Release Notes for Cisco UCS Central, Release 1.3

First Published: April 8, 2015

Updated: July 11, 2017

This document describes system requirements, new features, resolved caveats, known caveats, and open caveats with workarounds for Cisco UCS Central software Release 1.3. This document also includes information that became available after the technical documentation was published.

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:

Cisco Systems, Inc.
www.cisco.com

Revision History

Table 1 shows the revision history:

Table 1 Online Change History

Release	Date	Description
1.3(1a)	April 8, 2015	Created release notes for Cisco UCS Central Release 1.3(1a).
—	June 24, 2015	Added known limitation related to issue reported in CSCus21388.
—	July 1, 2015	Updated Feature Support Matrix for Cisco UCS Central Releases.
1.3(1b)	July 13, 2015	Created release notes for Cisco UCS Central Release 1.3(1b).
1.3(1b)	September 11, 2015	Added CSCur64858 to 1.3(1b) resolved caveats.
1.3(1c)	November 3, 2015	Created release notes for Cisco UCS Central Release 1.3(1c).
—	March 28, 2016	Updated CSCuw13997.
—	February 6, 2017	Added guidelines for downloading firmware images from Cisco.com.
—	July 11, 2017	Added supported versions of Cisco UCS Manager

Introduction

Cisco UCS Central, Release 1.3 allows you to take charge of the data center environment by delivering easy to use, integrated solution for managing multiple Cisco UCS Domains in data center and remote environments, from a single management point with high availability. With Cisco UCS Central, Release 1.3, you can efficiently manage server, network and storage policies, and generate network traffic reports for your entire UCS environment in one or more data centers.

Release 1.3 also introduces a new task based HTML5 UI. The current Flash-based user interface is available, and is the default interface for general operational purposes.

Guidelines for Downloading Firmware Images from Cisco.com

After March 3, 2017, Cisco UCS Central version 1.3 or earlier will be unable to fetch the updated firmware image list from Cisco.com. If you are running Cisco UCS Central version 1.3 or earlier, you can manually download firmware images directly from Cisco.com and import them to Cisco UCS Central. To continue to have Cisco UCS Central fetch the available image data from Cisco.com and place the firmware image in the Image Library, Cisco recommends that you upgrade to Cisco UCS Central release 1.5 or later.

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 29 and above
  - Chrome 34 and above
- Linux RHEL

  - Firefox 29 and above
  - Chrome 34 and above
- MacOS
  - Firefox 29 and above
  - Chrome 34 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 ISO is supported by the following:

- VMWare ESXi5.0 U3, ESXi5.1, ESXi5.5, and ESXi 6.0
- Microsoft Hyper-V Server 2008 R2 SP1 and Microsoft Hyper-V Server 2012
- KVM Hypervisor on Redhat Enterprise Linux 6.5

The released OVA is supported by VMWare ESXi5.0 U3, ESXi5.1, ESXi5.5, and ESXi 6.0

Note If you are using Cisco UCS Central Release 1.2(1a) or later, you must be running Cisco UCS Manager Release 2.1(2a) or higher. Some features of UCS Central 1.2(1a) may only work with later releases of Cisco UCS Manager.

New Software Features

This section contains:

New Software Features in Release 1.3(1a)

Release 1.3(1a) supports the following:

- HTML5 UI: New task based HTML5 user interface.
- KVM Hypervisor Support: Ability to install Cisco UCS Central in KVM Hypervisor
- Scheduled backup: Ability to schedule domain backup time. Provides you flexibility to schedule different backup times for different domain groups.
- Domain specific ID pools: The domain specific ID pools are now available to global service profiles.
- NFS shared storage: Support for NFS instead of RDM for the shared storage is required for Cisco UCS Central cluster installation for high availability.
- vLAN consumption for Local Service Profiles: Ability to push vLANs to the UCS Manager instance through Cisco UCS Central CLI only without having to deploy a service profile that pulls the vLANs.
- Support for Cisco M-Series Servers.
- Connecting to SQL server that uses dynamic port.
- Support for SQL 2014 database and Oracle 12c Database.

