Release Notes for Cisco UCS Central, Release 1.4

First Published: 2015-12-17

Last Modified: 2017-02-02

Introduction

This document describes system requirements, new features, resolved caveats, known caveats, and open caveats with workarounds for Cisco UCS Central software Release 1.4. 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.

Revision History

Release	Date	Description
1.4(1a)	December 11, 2015	Created release notes for Cisco UCS Central Release 1.4(1a).
—	December 24, 2015	Added HTML5 UI changes to Behavior Changes in Release 1.4(1a), on page 6.
—	February 17, 2016	Added CSCuy07572.
1.4(1b)	March 31, 2016	Created release notes for Cisco UCS Central Release 1.4(1b).
—	May 3, 2016	Added note on deploying in RHEL 7.2.
—	June 14, 2016	Added CSCuz88005.
1.4(1c)	June 30, 2016	Created release notes for Cisco UCS Central Release 1.4(1c).
—	February 01, 2017	Added guidelines for downloading firmware images from Cisco.com.

Release	Date	Description
—	February 02, 2017	Added guidelines for Cisco UCS Domain Management from Cisco UCS Central.

Guidelines for Downloading Firmware Images from Cisco.com

After March 3, 2017, Cisco UCS Central version 1.4 or earlier will be unable to fetch the updated firmware image list from Cisco.com. If you are running Cisco UCS Central version 1.4 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.

Guidelines for UCS Domain Management from UCS Central

Cisco recommends the following guidelines for managing Cisco UCS domains from Cisco UCS Central:

- Cisco recommends that you always register Cisco UCS domains using Cisco UCS Central's Fully Qualified Domain Name (FQDN). If domains are registered with FQDN, any change in the Cisco UCS Central IP address is transparent to the domain.
- Cisco UCS Central does not support changing Cisco UCS Central's IP address if a Cisco UCS domain is initially registered with a Cisco UCS Central IP address. For more information, see Changing a Cisco UCS Central IP Address in the *Cisco UCS Central Installation and Upgrade Guide*.
- Unregistering a registered Cisco UCS domain in a production system has serious implications. Do not unregister a Cisco UCS domain unless you choose to permanently not manage it again from Cisco UCS Central. For more information about registering and unregistering a Cisco UCS Domain from Cisco UCS Central, see Cisco UCS Domains and Cisco UCS Central in the *Cisco UCS Central Installation and Upgrade Guide*.

  Caution Cisco recommends that you contact Cisco Technical Support if you want to unregister any registered Cisco UCS Domain in a production system.

- You can migrate a Cisco UCS Central instance to support Data Center migration or disaster recovery scenarios. For more information about migrating a Cisco UCS Central instance, see Cisco UCS Central Instance Migration in the *Cisco UCS Central Installation and Upgrade Guide*.
- When you unregister any registered Cisco UCS domain from Cisco UCS Central:
  - You can no longer manage the service profiles, policies, and other configuration for the Cisco UCS domain from Cisco UCS Central.
  - All global service profiles and policies become local and continue to operate as local entities. When you re-register the domain, the service profiles, and polices remain local.

See Related Documentation, on page 16 on Cisco.com for current information on Cisco UCS Central.

System Requirements

Supported Browsers

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

Note If you plan to use the older flash-based UI, you will also need the Adobe Flash Player, version 11.7 and above. To use with the Chrome browser, remove the bundled flash player and install the flash player from Adobe.

Supported Operating Systems

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 and 7.2

Note If Cisco UCS Central is deployed on RHEL 7.2 KVM, the first time you register a Cisco UCS domain, you must regenerate the certificate using the **set regenerate yes** command.

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

Changes in Cisco UCS Central, Release 1.4

New Software Features in Release 1.4(1a)

This release includes full support for the HTML5-based user interface, which is now the default user interface. The previous flash-based user interface is available at http://*UCSCentral_IP*/flex.html.

