Release Notes for Cisco UCS Central, Release 2.0

First Published: 2017-05-15

Last Modified: 2024-03-06

Introduction

Cisco UCS Central 2.0 provides a scalable management solution for a growing Cisco Unified Computing System (Cisco UCS) environment. Cisco UCS Central simplifies the management of multiple Cisco UCS domains from a single management point through standardization, global policies, and global ID pools. Cisco UCS Central focuses on managing and monitoring the UCS domains on a global level, across multiple individual Cisco UCS Classic and Mini management domains worldwide.

This document describes system requirements, new features, resolved caveats, known caveats, and open caveats with workarounds for Cisco UCS Central software release 2.0. 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
2.0(1a)	May 15, 2017	Created release notes for Cisco UCS Central Release 2.0 (1a).
	June 5, 2017	Added support for Cisco HyperFlex Systems.
2.0(1b)	August 18, 2017	Created release notes for Cisco UCS Central Release 2.0(1b).
	October 24, 2017	Updated support for BIOS tokens in M5 servers supported in release 2.0(1b).
2.0(1c)	November 15, 2017	Created release notes for Cisco UCS Central Release 2.0(1c).
	November 17, 2017	Updated supported version of Cisco UCS Manager for Globalization of Service Profiles.

Release	Date	Description
2.0(1d)	March 21, 2018	Created release notes for Cisco UCS Central Release 2.0(1d).
2.0(1e)	May 18, 2018	Created release notes for Cisco UCS Central Release 2.0(1e).
2.0(1f)	August 14, 2018	Created release notes for Cisco UCS Central Release 2.0(1f).
2.0(1g)	January 02, 2019	Created release notes for Cisco UCS Central Release 2.0(1g).
2.0(1h)	March 18, 2019	Created release notes for Cisco UCS Central Release 2.0(1h).
2.0(1i)	May 29, 2019	Created release notes for Cisco UCS Central Release 2.0(1i).
2.0(1j)	September 23, 2019	Created release notes for Cisco UCS Central Release 2.0(1j).
2.0(1k)	March 4, 2020	Created release notes for Cisco UCS Central Release 2.0(1k). Added Upgrade path from 2.0(1d) or 2.0(1e) Updated support for BIOS tokens in M5 servers supported in release 2.0(1k).
2.0(11)	August 13, 2020	Created release notes for Cisco UCS Central Release 2.0(1l).
2.0(1m)	December 18, 2020	Created release notes for Cisco UCS Central Release 2.0(1m).
2.0(1m)	March 17, 2021	Updated Feature Support Matrix for the UCS Manager supported version for release 2.0(1m).
2.0(1n)	April 30, 2021	Created release notes for Cisco UCS Central Release 2.0(1n).
2.0(1o)	July 2, 2021	Created release notes for Cisco UCS Central Release 2.0(1o).
2.0(1p)	December 16, 2021	Created release notes for Cisco UCS Central Release 2.0(1p).
2.0(1q)	July 19, 2022	Created release notes for Cisco UCS Central Release 2.0(1q).

Release	Date	Description
2.0(1q)	September 1, 2022	Added a note in the **Behavior Changes in Release 2.0(1q)** section.
2.0(1r)	February 6, 2023	Created release notes for Cisco UCS Central Release 2.0(1r).
	March 10, 2023	Updated the **Open Caveats in Release 2.0(1r)** section
2.0(1s)	May 4, 2023	Created release notes for Cisco UCS Central Release 2.0(1s).
2.0(1t)	October 5, 2023	Created release notes for Cisco UCS Central Release 2.0(1t).
2.0(1u)	March 6, 2024	Created release notes for Cisco UCS Central Release 2.0(1u).

Important Guidelines for Cisco 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 registered with a Cisco UCS Central IP address. For more information, see the **Changing a Cisco UCS Central IP Address** section in the Cisco UCS Central Installation and Upgrade Guide.
- Before you upgrade Cisco UCS Central, it is recommended that you do a full state backup and take a VM snapshot.
- 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 the **Cisco UCS Central Instance Migration** section 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 the **Cisco UCS Domains and Cisco UCS Central** section 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 policies remain local.