Feature Support Matrix for Cisco UCS Central Releases

The following table provides a list of features in Cisco UCS Central, and Cisco UCS Manager release versions in which these features are supported. Features that are not listed are supported with Cisco UCS Manager 2.1(2a) and later.

Table 2 Cisco UCS Central Features and Supported Cisco UCS Manager Release

Cisco UCS Central Features	Supported Cisco UCS Central Versions	Supported Cisco UCS Manager Versions			
		2.1(2a)/ 2.1(3)	2.2(1)	2.2(2) or later	3.0(1) or later
Multi-version management support and viewing supported Cisco UCS Manager features	1.1(2a) and later	No	Yes	Yes	Yes
Importing policy/policy component and resources		No	Yes	Yes	Yes
Specifying remote location for backup files		No	No	Yes	Yes
3rd party certificates		No	No	Yes	Yes
IPv6 inband management support		No	No	Yes	Yes
Estimate Impact on Reconnect	1.2(1a) and later	No	No	Yes **Note**: Supported only from 2.2(3x)	Yes
Precision Boot Order Control		No	Yes	Yes	Yes
Scriptable vMedia	1.2(1e) and later	No	No	Yes **Note**: Supported only in 2.2(2c) and later 2.2(x) releases.	No **Note**: Supported in 3.0(2) and later.

Note 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, releases 2.2(1b) or higher

Supported Versions of Cisco UCS Manager

Cisco UCS Central 1.3 supports Cisco UCS Manager versions 2.1, and 2.2 up to 2.2(6).

Behavior and Design Changes in HTML5 UI

Feature Support

The following features available in the current UI is not supported in the HTML5 UI yet:

- Policy Import
- Threshold Policy
- Statistics

Behavior Changes Based on Design

- Create global service profile only using an initial or updating template. You have to make sure to create the global service profile template before creating service profile.
- The following inline options are not available in a service profile:
  - Manual vNIC
  - iSCSI
  - vHBA
  - Boot Policy
  - Static ID, etc.

If you have an existing global service profile with all these options, you cannot edit the global service profile in the HTML5 UI.

- You can use the vNIC template only in LAN connectivity policy.
- You can use the vHBA template only in SAN connectivity policy.
- vNIC and vHBA Placement is now referred to as Interface Placement.
- Registration Policy is now referred to as Domain Group Qualification Policy.
- ID Range Qualification Policy is now referred to as ID Range Access Control Policy.
- There are no qualified IP addresses for ID Range Access Control Policy.
- You can create server pool policies when creating a server pool. Select Server Pool Qualification Policies to create these policies.
- When assigning server pools, additional server pool qualification is not supported in the global service profile.
- The only backup option is config-all backup. Other backup types such as config logical and config system are not supported.
- Local service profile picks up Host Firmware Policy from the Org instead of the Domain Group.
- When import fails in HTML 5 UI, the message displays the reason for import failure. Make sure to correct errors and resubmit the configuration for import.
- Local service profile inventory is not displayed.
- The maintenance policy and schedules that are currently used by local service profiles and currently under domain groups will not be available in HTML5 UI.

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. You can upgrade Cisco UCS Central to release 1.3(1a) or later from any of the following two releases:

- From 1.1(2a) to 1.3(1a) or later
- From 1.2(x) to 1.3(1a) or later

Note To upgrade Release 1.0(1a), you must first upgrade to 1.1(1b) release. After the upgrade has successfully completed, you can then upgrade to Release 1.2(1x). Also, make sure the registered Cisco UCS Domains are running Cisco UCS Manager, release 2.1(2a) or later.

