



Release Notes for Cisco UCS Central, Release 1.1

First Published: July 15, 2013

Updated: June 26, 2015

OL-29853-01

This document describes system requirements, new features, resolved caveats, known caveats, and open caveats with workarounds for Cisco UCS Central software Release 1.1(1a), 1.1(1b), and 1.1(2a). This document also includes information that became available after the technical documentation was published.

Use this release notes as a supplement with the other documents listed in documentation roadmap <http://www.cisco.com/go/unifiedcomputing/b-series-doc>.

Make sure to review other available documentation on Cisco.com to obtain current information on Cisco UCS Central.

Contents

This document includes the following sections:

- [Revision History](#)
- [Introduction](#)
- [New Software Features](#)
- [Upgrade Paths](#)
- [Resolved Caveats](#)
- [Open Caveats](#)
- [Known Limitations and Behaviors](#)
- [Related Documentation](#)
- [Obtaining Documentation and Submitting a Service Request](#)



Revision History

Table 1 shows the revision history:

Table 1 Online Change History

Part Number	Release	Date	Description
OL-29853-01	All releases	June 24, 2015	Added known limitation related to issue reported in CSCus21388.
	1.1(1a)	July 15, 2013	Created release notes for Cisco UCS Central Release 1.1.
	1.1(1a)	July 30, 2013	Added additional caveats.
	1.1(1a)	August 19, 2013	Added CSCui54228 in open caveats.
	1.1(1b)	October 31, 2013	Updated release notes for Release 1.1(1b).
	1.1(1b)	December 12, 2013	Added CSCum00747 in open caveats.
	1.1(2a)	March 10, 2014	Updated release notes for Release 1.1(2a).
	1.1(1a)	March 26, 2014	Added CSCun84897 in open caveats for 1.1(1b); changed 2.2(1b) heading (in Feature Support Matrix) to 2.2(1x).
	-	November 11, 2014	Added information on Bash Update bin . Updated release version 2.2(2x) in feature support matrix.

Introduction

Cisco UCS Central, Release 1.1 allows you to take charge of the data center environment by delivering easy to use, integrated solution for managing multiple Cisco UCS Domains from a single management point with high availability. With Cisco UCS Central 1.1, you can efficiently manage server, storage and network policies, and generate network traffic reports for your entire UCS environment in one or more data centers.

System Requirements

To access the browser based Cisco UCS Central GUI, your computer must meet or exceed the following minimum system requirements:

- Windows
 - Internet Explorer 9 and above
 - Firefox 15 and above
 - Chrome 22 and above
- Linux RHEL
 - Firefox 15 and above

- Chrome 22 and above
- MacOS
 - Firefox 15 and above
 - Chrome 22 and above
 - Safari 6 and above

Adobe Flash Player 11.7 and above.

For the Chrome browser, remove the bundled flash player and install the flash player from Adobe.

The released OVA or ISO is supported with ESXi4.1U2, ESXi5.0, ESXi5.1GA and ESXi5.5GA.

The released ISO is supported with Microsoft Hyper-V Server 2008 R2 SP1 and Microsoft Hyper-V Server 2012.



Note

If you are using Cisco UCS Release 1.1(2a), you must be running Cisco UCS Release 2.1(2a) or higher. Some features of UCS Central 1.1(2a) may only work with later releases of Cisco UCS Manager.

New Software Features

This section contains:

- [New Software Features in Release 1.1\(2a\)](#)
- [Feature Support Matrix for Release 1.1\(2a\)](#)
- [New Software Features in Release 1.1\(1b\)](#)
- [New Software Features in Release 1.1\(1a\)](#)

New Software Features in Release 1.1(2a)

Release 1.1(2a) supports the following:

- Browse and import service profile templates and policies from registered UCS domains¹
- Cisco UCS Manager multi-version management
- Remote Management, which includes the ability to do the following:
 - Perform remote actions on endpoints in registered UCS domains
 - Collect tech support on registered UCS domains
 - Copy backup files to a remote location¹
- Additional report options in statistics management, including:
 - Cooling
 - Power
 - Temperature
- 3rd party certificates¹
- Support for IPv6 inband management¹
- Operational policies specific to Cisco UCS Central are moved to the Administration tab