Release 1.4(1a) supports the following new features in the HTML 5-based user interface:

Feature	Functions
Advanced Local Storage Configuration	• Configuration of Storage Profiles and multiple virtual drives—To allow flexibility in defining the number of storage disks, roles and usage of these disks, and other storage parameters, you can create and use storage profiles. A storage profile encapsulates the storage requirements for one or more service profiles. You can also configure multiple virtual drives. • Configuration of a local LUN or a JBOD as the primary boot device • Support for local storage configuration on multiple storage controllers • Support for out-of-band configuration for local storage
Port Configuration and Disjoint Layer-2 Network	Enables configuration support for ports and port channels, including scalability ports. Also allows upstream disjoint L2 configuration.
Equipment Policies	Global support for chassis discovery policy, rack discovery policy, rack management connection policy, and other equipment-related policies.
Global Service Profile enhancements	• Manual creation of vNICs and vHBAs inside service profiles. • Naming conventions when creating service profiles from templates. • Service profile qualification policy
Adapter Policy enhancements	RoCE, NVGRE, ARFS, and VxLAN added to adaptor policies.

Feature	Functions
New connection policies	• VMQ connection policy • usNIC connection policy
PVLAN	Configuration support for private VLANs.
Advanced Host Firmware Pack	Component exclusion support in host firmware package policy.
Maintenance Policy enhancements	Can now schedule maintenance policies to automatically apply changes at the next reboot.
Smart Call Home	Enables support for Smart Call Home on Cisco UCS Central.
Support for traditional licence management and Smart Licensing	Enables support for the new Smart licensing, as well as continuing support for traditional license management.
Remote Authentication enhancements	Added support for TACACs and RADIUS.
BIOS token support	Includes support for all BIOS tokens included in Cisco UCS Manager, including Consistent Device Naming (CDN).
SNMP Support	Support for sending Cisco UCS Central alerts via SNMP to other management tools.
Cisco UCS Manager 3.1	Pre-enabled support for Cisco UCS Manager release 3.1 and associated hardware platforms.
Boot Policy enhancements	Enables support for booting from multiple LUNs, embedded LUNs and embedded JBOD.
API Communications Report	Enables reporting on active API communications between the GUI and back-end.
Tomcat Logging	Enables logging for Tomcat processes.
Improved VLAN permission management	Allows different organizations to have permissions to different VLANs.
Multi-delete usage analysis	Allows you to see the effect of deleting multiple policies, such as what service profiles use them.

Feature	Functions
General UI enhancements	• Export, saved searches • Domain group and organization view UI enhancements • Enhanced widgets and additional widgets added • Hardware components table view that displays all hardware components within the system, such as FANs, PSUs, and Memory.
Configuration Status	Can view configuration status for Ports, Service Profiles, and Firmware Upgrade scheduling.
Security enhancements	• Added multiple security enhancements as well as updates to the underlying operating system. • Unified KVM launch with KVM-only permissions
Direct-attached Storage (DAS)	Enables connecting a storage array directly to the FI.

New Software Features in Release 1.4(1b)

Release 1.4(1b) supports the following new features in the HTML 5 User Interface:

Feature	Functions
Windows font enhancements	Windows users can now personalize the font size that they want to view on the User Preferences screen.

Behavior Changes in Release 1.4(1a)

Feature Support

The following features that are available in the older flash-based user interface are not supported in the new HTML5 user interface at this time:

- Policy Import
- Threshold Policy
- Statistics

Note Any functionality introduced in Cisco UCS Central release 1.4(1a) and newer releases will be available in the HTML 5 user interface only.

Behavior Changes Based on Design

- You must create the global service profile template before you can create a service profile.
- The following inline options are not available in a service profile:
  - Boot Policy
  - Static ID

  If you have an existing global service profile with any of these options, you cannot edit the global service profile in the HTML5 UI.
- The iSCSI target configuration under the boot policy is not available in the Flex UI.
- 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.
- 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.

Changes in the HTML5 User Interface since Release 1.3

- Ethernet uplink ports configured for Cisco UCS Manager releases prior to 3.1 were supported in Cisco UCS Central release 1.3, but are not supported in Cisco UCS Central release 1.4. Any additional configuration of those ports must be done in Cisco UCS Manager.
- The Cisco UCS Central Release 1.3 Classic Firmware widget and Mini Firmware widget have been combined into one Firmware widget. Any firmware widgets pinned in Release 1.3 are automatically unpinned when you upgrade to Release 1.4. You will need to pin the firmware widgets again.

