exactly what will boot from the various devices in the configuration.



### Note

The Actual Boot Order tab always shows "Internal EFI Shell" at the bottom of the boot order list.

## Passwords

(CSCtc70962) Choose a strong password with at least one capital letter and one number. This password cannot be blank. If a blank password is created, the account will become unusable.

## Changing Management IP Port

(CSCtb42606) After the initial configuration, you can change the management IP port and the related subnet mask in the Cisco UCS Manager CLI. You cannot make this change in the Cisco UCS Manager GUI.

# Errata

The following known issues will be corrected in future versions of these documents.

## Incorrect VLAN IDs Range

The USCM GUI and CLI configuration guide sections on named VLANs specified an incorrect reserved VLAN ID range. The text read: "You cannot create VLANs with IDs from 3968 to 4048. This range of VLAN IDs is reserved." The correct range is 3968 to 4047.

## Password Recovery

Refer to the [Password Recovery](#) section if the [Release 1.1\(1\) configuration guides](#) for complete and corrected procedures.

The documentation was updated to:

- Clarify that a user can log in with any Cisco UCS account to view the firmware versions.
- Emphasize the recommendation that additional user accounts be created on a Cisco UCS instance (already in the documentation) and that users not rely on having only the superuser admin account created when the fabric interconnects are configured.

- Add a recommendation that, if no additional accounts are created, that the users note down and save the firmware versions outside of the Cisco UCS instance.
- Add examples of the firmware versions and updated the installables path (replacing 'fabric' with 'switch' in the procedures).

The documentation was updated to add information about Admin password requirements to the following topics:

- Performing the Initial System Setup for a Standalone Fabric Interconnect
- Performing the Initial System Setup for the First Fabric Interconnect
- Recovering an Admin Password for a Standalone Configuration
- Recovering an Admin Password for a Cluster Configuration

#### Error in upgrade sequence

The USCM GUI and CLI configuration guide sections regarding upgrade sequences has "Updating and Activating the Firmware on a Fabric Interconnect" before "Updating and Activating the Cisco UCS Manager Software" which is incorrect. The correct sequence should be "Updating and Activating the Cisco UCS Manager Software" and then "Updating and Activating the Firmware on a Fabric Interconnect."

## Open Caveats

This section lists the open caveats for this release.

#### Adapters

- CSCtb99003

**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.

#### BIOS

- CSCtc21336

**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.

- CSCta10138

**Symptom** If the BIOS scrub policy is enabled for a Service Profile. In some rare circumstances, the BIOS clear will cause the Association/Dissassociation time to increase to as much as 15 minutes.

**Workaround** The default setting is for the BIOS Scrub policy to be set to DISABLED. Rather than use the BIOS scrub policy; the "Clear CMOS" should be used to reset all BIOS settings.

- CSCta21849

**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 don't 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.

- CSCsy54097

**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**.

- CSCsz41907

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

**Workaround** Reboot the server.

#### **Fabric Interconnect**

- CSCta73919

**Symptom** When a fabric interconnect moves from standalone mode to cluster mode it is possible that the virtual IP gets overwritten by the out of band IP of the primary fabric-interconnect. This issue happens only if the OOB IP was modified in stand-alone mode before changing the mode to cluster.

**Workaround** After using the cluster enable option, change the cluster IP again. This should fix the cluster IP.

## Firmware Management

- CSCtc66393

**Symptom** IOM Activation status gets stuck in "rebooting" even though IOM was not rebooted. This can happen if IOM was activated back and forth with and without "set-startup-only" options respectively.

**Workaround** None needed. IOM functionality is not disrupted by this. IOM can be updated and activated as usual. Also, the activate state will converge if there is a switch or IOM reboot.

## HTTP

- CSCtc13234

**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.

## Pinning

- CSCtb83759

**Symptom** In End Host Mode, a server MAC address is only learned on the server facing interface and not the network facing interface. When a MAC address moves out of a UCS-6100, the flushing of the MAC from the original switch depends on gratuitous broadcast packets being sent from the new location and being received by the original switch. In case of a high burst of moves, the notification mechanism on the original switch may not be able to keep up with the events. The loss of such move events will cause the mac to not get flushed from the original switch and cause traffic black-hole for hosts on the same switch trying to communicate with this MAC.