Important

- Cisco UCS Central does not support High Availability (HA) for new installations. Cisco recommends that you install Cisco UCS Central in Standalone mode in a single virtual machine, and leverage the High Availability capabilities of the Hypervisor.
- Upgrading Cisco UCS Central release 2.0(1d) or 2.0(1e) to 2.0(1k) could fail due to CSCvt12270. Cisco recommends that you first upgrade to Cisco UCS Central 2.0(1j) and then upgrade to 2.0(1k). For more information about this defect, see Open Caveats in Release 2.0(1k).

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

See Related Documentation, on page 37 on Cisco.com for current information on Cisco UCS Central.

System Requirements

Supported Browsers

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

- Windows
  - Microsoft Edge 106 and above
  - Internet Explorer 11 and above
  - Firefox 45.0.2 and above
  - Chrome 49 and above
- Linux RHEL
  - Firefox 45.0.2 and above
  - Chrome 49 and above
- MacOS
  - Firefox 45.0.2 and above
  - Chrome 49 and above
  - Safari 9.0.3 and above

Note Cisco UCS Central does not support browser full screen mode.

We recommend the below screen resolutions to launch the Cisco UCS Central GUI:

- 1920 x 1080
- 1600 x 900
- 1440 x 900
- 1360 x 768
- 1280 x 768
- 1280 x 720
- 1280 x 600

Supported Operating Systems

The released ISO is supported by the following:

- VMWare EXSi 7.0 and higher.

  See VMware Product Lifecycle wesbite at *https://lifecycle.vmware.com/#/*

- Microsoft Hyper-V Server 2016, Microsoft Hyper-V Server 2019
- KVM Hypervisor on Red Hat Enterprise Linux 7.2, 7.3 and 7.4

The released OVA is supported by VMWare ESXi 7.0 and higher.

Support for Transport Layer Security

Support for TLS 1.1 and 1.2

Cisco UCS Central 2.0 supports TLS1.1 and TLS1.2 HTTPS connection.

Support for Cisco HyperFlex Systems

Cisco UCS Central only supports inventory and monitoring of Cisco HyperFlex server nodes connected to a Cisco UCS Fabric Interconnect running a supported version of Cisco UCS Manager. The Cisco HX Data Platform Installer OVA currently creates and manages all required policy and service profiles locally via Cisco UCS Manager APIs and does not support global policies and service profiles. The Globalization feature of Cisco UCS Central 2.0 is not supported for Cisco HyperFlex Systems. Cisco recommends that you do not manually configure global service profiles and policies in Cisco UCS Central for Cisco HyperFlex as the upgrade functionality and procedures that are part of the Cisco HX Data Platform Installer will not work with any custom global configuration manually created through Cisco UCS Central.

Changes in Cisco UCS Central, Release 2.0

New Features in Cisco UCS Central Release 2.0

Cisco UCS Central 2.0 supports new features listed in the sections in this topic. Some of these features are built in Cisco UCS Central to be compatible with Cisco UCS Manager release 3.1(3) and later. For more information about the appropriate supported Cisco UCS Manager releases, see Feature Support Matrix, on page 14.