Feature Support Matrix

The following tables provide a list of features in Cisco UCS Central, and Cisco UCS Manager release versions in which these features are supported:

Note Some features are built in Cisco UCS Central to be compatible with upcoming Cisco UCS Manager releases.

Feature Support for Release 1.4

Cisco UCS Central Features	Supported Cisco UCS Central Versions	Supported Cisco UCS Manager Versions				
		2.1	2.2	2.5	3.0	3.1
Port Configuration	1.4(1a)	No	2.2(7) and later	No	No	3.1(1) and later
Advanced Local Storage Configuration	1.4(1a)	No	2.2(7) and later	2.5(1) and later	No	3.1(1) and later
Multiple LUNs in Boot Policy	1.4(1a)	No	2.2(7) and later	2.5(1) and later	No	3.1(1) and later
Consistent Device Naming	1.4(1a)	No	2.2(4) and later	2.5(1) and later	3.0(1) and later	3.1(1) and later
Direct-Attached Storage/FC Zoning	1.4(1a)	No	2.2(7) and later	No	No	3.1(1) and later
Advanced Host Firmware Pack	1.4(1a)	No	2.2(6) and later	No	No	3.1(1) and later
usNIC Connection Policy	1.4(1a)	No	2.2(6) and later	No	No	3.1(1) and later
VMQ Connection Policy	1.4(1a)	No	2.2(6) and later	No	No	3.1(1) and later
Equipment Policies	1.4(1a)	No	2.2(7) and later	No	No	3.1(1) and later
Maintenance Policy on Next Reboot	1.4(1a)	No	2.2(8) and later	No	No	3.1(1) and later

Feature Support for Release 1.3 and earlier

Cisco UCS Central Features	Supported Cisco UCS Central Versions	Supported Cisco UCS Manager Versions				
		2.1	2.2	2.5	3.0	3.1
Multi-version management support and viewing supported Cisco UCS Manager features	1.1(2a)	No	2.2(1b) and later	2.5(1a) and later	3.0(1c) and later	3.1(1a) and later
Importing policy/policy component and resources		No	2.2(1b) and later	2.5(1a) and later	3.0(1c) and later	3.1(1a) and later
Specifying remote location for backup image files		No	2.2(2b) and later	2.5(1a) and later	3.0(1c) and later	3.1(1a) and later
3rd party certificate		No	2.2(2c) and later	2.5(1a) and later	3.0(1c) and later	3.1(1a) and later
IPv6 inband management support		No	2.2(2c) and later	2.5(1a) and later	3.0(1c) and later	3.1(1a) and later
Estimate Impact on Reconnect	1.2(1a)	No	2.2(3a) and later	2.5(1a) and later	3.0(1c) and later	3.1(1a) and later
Precision Boot Order Control		No	2.2(1b) and later	2.5(1a) and later	3.0(1c) and later	3.1(1a) and later
Scriptable vMedia	1.2(1e) and later	No	2.2(2c) and later	2.5(1a) and later	3.0(2c) and later	3.1(1a) 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.
- For precision boot order control, the blade server must have CIMC version 2.2(1b) or above.

Upgrade Paths

You can only upgrade Cisco UCS Central to release 1.4(1a) or 1.4(1b) from any of the following two releases:

- From 1.2 to 1.4(1a) or 1.4(1b)
- From 1.3 to 1.4(1a) or 1.4(1b)

Note For information about how to upgrade to previous releases of Cisco UCS Central, see the installation and upgrade guide for that release.

Known Limitations and Behaviors

The following known limitations and behaviors are not otherwise documented:

Defect ID	Symptom	Workaround
CSCus21388	In a cluster set up, when the RDM shared storage 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.

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

—	When using the Cisco 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.