**Workaround** The MAC address age is being displayed in the output of the NX-OS **show mac address-table** CLI command. If duplicate MAC addresses are seen on multiple switches, the **clear mac address** command can be used to remove the ones not being used.

## UCS Manager GUI

- CSCtb05260

**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.

- CSCta94641

**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.

- CSCtc41465

**Symptom** When VHBA templates are modified, it can take up to a few minutes for the changes to propagate to the affected VHBA instances that are bound to the template.

**Workaround** None.

#### UUID

- CSCtc59481

**Symptom** When checking for UUID uniqueness, currently only the UUID suffix is checked.

**Workaround** Use a single UUID prefix.

- CSCtb45761

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

**Workaround** If TFTP performance is slow, use SCP or another protocol

## Resolved Caveats

The following caveats are resolved for the 1.0(2k) release:

- (CSCte26215) Data path over IPv6 is now functional.
- (CSCte64738 ) VHBA no longer intermittently experiences loss of path every few days.

The following caveats are resolved for the 1.0(2h) release:

- (CSCtd65852) The BIOS scrub had not been working correctly. The GUI and CLI can no longer configure a BIOS scrub, and if a scrub policy is currently configured it will not be performed.
- (CSCtd44556) Blades were sometimes not completely discovered and got stuck in discovery. This was due to an indefinite RPC block between UCSM and a blade. The RPC timeout mechanisms were fixed so that blades are never stuck in discovery.
- (CSCtc91207) LDAP users are now required to have a password, which cannot be blank.



This section lists caveats in Release 1.0(1e) that are resolved in the 1.0(2d) release.

### AAA

- (CSCsz91123) The output of **keyring** commands in the **show configuration** command is now in the expected sequence.
- (CSCsz91527) The default keyring no longer allows you to set a trusted point name.
- (CSCta91396) When configuring an LDAP provider, the distinguished name (DN) may contain a space.

### Adapters

- CSCta29118 Known Limitation: the mezzanine card does not support more than 64 Multicast IDX.
- CSCta49993 You can now qualify a server adapter by selecting a non-virtualized-eth.

### BIOS

- CSCsz37847 The blade server boot order can now be specified as desired.
- CSCsz47261 Boot device selection will perform as configured. We still suggest that at least two bootable devices are present in the boot order.
- CSCsz49172 BIOS recovery no longer causes the GUI to have both Boot Server and Shutdown Server grayed out.
- CSCta60324 After changing the boot order and saving the changes, a GUI pop up no longer appears.

### BMC

- CSCta65166 Upgrading from an earlier software version will not cause a falsely-reported bad software image on the BMC controller.

### Fabric Interconnect

- CSCsz83593 There is no longer a five minute delay needed to enter commands for a subordinate fabric interconnect
- CSCsz88780 Hosts are now able to obtain CDP neighbor information from the fabric interconnect.
- CSCta29227 The fabric interconnect management interface IP address is now correctly propagated to the upstream MDS Fibre Channel switch.
- CSCtd37231 During a UCS system upgrade customers no longer experience loss of network connectivity for more than the expected minute.

### Firmware Management

- CSCtc69186 An attempt to execute Update Firmware ALL no longer fails with a dependency on a deployed FW pack.
- CSCta04662 When IOM is activated with "set startup only" selected, then on sam manager activation, the flag no longer changes from "pending-next-boot" to "ready" though IOM is not rebooted.

### HTTP

- CSCta10001 When the HTTP or HTTPS service is set to a port that is already in use by another service, the web process will restart.

**UCS Manager**

- CSCta57665 Terminology is now consistent between CLI and GUI for adapter policies.
- CSCta76741 Removing VHBA from the storage boot order in updating-template now updates the boot order on the service profile instance.
- CSCsz01075 A warning is now issued when a service profile is assigned to a server that already has a service profile associated to it.
- CSCsz84016 Telnet and SSH connections to the virtual IP address are now immediately cleared if an admin failover is performed in a loop multiple times.
- CSCta14482 When you create, delete, or modify the DNS, domain name, or time zone configurations, the operation is listed in the audit log records.

**UCS Manager CLI**

- CSCta19783 The average, maximum and minimum statistics values display changes in values.
- CSCta30226 The node-wwnn object config-state is displayed as “applied” when deployed on the server during association.
- CSCta32500 The UCS Manager will automatically power off the server after you change the UUID in a service profile.