Feature	Function
Support for Cisco UCS 5th Gen FI (UCS-FI-6536)	The Cisco 6536 Fabric Interconnects provide both network connectivity and management capabilities for the system. The Cisco 6536 offer line-rate, low-latency, lossless 10/25/40/100 Gigabit Ethernet, Fibre Channel over Ethernet (FCoE), and Fibre Channel functions.
Support for IOE Controller	Supports a second RAID Controller in the IO Expander on Cisco UCS S3260 Storage Server (UCS-C3K-M4RAID).
Support for HBA Controller	Supports Dual HBA Controllers on Cisco UCS S3260 Storage Server (UCS-S3260-DHBA).
BIOS Asset Tag	Service profiles now display an Asset Tag to uniquely identify servers.
Globalization of Service Profiles	Allows you to globalize Local Service Profiles from Cisco UCS Manager intoCisco UCS Central to deploy and use Cisco UCS Central in a legacy software environment.
Integrated Server Diagnostics	Enables you to verify the health of hardware components on your servers and provides various tests to stress and exercise the hardware subsystems, such as memory and CPU, on the servers.
Lightweight Upgrades/ Hot Patching	Delivers Cisco UCS Manager firmware security updates for infrastructure and server components through service pack bundles.
Set KVM IP on Physical servers	Allows you to configure KVM IP s on physical servers for Inband and Outband management.
SED Management, KMIP Support	Introduces security policies for Self-Encrypting Drives (SEDs) for management of data encryption. The security keys required to encrypt the media encryption key can be configured locally, or remotely using the KMIP server.
Smart SSD	Supports monitoring SSD health and provides statistics about various SSD properties, and a threshold limit for each property.
User-defined FC Zoning	Allows you to create an FC Zone profile to group all zoning needs for a VM to represent a single data replication solution between storage arrays.
Fabric Evacuation in Firmware Auto Install	Supports automatic configuration of Fabric Evacuation during an FI upgrade and reboot during AutoInstall, and ensures that the appropriate failover settings are configured for the firmware upgrade.

Feature	Function
Launch HTML5 KVM Client	Launches the HTML5 based KVM client directly from the Cisco UCS Central GUI.
New Policies	The following new policies are introduced in Cisco UCS Central 2.0: • Multicast Policy with IGMP Snooping • Power Sync Policy • Statistics Threshold Policy • Graphics Card Policy • QoS System Class • Hardware Change Discovery Policy • Port Auto-Discovery Policy • KMIP Certification Policy
Server Reboot Log	Displays a server reboot log with the last five reasons for the reset, along with the time and source of power transition.
Cisco UCS Manager DirectView tabs	Launches DirectView of Cisco UCS Manager Server Statistics tabs from 2.0 to view details of CIMC Sessions, System Event Logs, VIF paths, Statistics, Temperatures, Power, and Installed Firmware.
UI enhancements	Introduces the following UI enhancements: • Spotlight search bar to enable a comprehensive search for objects by their names. Top 10 results and suggested entries are displayed. • Restore Tabs to save open tabs and enable direct access to the same session when you log back in to Cisco UCS Central. • Favorites widget on the widgets menu bar to save your most used components, tabs, and dialogs for creating or editing policies. • Clone Policies icon to enable deep cloning a policy with a new name, parent organization or domain group, and description if applicable, in order to help you make minor edits without having to create a new policy.

Behavior Changes in Release 2.0(1u)

Cisco UCS Central 2.0(1u) has added support for the following:

- Support for the 5th Gen Intel® Xeon® Scalable Processors with Cisco UCS X210c M7, C220 M7 and C240 M7 servers
- Support for the following Cisco UCS VIC adapters:
  - Cisco UCS VIC 15427

    - Cisco UCS VIC 15237
    - Cisco UCS VIC 15230

- New policies added under root domain and sub-domain:
    - Power Save Policy
    - Cisco UCS X9508 Chassis Power Extended Mode Policy
    - Cisco UCS X9508 Chassis Fan Control Policy

- Under sub-domain, the **Power Allocation** and **Profile power** options are replaced with the **Power Cap Management** option.