1. For version support information, see [Feature Support Matrix for Release 1.1\(2a\)](#).

- Logs and Faults tab for centralized view of logs and faults
- Sequential ID allocation for pools, such as MAC addresses, WWNs, Management IP, and UUIDs
- VLAN/VSAN localization for registered Cisco UCS domains
- Microsoft SQL database support
- Authentication Domain selection

Feature Support Matrix for Release 1.1(2a)

The following table provides a list of features in Cisco UCS Central Release 1.1(2a) and Cisco UCS Manager release versions in which these features are supported.



Note

New features such as specifying remote a location for backup image files, 3rd party certificates, and IPv6 inband management support are built in Cisco UCS Central to be compatible with upcoming Cisco UCS Manager releases.

Table 2 Cisco UCS Central 1.1(2a) Features and Supported Cisco UCS Manager Release

Cisco UCS Central Features	Supported Cisco UCS Manager Versions		
	2.1(2a)*	2.2(1x)	2.2(2x)
Multi-version management support and viewing supported Cisco UCS Manager features	No	Yes	Yes
Importing policy/policy component and resources	No	Yes	Yes
Specifying remote location for backup files	No	No	Yes
3rd party certificates	No	No	Yes
IPv6 inband management support	No	No	Yes



Note

- * Includes maintenance and patch releases.
- Searching for policy/policy components or resources is supported in Cisco UCS Manager, Releases 2.1(2x) and 2.1(3x). To import policies, you must have Cisco UCS Manager, Release 2.2(1c) or higher, and yet some of the features might not be available.

New Software Features in Release 1.1(1b)

Release 1.1(1b) supports the following:

- LDAP Group maps
- Nested LDAP groups

New Software Features in Release 1.1(1a)

Release 1.1(1a) supports the following:

- Global Service Profile and Templates
- Global Policies
 - Server Policies
 - Adapter
 - BIOS
 - Boot
 - IPMI Access Profiles
 - iSCSI Authentication
 - Host Firmware Packages
 - Local Disk Configuration
 - Power Control
 - Maintenance
 - Scrub
 - Serial over LAN
 - Server Pool
 - Server Pool Qualification
 - Stats Threshold
 - vNIC/vHBA Placement
 - Network Policies
 - VLAN
 - vNIC
 - vNIC Template
 - Default vNIC Behaviour
 - QoS
 - Network Control
 - Dynamic vNIC Connection
 - LAN Connectivity
 - Threshold
 - Storage Policies
 - VSAN
 - vHBA
 - vHBA Template
 - Default vHBA Behaviour
 - SAN Connectivity

-Threshold

- Policy Globalization and Localization
- Global VLAN and VSAN Support
- VLAN Aliasing
- Org Aware Policies
- Domain-specific ID pools
- Enhanced Inventory
- Network Statistics Collection and Aggregation
- Reporting on Collected Statistics for Networks
- Centralized XML API
- High Availability
- SNMP support
- Licensing
- 64-Bit Support
- SQL MIT
- Service Profile Renaming

Upgrade Paths

To deploy a fresh installation of Cisco UCS Central, Release 1.1(1b) or higher, you can use either the OVA file or the ISO image. See the [Cisco UCS Central Install and Upgrade Guides](#) for more information.

To upgrade Cisco UCS Central, you must use the ISO image. The following upgrade paths are supported:

- Release 1.1(1b) to Release 1.1(2a)
- Release 1.1(1a) to Release 1.1(2a)



Note

To upgrade Release 1.0(1a), you must first upgrade to 1.1(1a). After the upgrade has successfully completed, you can then upgrade to Release 1.1(2a).