**UCS Manager XML API**

- CSCta67441 Internally, timestamp properties (in faults and statistics) are represented in milliseconds. but the string value is represented in the form YYYY-MM-DDTHH:MM:SS. With the loss of precision in the string value, the XML API equality filter can now be used to resolve queries.

**Pinning**

- CSCta67637 An attempt to configure hard pinning on a vHBA after a service profile is associated with a server will no longer fail.
- CSCta71657 If a VSAN, SAN pin group, VLAN, or LAN pin group is changed, the server reboots if necessary.

**Power and Thermal**

- CSCta43209 The I/O module (IOM) temperature sensor statistics read correct values.
- CSCta40269 The Admin and Oper server power states stay in sync when the server crashes, the front power button is used, or you shut down the server from the OS.

**Pools and Policies**

- CSCta76469 vNIC templates are exported when you backup all system and logical configuration settings.
- CSCta76749 When defining a statistics threshold in a given direction (above normal or below normal), if the current update is in the opposite direction, an invalid fault for the opposite direction is no longer raised.
- CSCta84769 The link between the UCS 6100 fabric interconnect and the UCS 2100 fabric extender will not come up with an erroneous “FEX-fabric sfp invalid” error.

**Statistics**

- CSCsz91750 HDD metrics are now displayed after you hot-swap or remove and reinsert the HDD.

- CSCta19830 User-defined statistics threshold policies that are set at the vNIC or vHBA level are evaluated for vNIC and port statistics.

### Sun JAVA

- CSCsq23360 The "BadFieldException" is no longer given by Java Web Start when launching the KVM viewer.

### Service Profile

- CSCta11597 Creation of a service profile by a server autoconfiguration or server inheritance policy can now delete service profiles created previously by a policy.
- CSCta29147 New Dynamic Connection Policy values are now show up when you edit a service profile
- CSCta30015 When modifying the Serial Over LAN SOL Policy of a service profile, the Serial Over LAN Policy drawer will now immediately reflect the new value.

### Server

- CSCta74115 If a service profile is created through a server autoconfiguration policy and from a template associated with a server pool, changes to the template will get applied on the server.

## Caveats from Previous Releases

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

### AAA

- CSCsz44814

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

**Workaround** Do not include the "\$" character in local user passwords.

- CSCta09972

**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.

- CSCta48483

**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.

### Adapters

- CSCsw39341

**Symptom** With fabric failover being enabled in a service profile associated with a QLogic or Emulex CNA, there is a potential traffic loss in the network-to-host direction if the fabric interconnect is operating in End Host mode. The duration of loss depends on how soon after failover the host sends a packet towards the network.

**Workaround** The traffic loss ends as soon as the host sends a packet after the failover. If the host is a silent host, inject traffic from the host towards the network.