Resolved Caveats

Resolved caveats are provided in the following release-specific tables:

- Resolved Caveats in Release 1.3(1c)
- Resolved Caveats in Release 1.3(1b)
- Resolved Caveats in Release 1.3(1a)

Resolved Caveats in Release 1.3(1c)

The following caveats are resolved in Release 1.3(1c):

Table 3 Resolved Caveats in Release 1.3(1c)

Defect ID	Description
CSCuw91046	After you create a service profile using service profile template, with UUID pool and management vLAN, you can edit and add a new value to the management vLAN and save the service profile.
CSCuv33856	A vulnerability in the web framework has been fixed, preventing unauthenticated remote attackers from executing arbitrary commands on the Cisco UCS Central operating system.
CSCuv35794	After upgrading to Cisco UCS Central release 1.3, you can now delete UCS Manager infra bundles from UCS Central.
CSCuv61721	You can now change the Call Home policy on a UCS Domain from being locally managed to being managed in UCS Central without receiving a “contact information must be populated” error.
CSCuv93840	You will no longer receive an `Invalid vmedia mount configuration` error after associating a global service profile with a vMedia policy and management IP address to a server that belongs to a server pool.
CSCuw03779	The UCS Central remote backup no longer fails after changing the IP address for a Cisco UCS domain.

Table 3 Resolved Caveats in Release 1.3(1c) (continued)

Defect ID	Description
CSCut91863	A vulnerability in password handling has been fixed, preventing unauthenticated remote attackers from executing arbitrary commands on the Cisco UCS Central operating system.
CSCuu41704	You can now download a Cisco UCS Manager tech support file from the Cisco UCS Central GUI.
CSCuv41835	Cisco UCS Central no longer fails to update firmware when there are different files with the same name but different file sizes, for example, blade or rack server bundles using the same file name when the file sizes are different.
CSCuw13929	The Cisco UCS Central httpd process no longer crashes during normal operation.
CSCuw13997	Cisco UCS Central no longer generates svc_statsMgr_dme[14809] alerts with a registered UCS domain that has stats collection enabled.
CSCuw51297	The incorrect response is no longer received from central-mgr when you use the UCS Central lsInstantiateTemplate API and send a post to http://<IP_Address>/xmlIM/central-mgr.
CSCuw55036	Support for additional UCS Central per domain SKUs, including UCS-CTR-LIC= and UCS-MDMgr-1Dmn=, has been added.
CSCut95198	Extra messages are no longer saved to the licenseAG log files.
CSCuw31849	The Welcome screen in the UCS Central GUI no longer displays every time you launch the HTML5 UI. Note: You must complete the welcome tour one time, click “Don’t show this tour again”, and then click “Done”.
CSCuu32086	If you create a global service profile from a service profile template, where the LAN connectivity policy has a vNIC created from a vNIC template with dynamic vNIC, renaming the service profile no longer causes duplicate dynamic vNICs to be created.

Resolved Caveats in Release 1.3(1b)

The following caveats are resolved in Release 1.3(1b):

Table 4 Resolved Caveats in Release 1.3(1b)

Defect ID	Description
CSCur64858	The LDAP provider bind DN password now accepts special characters. You can enter any standard ASCII characters except for space, § (section sign), ? (question mark), or = (equal sign).
CSCut63069	Users in one locale can no longer view objects that belong to a domain in a different locale.
CSCut75549	The values of modified global default policies no longer reset to factory default when the UCS Central services are restarted.
CSCuu33789	If you change the IP address in UCS Manager, then restart PMON in UCS Central, the Managed System Oper State no longer remains in resetting state.

Table 4 Resolved Caveats in Release 1.3(1b) (continued)

Defect ID	Description
CSCuu35918	VLANs with names between 17 and 32 characters can now be assigned to iSCSI vNIC.
CSCuu41377	Unauthenticated users can not download files from the server.
CSCuu76848	Service profile configuration issues on vNICs will now be cleaned after successful resolution.
CSCuu77620	Global service profiles with advanced boot order no longer fail association on servers running Cisco UCS Manager Release 2.2(4) and 2.2(5).
CSCut75144	UCS Central no longer displays an incorrect timezone after upgrading.
CSCut92204	You can now export table rows in Cisco UCS Central HTML5 UI.
CSCuu56132	The following Apache vulnerabilities are fixed: CVE-2013-5704, CVE-2014-0118, CVE-2014-0226, CVE-2014-0231.
CSCuu91088	Domain inventory no longer fails after upgrading Cisco UCS Central.
CSCuu93384	The Create vNIC Template task in the HTML5 UI no longer fails.
CSCuu14099	Authentication profiles with iSCSI targets no longer fail to save and be applied.
CSCuu29481	You can now acknowledge pending reboot of integrated C-Series servers in the HTML5 UI.
CSCuv06718	It is now possible to acknowledge pending reboot from the second Pending Activities pages in the HTML5 UI.