Bash Update bin

UCS Central bash update bin (ucs-central-bash-update-3.2-33.el5_11.4.bin) provides a fix for the Security Vulnerabilities CVE-2014-6271 and CVE-2014-7169. This bash update bin is included in release 1.2(1d) ISO.



Note

You are not required to upgrade to 1.2(1d) to use the bash update bin. You can use the bash update bin to just fix the security vulnerabilities on any Cisco UCS Central 1.1 releases. Download the bash update bin from here: [Download bash update bin](#).

Do the following using the Cisco UCS Central CLI to download and install the bash bin update

- Download the bash update bin from Cisco.com to a local scp/ftp/sftp/tftp server.
- Update the bash update bin using the following update command:

```
UCSC-VM1# connect local-mgmt
UCSC-VM1(local-mgmt)# update
<protocol>://<user_name>@<server_ip>/<file_location>/ucs-central-bash-update-3.2-33.e15_11
.4.bin
```

protocol: protocol supported by the local server where the file is downloaded
user_name: authorized user name on the local server
server_ip: ip/hostname of the local server
file_location: location of the bin file on local server

**Note**

If you have installed Cisco UCS Central in HA setup, make sure to install the bash bin update in both nodes.

Resolved Caveats

Resolved Caveats in Release 1.1(2a)

The following caveats are resolved in Release 1.1(2a):

Table 3 **Resolved Caveats in Release 1.1(2a)**

Defect ID	Description
CSCuh01992	The Estimate Impact action no longer states that a reboot is not required for changing policies and upgrading host firmware packs.
CSCuh90667	The Status column on the Global Service Profiles table no longer fails to match the actual status of the service profile as reported by Cisco UCS Manager.
CSCui51884	When you create a global service profile using the service profile template and create an iSCSI vNIC using the LAN connectivity policy, the global service profile no longer enters a loop and fails to complete the process.
CSCuj84470	The Cisco UCS Central SecAG process no longer crashes if local users have usernames with specific strings and use the password reset ISO to reset the password.
CSCud25361	NFS mount failures no longer occur on Cisco UCS Manager after regenerating the certificate from Cisco UCS Central.

Resolved Caveats in Release 1.1(1b)

The following caveats are resolved in Release 1.1(1b):

Table 4 **Resolved Caveats in Release 1.1(1b)**

Defect ID	Description
CSCui08318	Microsoft Hyper-V Server 2008 and 2012 no longer experiences time-drift issues.
CSCuj76375	Cisco UCS Central LDAP user will no longer have any authentication issues to log into one VM using the CLI when logged into another VM.
CSCui67339	When you upgrade Cisco UCS Central from release 1.0 to 1.1, the local service profiles will no longer be missing from the GUI.
CSCuj60761	The UCS Central resource manager will no longer crash and fail to restart.

Table 4 *Resolved Caveats in Release 1.1(1b) (continued)*

Defect ID	Description
CSCui38707	When you delete a service profile template with at least one global service profile, the Fabric VCon from the placement policy will get deleted.
CSCui56705	When you move IP address from one IP pool to another the ID usage will automatically be updated.
CSCui02748	The UCS fault panel will no longer show blank space.
CSCui08275	Overall status icon will no longer display wrong status message.
CSCuj63268	Cisco UCS Central resource manager no longer crashes after PMON restart when restrict migration is set on any associated global service profiles.

Resolved Caveats in Release 1.1(1a)

The following caveats are resolved in Release 1.1(1a):