Defect ID	Symptom	Workaround
CSCux75985 CSCuy07572	Excluding components from the host firmware package policy is supported in Cisco UCS Manager release 2.2.7 and above. When excluding components, you should be aware of the following: • The global-default host firmware package policy includes all components, but if you create a new custom host firmware package policy, the local disk component is automatically excluded. • Host firmware package policies created in Cisco UCS Central 1.3 or previous do not support excluding components. These policies are not changed when you upgrade to Cisco UCS Central release 1.4. • If you create your own custom host firmware package policy with excluded components, including the local disk component that is excluded by default, you cannot include that host firmware package policy in a service profile associated with a server running a Cisco UCS Manager version prior to 2.2.7. If you do, you will see the following error during service profile association: `ucs domain does not have the matching server capabilities for this service-profile`	If you have issues with your custom host firmware package policies that include excluded components, you can either remove all excluded components in the host firmware package policy, or upgrade your version of Cisco UCS Manager to release 2.2.7 or above.
CSCuz88005	Cisco UCS Manager release 2.2(7) and below supports 128 LDAP group maps, and release 2.2(8) and above supports 160 LDAP group maps. However, only 28 LDAP group maps can be pushed to Cisco UCS Manager from Cisco UCS Central release 1.4.	Create the LDAP group maps in Cisco UCS Manager.

Security Fixes

The following security fixes are resolved:

Release	Defect ID	CVE ID	Symptom
1.4(1a)	CSCuu68852	CVE-2015-4000	A vulnerability in OpenSSL has been addressed.
	CSCux33573	CVE-2015-6387	A vulnerability in the HTTP web based management interface has been addressed.
	CSCux33575	CVE-2015-6388	A vulnerability in SSRF protection has been addressed.
1.4(1b)	CSCux95108	CVE-2015-7973, CVE-2015-7974, CVE-2015-7975, CVE-2015-7976, CVE-2015-7977, CVE-2015-7978, CVE-2015-7979, CVE-2015-8138, CVE-2015-8139, CVE-2015-8140, CVE-2015-8158	A vulnerability in the network time protocol daemon (ntpd) has been addressed.
	CSCux41334	CVE-2015-3193, CVE-2015-3194, CVE-2015-3195, CVE-2015-3196, CVE-2015-1794	A vulnerability in OpenSSL has been addressed.
	CSCuy07297	CVE-2016-0701, CVE-2015-3197	A vulnerability in OpenSSL has been addressed.
	CSCuy91250	—	A vulnerability in the HTTP web-based management interface has been addressed.

Open and Resolved Caveats for Release 1.4(1a)

Open Caveats in Release 1.4(1a)

The following caveats are open in Release 1.4(1a):

Defect ID	Symptom	Workaround
CSCux44445	If you edit a boot policy and delete all of the existing local storage boot orders, then add another local storage boot order without saving, you may see the following error: `child [boot order name] can't be added to deleted object`	Save the local storage boot order before adding a new one.

Resolved Caveats in Release 1.4(1a)

The following caveats are resolved in Release 1.4(1a):

Defect ID	Symptom
CSCuu14611	Cisco UCS Central no longer displays an incorrect license state for registered Cisco UCS domains.
CSCuu18772	Cisco UCS Central now only allows one initial license to be configured.
CSCut04955	Direct-attached storage is now configurable in Cisco UCS Central.
CSCuv28064	If you modify the vHBA name for the primary or secondary SAN boot in a boot policy in Cisco UCS Central, the changes will now be reflected in Cisco UCS Manager.
CSCuw14379	Advanced host firmware policies are now available in Cisco UCS Central.
CSCuw45330	The 'rx-...-delta' and 'tx-...-delta' properties under the 'ether-if-stats' class in a threshold policy can now be set using the Cisco UCS Central CLI.
CSCuw67774	Host firmware packages can now only be created under Organizations, and no longer impact different sub-organizations and domains in Cisco UCS Central.
CSCuw68037	Sub-organizations that have been deleted in Cisco UCS Central are no longer visible in the Cisco UCS Central GUI.

Defect ID	Symptom
CSCuw73554	Cisco UCS Central now truncates runs cron.daily and logrotate scripts when the logs in the /var/log/messages and /var/log/ucsCentral_messages directories reach 100 MB.
CSCuw76011	Plain-text descriptions can now be added to global VLANs and VSANs in the Cisco UCS Central CLI.
CSCuw85224	Cisco UCS Central powershell scripts no longer display incorrect AdminVcon, Order, and vHBA information.
CSCux15438	Selecting a MAC pool during vNIC template creation no longer saves the incorrect MAC pool.
CSCut69263	Changing the NFS mount path on a Cisco UCS Central HA cluster no longer causes Cisco UCS Manager backups and firmware updates to fail.
CSCut75549	Modified global_default maintenance policies, boot policies, and local disk configuration policies are no longer reset to the factory default when Cisco UCS Central is restarted.
CSCut74984	After upgrade, the Cisco UCS Manager registration status no longer displays as 'Failed' in Cisco UCS Manager and 'Visible' in Cisco UCS Central.