Resolved Caveats in Release 1.3(1a)

The following caveats are resolved in Release 1.3(1a):

Table 5 Resolved Caveats in Release 1.3(1a)

Defect ID	Description
CSCus42724	The following OpenSSL based vulnerabilities are fixed: CVE-2014-3569 CVE-2014-3570 CVE-2014-3571 CVE-2014-3572 CVE-2014-8275 CVE-2015-0204 CVE-2015-0205 CVE-2015-0206
CSCus38312	LDAP user from one locale cannot make changes to systems in another locale.
CSCur24146	When you create a backup and delete the backup using Cisco UCS Central GUI, the backup file will not fill bootflash with unnecessary backup files.
CSCuq67945	Firmware download in Cisco UCS Central will not fail with longer usernames.
CSCus29680	Cisco UCS Central user with Server Maintenance privileges will be able to acknowledge pending activities.
CSCus29694	Changes made in the system by users other than an administrative user will not be displayed as changes made by an administrative user.
CSCup85700	After restoring Cisco UCS Central and changing management IP address, you will not have any problem with logging into the system.
CSCup86013	Any scheduled activities will be displayed as scheduled activities in global service profile.

Table 5 Resolved Caveats in Release 1.3(1a) (continued)

Defect ID	Description
CSCus53881	The domain feature capability resolution issue is addressed.
CSCus92628	Using global policy in Cisco UCS Central, you can activate selective cores for new generation blade servers.
CSCus99108	Cisco UCS Central will not accpet any invalid third party certificates anymore.
CSCut39575	Time drift of less than 1 second will not prevent UCS Domain registration in Cisco UCS Central.

Open Caveats

The following caveats are open in release 1.3(1a):

Table 6 Open Caveats in Release 1.3(1a)

Defect ID	Symptom	Workaround
CSCut69263	Changing NFS path on Cisco UCS Central HA cluster will result in following situation for UCS Manager releases 2.2(2x) or earlier: • UCS domain backup from UCS Central will not work. • UCS Manager firmware Upgrade from UCS Central will not work.	Use the default fixed path for NFS shared storage in cluster setup.
CSCut75549	Modifying global_default policies in Cisco UCS Central may result in unexpected server reboots when services are restarted in Cisco UCS Central.	Do not modify any default policies in Cisco UCS Central. If you want to modify any global default policy settings, create a new policy with a different name and desired settings.
CSCut74984	When upgrading Cisco UCS Central, registration status displays **Failed** status for Cisco UCS domains with Cisco UCS Manager releases 2.2(3x) and 3.0(2x).	Suspend and acknowledge the UCS domain that displays failed status. This action will trigger Repair Cert FSM and sync-up the UCS domain with UCS Central.

Known Limitations and Behaviors

The following known limitations and behaviors are not otherwise documented:

Table 7 Known Limitations in All Releases

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.

Table 7 Known Limitations in All Releases (continued)

Defect ID	Symptom	Workaround
—	When using the UCS Central HTML5 GUI, you may experience display issues such as missing icons or unclear fonts.	Clear your browser cache and restart the Cisco UCS Central HTML5 GUI.

CSCuv32055	After installing UCS Central on VMware using the ISO image, domain registration may fail due to a time sync issue between UCS Manager and UCS Central.	If this issue occurs, regenerate the certificate manually from the CLI in UCS Central using the following commands:
		`# connect policy-mgr`
		`# scope org`
		`# scope device-profile`
		`# scope security`
		`# scope keyring default`
		`# set regenerate yes`
		`# commit-buffer`

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*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.

This document is to be used in conjunction with the documents listed in the "Known Limitations and Behaviors" section.