Table 5 *Resolved Caveats in Release 1.1(1a)*

Defect ID	Description
CSCuc94589	When creating a maintenance policy in the CLI, the set reboot-policy immediate command is now saved when the maintenance policy is created.
CSCuc98962	In the Cisco UCS Central GUI, the suspend state shown in the Equipment > UCS Domains table now updates immediately.
CSCud20882	If there are two DNS entries configured in Cisco UCS Central, and the first DNS entry is incorrect or non-reachable, UCS Central will import or export files using the second DNS entry.
CSCud26790	When the CIMC management ip-address is changed from pool ip-address to static ip-address for a server, Cisco UCS Central can crosslaunch KVM for that server.
CSCue21033	Cisco UCS Central OVA no longer misaligns I/O requests at the storage filers hosting the related VMDKs.
CSCue62790	Special characters for password and shared secret no longer corrupt the sam.config file.
CSCud25795	When a full-state restore is done on Cisco UCS Central, subsequent Cisco UCS Manager registrations will now be successful.
CSCud21949	After full-state import and erase samdb, the equipment tab no longer remains in loading state.
CSCud26193	The "Overall Status" column on the Tech Support Files page (Administration > Diagnostics > Tech Support Files) now changes from "in-progress" to "available" when tech-support collection process is complete.

Open Caveats

Open Caveats in Release 1.1(2a)

The following caveats are found in Release 1.1(2a):

Defect ID	Symptom	Workaround
CSCug53341	When the snmpwalk or snmpget commands are issued, the values for some devices are not retrieved.	There is no workaround for this issue.
CSCun33749	If Cisco UCS Central backup policies that use a remote server are used by Cisco UCS Manager 2.1(1c) or earlier, the backup file is set to the remote server, but the date, time, and Cisco UCS Manager domain information is stripped from the backup file name.	Use a local backup policy instead of backing up to a remote server.
CSCu179152	If you create VLANs and VSANS in a Cisco UCS Manager vNIC or vHBA template, and then register Cisco UCS Manager, the VLANs and VSANS are not imported into Cisco UCS Central.	Import the required VLAN or VSAN directly from Cisco UCS Manager using the Import tab.
CSCun25187	When certificate chains are configured in Cisco UCS Central, Cisco UCS Manager goes into Lost-Visibility.	Key-rings signed by a subordinate CA are not supported. Only use key-rings signed by a root CA.

Open Caveats in Release 1.1(1b)

The following caveats are found in Release 1.1(1b):

Table 6 Open Caveats in Release 1.1(1b)

Defect ID	Symptom	Workaround
CSCun84897	User ack maintenance policy setting is ignored when changing MTU in a vNIC template in Global Service Profile and causes an immediate reboot.	Create vNICs either directly under Global Service Profile (or SP template) or through Global LAN Connection Policy.
CSCum00747	Local service profile templates are not deleted from Cisco UCS Central inventory when they are deleted from a registered UCS domain.	Log into the Cisco UCS Central resource manager using CLI, from the specific domain, run “refresh-inventory” command to remove the local service profile templates.

Table 6 *Open Caveats in Release 1.1(1b) (continued)*

Defect ID	Symptom	Workaround
CSCUj84470	If the local-users have usernames with specific strings and use password reset ISO to reset the password, Cisco UCS Central SecAG keeps crashing. Resolved in 1.1(2a).	Out of sync entries must be removed from the config files. Contact Cisco TAC for workaround.
CSCUi51884	When you create a global service profile using the service profile template and create iSCSI vNIC using LAN connectivity policy, the global service profile enters a loop and does not complete the process. Resolved in 1.1(2a).	Make sure to create iSCSI vNIC using the expert mode. Do not create iSCSI vNIC from the LAN connectivity policy.
CSCUj65996	When you create a simple password using Cisco UCS Central GUI, if password strength is enforced, the simple password will not be applied on the server.	The new password change did not take effect, because it was weak. Login using the original password, and change the password using the CLI.

Open Caveats in Release 1.1(1a)

The following caveats are found in Release 1.1(1a):

Table 7 *Open Caveats in Release 1.1(1a)*

Defect ID	Symptom	Workaround
CSCUi54228	On Microsoft Hyper-V, If the storage reserved for disk1, disk 2 or shared storage is exactly 40 GB, Cisco UCS Central installation fails even if the minimum storage requirement is set at 40 GB.	To install Cisco UCS Central in standalone or high availability mode, the minimum storage requirement for disk 1,disk 2 and shared storage is 45 GB.
CSCUf85283	When the system boots, you may experience errors when issuing CLI commands before the system has booted successfully.	Wait for the system to complete the boot process before continuing.
CSCUf85283	The Cisco UCS Central CLI session might fail to communicate with the data management engine (DME) and return the following error: Exception during execution: [Error: Timed out communicating with DME] This occurs when the CLI is accessed immediately after a reboot before the DME is ready.	Wait a few seconds, then run the Cisco UCS Central CLI command again.