Resolved Caveats for Release 1.4(1b)

Resolved Caveats in Release 1.4(1b)

The following caveats are resolved in Release 1.4(1b):

Defect ID	Symptom
CSCuy34188	Users with accounts provisioned on separate AAA servers are now able to save Cisco UCS Central dashboard preferences, even when multiple locales are assigned.
CSCuy02538	Creating an appliance port in Cisco UCS Central using the same ID as an appliance port in Cisco UCS Manager no longer overwrites the existing appliance port in Cisco UCS Manager.
CSCuy15529	The root filesystem will no longer reach 100% utilization after the syslog is rotated when it reaches 100MB in size.

Defect ID	Symptom
CSCux60035	Global service profiles containing a boot policy with iSCSI boot and auto target will no longer fail on association.
CSCuw84513	Cisco UCS Central fault F10000338 now displays the detected disk speed when the disk speed is under threshold.
CSCux54643	The hash values of the admin password and shared secret are no longer included in the **show tech-support** command output.
CSCux56137	Enabling or disabling ports after viewing port channels in the Cisco UCS Central GUI no longer impacts the port channels.
CSCux56721	The rack server count no longer fails to display correctly in the Cisco UCS Central GUI.
CSCuy13456	VLAN ID overlap is now checked when editing an existing VLAN.
CSCuy14299	When a trust point is deleted from Cisco UCS Central, the symbolic links are now deleted as well.
CSCuy14536	When upgrading to release 1.4, you will no longer receive a `backstore-cannot-be-resolved-from-pool-failure` error when you have a global service profile with a storage profile and an empty server pool.
CSCuy15555	The local syslog file size no longer exceeds the maximum defined limit of 100MB.
CSCuy27160	With VLAN ID overlap check, you can now create a VLAN with the same VLAN ID that was previous used and later modified to a different ID.
CSCuy35503	Associating global service profiles to Cisco UCS C220 M4 or C240 M4 servers no longer fails with a `server unavailable` error message.
CSCux72777	When using the Cisco UCS Central API, adding two native VLANs to a vNIC template will now return a failure.
CSCux71135	Non-XML characters in data received no longer causes inventory sync to fail.
CSCuy01951	Duplicate IDs are now correctly displayed when you create UUID pools.
CSCux97319	Deleted VLANs will no longer be available for selection when configuring unified uplink ports.
CSCux98827	The `auto-acknowledge` option has been removed from the firmware auto-sync policy (fw-autosync-policy).
CSCux99537	IQN configuration failure will now be cleared after changing IQN to none.

Resolved Caveats for Release 1.4(1c)

Resolved Caveats in Release 1.4(1c)

The following caveats are resolved in Release 1.4(1c):

Defect ID	Symptom
CSCuz11963	Any non-valid FSM-related faults in Cisco UCS Central release 1.3 are now automatically cleared when you upgrade to Cisco UCS Central release 1.4(1c).
CSCuz25412	Any faults received with the traditional licensing method, for example, grace period expired license warnings, are now automatically cleared when you enable Smart Licensing.
CSCuz97481	Servers are no longer rebooted when Cisco UCS Manager is upgraded to version 3.1(1h) after Cisco UCS Central is upgraded to 1.4(1c) and changes are made to an associated global service profile.
CSCuz92490	Connection policies are no longer removed when you edit a vNIC template using the HTML5 UI. This prevents an unnecessary server reboot.

Related Documentation

In addition to these release notes, you can find documentation for Cisco UCS Central in the following locations on Cisco.com:

- Cisco UCS Documentation Roadmap
- Cisco UCS Central Install and Upgrade Guides
- Cisco UCS Central Configuration Guides
- Cisco UCS Central Videos
- Cisco UCS Central CLI Reference Manual