- CSCsz68887

**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.

- CSCsx42435

**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
```

## BIOS

- CSCsy97698

**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.

- CSCsz99666

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

**Workaround** None.

- CSCsz41107

**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.

## Fabric Interconnect

- CSCsv92356

**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.

- CSCsx13134

**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.

- CSCsy15489
 

**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.
- CSCsz75747
 

**Symptom** When you set TFTP core exporter IP address through the UCS Manager, the fabric interconnect accepts the address even if it is malformed; for example, 1.2.3.412. This has no functional impact to core exporter with valid IP addresses.

**Workaround** Remove the malformed core exporter IP address.
- CSCta09325
 

**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.
- CSCta16847
 

**Symptom** Changing the QoS class of service value for FCoE traffic can disruptive FCoE traffic. FC I/O would be dropped.

**Workaround** The QoS architecture should be planned before deploying. Be aware that a change in class of service value for FCoE traffic can disrupt FCoE traffic.
- CSCta25287
 

**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.
- CSCta31689
 

**Symptom** Under some circumstances, syslog messages are not shown on a terminal monitor even though logging on the terminal monitor is enabled globally and on a particular session.

**Workaround** Use a different syslog destination, such as console, remote server, or local log file.
- CSCta36817
 

**Symptom** When multiple SNMP trap hosts are configured, SNMP traps are only sent to the first host.

**Workaround** Configure only one SNMP trap host.

#### Faults and Alerts

- CSCsz01878
 

**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.

- CSCta76573

**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.

### High Availability

- CSCsz40462

**Symptom** On a system with five or more chassis, the following sequence of events causes the system to not be HA ready for up to five minutes:

1. Discover all chassis
2. Wait for HA READY
3. Decommission all chassis
4. Recommission all chassis

**Workaround** Wait for HA READY.

- CSCsz85876

**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.

### Inventory

- CSCta12005

**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 sprom component** command and look for **H/W Version:** field in the command output.

- CSCta56527

**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.

### Operating Systems

- CSCsy24735

**Symptom** When the RHEL 5.3 XEN kernel is booted, the "MCFG area at a0000000 is not E820 reserved" error message appears as a part of the boot messages.

**Workaround** This is a known issue and a misleading error statement (to be removed by Red Hat in the 5.5 release). It does not affect any functionality of the system. Ignore the error message.

### Pinning

- CSCta60495

**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.

### Pools and Policies

- CSCta06882

**Symptom** The assignment of servers to pools in a dynamic pool are not dynamically assigned. To have a server assigned to a pool, it must be re-acknowledged. This should happen automatically based on the server pool policy qualifications as soon as the qualification is associated to a pool.

**Workaround** Re-acknowledge the server to enable it as a candidate for pool assignment.

### Server

- CSCsx33526

**Symptom** Do not mix local disk and SAN boot targets at same time.

**Workaround** Define one boot option at a time under the Storage Type.

- CSCsy80888

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

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

- CSCsy20036

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

**Workaround** None.

**SNMP**

- CSCta22029

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

**Workaround** None.

- CSCta24034

**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.

**SMASH**

- CSCsv87256

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

**Workaround** None.

**UCS Manager CLI**

- CSCsz47512

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

**Workaround** Clear the counters using the UCS Manager GUI.

**UCS Manager GUI**

- CSCta24307

**Symptom** In the Service Profile Navigator GUI, when changing the boot policy type, such as from no boot policy to a specifically-created boot policy, clicking **Reset Values** fails to reset the page to the initial status.

**Workaround** Select a different object in the navigation tree, such as the root organization, and then select the service profile again.

- CSCta38463

**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.

- CSCta54895

**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.

- CSCta66375

**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.



**UUID**

- CSCta40790

**Symptom** When the time-based UUID generation method is used in the uuidgen tool, the system reports duplicate UUIDs because UUIDs are validated based on their suffix, whereas time-stamp method creates UUIDs with unique prefixes, but non-unique suffixes.

**Workaround** Use the random method in the uuidgen tool to ensure that suffixes are unique.

## New Hardware Features in Release 1.0(2)

This release adds support for the UCS B250 M1 Extended Memory Blade Server.

## New Software Features in Release 1.0(2)

The B-200 blade server's BIOS vendor now displays as "Cisco Systems, Inc."

CDP can be enabled/ disabled on a per vNIC basis.

A new CLI command is added in the network control policy. The **set uplink-fail-action** command can be set to either *link-down*, or *warning*.

UCSM enforces mutual exclusion of local disk and SAN boot in a single boot policy.

The boot order table in the BIOS strictly follows the UCS Manager boot order.

UCS instances now scale to up to 8 UCS 5108 chassis.

## Related Documentation

- [Cisco UCS Documentation Roadmap](#)
- [Cisco UCS Manager Troubleshooting Guide](#)
- [MIB Quick Reference for Cisco UCS Manager](#)

## Hardware Documents

- [Cisco UCS Site Preparation Guide](#)
- [Cisco UCS 5108 Server Chassis Hardware Installation Guide](#)
- [Cisco UCS 6100 Series Fabric Interconnect Hardware Installation Guide](#)
- [Regulatory Compliance and Safety Information for Cisco UCS](#)

## Software Documents

- [Cisco UCS Manager CLI Configuration Guide](#)
- [Cisco UCS Manager GUI Configuration Guide](#)
- [Cisco UCS Manager CLI Command Reference](#)
- [Cisco UCS Manager XML API Programmer's Guide](#)

# Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

---

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

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [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. (1005R)

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.

© 2009–2010 Cisco Systems, Inc. All rights reserved.