Table 7 **Open Caveats in Release 1.1(1a) (continued)**

Defect ID	Symptom	Workaround
CSCuh90667	The Status column on the Global Service Profiles table may not match the actual status of the service profile as reported by Cisco UCS Manager. Resolved in 1.1(2a).	To view the actual status of a global service profile, right-click the service profile and choose Properties . The Properties dialog box displays the overall status, assigned status, associated status, and any configuration errors.
CSCui06133	Dynamic vNIC connection policy configuration for SRIOV is not supported in Cisco UCS Central, Release 1.1(1a).	Create a dynamic vNIC connection policy for SRIOV in Cisco UCS Manager, and reference the policy in a local service profile.
CSCuh01992	The Estimate Impact action states that a reboot is not required when changing from one policy to another, and that the new policy does not exist in Cisco UCS Manager. The Estimate Impact action also states that a reboot is not required when a new host firmware pack with a different firmware version is selected on the global service profile properties page. A reboot is part of the firmware activation and is not being reported by Estimate Impact. Resolved in 1.1(2a).	This issue has no known workaround.
CSCub26954	Pending user-acks from maintenance policies defined in Cisco UCS domains are not displayed in Cisco UCS Central.	To see pending user-acks in Cisco UCS Central, use the schedules defined in Cisco UCS Central. Modify the maintenance policy to refer to a schedule owned by Cisco UCS Central. If you are using the local scheduler, use Cisco UCS Manager to acknowledge the pending acks.
CSCug53341	An hrDeviceStatus value is not retrieved for all devices while doing an snmpwalk or snmpGet. A value is only retrieved for interfaces and not for hard disks.	This issue has no known workaround.
CSCtz35499	When you modify the UCS Central IP address, Cisco UCS Manager may not be receive the update, and might go into lost-visibility status.	Unregister the Cisco UCS domain and re-register the domain with Cisco UCS Central.

Table 7 Open Caveats in Release 1.1(1a) (continued)


Defect ID	Symptom	Workaround
CSCud27361	<p>The following is not supported on the Cisco UCS Central GUI:</p> <ul style="list-style-type: none"> • Changing the Cisco UCS Central shared-secret. • Changing the Cisco UCS Central hostname. • Changing the Cisco UCS Central IP address. <p> Note If Cisco UCS Central is running in High-Availability mode, you can change the IP address under Administration > Service Registry > System > General.</p>	<p>Run the following commands from the Cisco UCS Central CLI:</p> <ul style="list-style-type: none"> • Use the local-mgmt command to change the shared-secret. • Use the scope system command to change the hostname. • Use the scope network-interface mgmt command to change the IP address.
CSCuc96920	<p>In the Cisco UCS Central GUI, the policies under Operation Management > Domain Group > Operational Policies cannot be saved simultaneously. This includes Time Zone, DNS, Remote Access, SNMP, Debug, Call Home, Security, Equipment, and Identifier policies.</p>	<p>When you configure an operational policy, click Save before viewing or changing a different policy.</p>

Table 7 Open Caveats in Release 1.1(1a) (continued)

Defect ID	Symptom	Workaround
CSCui08318	Microsoft Hyper-V Server 2008 and 2012 experience time-drift issues. Resolved in Release 1.1(1b).	<p>Perform the following:</p> <ol style="list-style-type: none"> 1. Disable the Time Synchronization option on the Central VM Guest OS using Hyper-V Manager. 2. Acquire a Redhat version 5.8 compatible Rescue CD and perform the boot process. For more information, see http://www.redhat.com/advice/tips/rescue_mode.html 3. After booting the RedHat Rescue CD, mount the /boot filesystem to a temporary mount location, for example, /tmp/boot. 4. Open the grub.conf file, locate the kernel line, and add the following: notsc divider=10 It should look like: ***** UCSCentral#cat /boot/grub/grub.conf ***** # grub.conf generated by anaconda # # Note that you do not have to rerun grub after making changes to this file # NOTICE: You have a /boot partition. This means that # all kernel and initrd paths are relative to /boot/, eg. # root (hd0,0) # kernel /vmlinuz-version ro root=/dev/VolGroup00/LogVol100 # initrd /initrd-version.img #boot=/dev/hda default=0 timeout=0 title Cisco UCS Central root (hd0,0) kernel /vmlinuz-2.6.18-308.11.1.el5 ro root=/dev/VolGroup00/LogVol100 notsc divider=10 initrd /initrd-2.6.18-308.11.1.el5.img 5. Reboot the system, and verify the change works successfully by monitoring for one hour.

Known Limitations and Behaviors

The following known limitations and behaviors are not otherwise documented:

Table 8 *Known Limitations in Release 1.1(1a)*

Defect ID	Symptom	Workaround
CSCus21388	In a cluster set up, when the RDM link goes down on the primary node, DMEs cannot write to the database. This causes a crash on the primary node and failover to the subordinate node. The subordinate node takes over as the primary node. The database is then mounted in read-write mode on the new primary node. Because the RDM link is down, umount fails on the old primary node. When the RDM link comes up, the database is mounted on the old primary (current subordinate) node in read-only mode.	Restart pmon services on the current subordinate node or restart the node itself. Either of these processes will unmount the read-only partition and enable proper cleanup.
CSCug39587	Running VMware vMotion, suspending a VM, or restoring a suspended VM on a Cisco UCS Central VM that is currently the primary node in a cluster results in process crashes on the node.	Before triggering a vMotion or suspend operation on the primary Cisco UCS Central VM, use the local-mgmt cluster lead b command in the Cisco UCS Central CLI to do an administrative failover, which changes the primary node to the secondary node.
CSCuh71425	The Estimate Impact option does not display that a reboot is required under some situations. For example: <ul style="list-style-type: none"> When you add or remove vNICs or vHBAs from an associated global service profile where the MAC or WWxN IDs are derived from ID pools. When you change policies in a global service profile to a policy that was created in Cisco UCS Central, and does not yet exist in Cisco UCS Manager. When a new host firmware pack with a different firmware version is selected in the global service profiles properties page. 	<ul style="list-style-type: none"> For vNICs/vHBAs in pools, add and remove vNICs and vHBAs during a maintenance window. Estimate impact analysis works correctly for vNICs/vHBAs where the IDs are set manually. For policies, create an unassociated local service profile in Cisco UCS Manager. Reference the new policy in the service profile. Estimate impact analysis will now work correctly. For host firmware packages, create a host firmware package in Cisco UCS Central under the same domain group as the global service profile. Create an unassociated service profile in Cisco UCS Manager and reference the new host firmware package in the service profile. Estimate impact analysis will now work correctly.

Table 8 **Known Limitations in Release 1.1(1a) (continued)**

Defect ID	Symptom	Workaround
CSCud26491	A critical disk read speed fault is shown in an UCS Central deployed on a Hyper-V host.	None. In testing, it was found that the disk read speed measured on Hyper-V guests showed a lower speed in comparison to guests running on ESX on the same datastore. Typically, this didn't result in a functional impact.
CSCug68204	When performing maintenance operations such as admin failover or pmon restart on a UCS Central VM running on VMware ESX, the file system goes into read-only state. For more information, see http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&externalId=51306 .	There is no known workaround.

Related Documentation

For more information, you can access related documents from the following links:

- [Cisco UCS Documentation Roadmap](#)
- [Cisco UCS Central Install and Upgrade Guides](#)

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. 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.

© 2013–2014 Cisco Systems, Inc. All rights reserved.