Behavior Changes in Release 2.0(1t)

Cisco UCS Central 2.0(1t) supports the following:

- Support for the following Cisco UCS C-series servers:
    - Cisco UCS C220 M7 Server
    - Cisco UCS C240 M7 Server

- Support for Cisco UCSX-9508 Chassis
- Support for the following Cisco UCS X-Series servers with Cisco UCSX-9508 Chassis:
    - Cisco UCS X210c M6 Compute Node
    - Cisco UCS X210c M7 Compute Node
    - Cisco UCS X410c M7 Compute Node

- Support for the following Intelligent Fabric Modules with Cisco UCS X-Series Servers:
    - UCSX-I-9108-25G
    - UCSX-I-9108-100G

- Support for the following UCS VIC cards:
    - Cisco UCS VIC 15420
    - Cisco UCS VIC 15422
    - Cisco UCS VIC 15425
    - Cisco UCS VIC 15231
    - Cisco UCS VIC 15235
    - Cisco UCS VIC 14425
    - Cisco UCS VIC 14825

- N+2 Power Redundancy to satisfy non-redundancy plus two additional power supplies for redundancy. Only Cisco UCS X9508 chassis supports N+2 redundancy mode.

Behavior Changes in Release 2.0(1s)

No new hardware has been qualified in the Cisco UCS Central 2.0(1s) release.

Behavior Changes in Release 2.0(1r)

Cisco UCS Central 2.0(1r) supports the following hardware:

- Cisco UCS 5th Gen FI (UCS-FI-6536)
- Cisco UCS VIC 15411 – 4 x 10G mLOM adapter on Cisco UCS B-series M6 servers
- Cisco UCS VIC 15238 – 2 x 40G/100G/200G mLOM adapter on Cisco UCS C-series M6 rack servers

Behavior Changes in Release 2.0(1q)

Note For a seamless download of the Firmware Image Packages under the Image library, it is highly recommended that you upgrade to the Cisco UCS Central 2.0(1q) release.

Cisco UCS Central 2.0(1q) supports the following hardware:

- Support for Cisco UCS VIC 1440+PE with Cisco UCS 6300/6400 fabric interconnects and 22xx series IOMs.
- Support of Cisco UCS VIC 15428 MLOM 4-port adapter on Cisco UCS C-series M6 rack servers.

Note Release 2.0(1r) supports Cisco UCS 5th Gen FI (UCS-FI-6536).

Note Release 2.0(1q) does not support Cisco UCS 5th Gen FI (UCS-FI-6536).

- QSFP-40/100-SRBD Network Interface Card at 40G on Cisco VIC 1300 and 1400.
- Intel X710T4LG 4x10 GbE RJ45 PCIe NIC (Carlsville ASIC) with Cisco UCS C220 M6, C240 M6, C225 M6, and C245 M6 servers.
- Qlogic QLE 2772 Fibre Channel Adapter with Cisco UCS C125 M5 servers.
- Qlogic QLE 2772 or QLE 2742 Fibre Channel Adapter with Cisco UCS S3260 servers.
- QLogic QLE2772 2x32GFC Gen 6 Enhanced PCIe HBA) with Cisco UCS C225 M6 and C245 M6 servers.
- MLNX MCX623106AS-CDAT, 2x100 GbE QSFP56 PCIe (non-Crypto/TLS) with Cisco UCS C225 M6 and C245 M6 servers.
- UCSC-P-B7D32GF (Cisco-Emulex LPe35002-M2-2x32GFC Gen 7 PCIe HBA)

Behavior Changes in Release 2.0(1p)

Cisco UCS Central 2.0(1p) supports the following hardware:

- **Cisco UCS C245 M6** —The Cisco UCS C245 M6 contains one or two AMD EPYC CPUs with up to 64 cores per socket. It also comes with 32 DIMM slots with a network speed of 3200 MHX DDR4, providing up to 8 TB of capacity. You can install up to 28 small-form factor (SFF) front-loading hot-pluggable drives.

Behavior Changes in Release 2.0(1o)

Cisco UCS Central 2.0(1o) supports the following hardware:

- **Cisco UCS B200 M6 Server**—The Cisco UCS B200 M6 Server is a half-width blade server that is designed for the Cisco UCS 5108 Blade Server Chassis. You can install up to eight UCS B200 M6 blade servers in a UCS 5108 chassis, mixing with other models of Cisco UCS blade servers in the chassis, as required.
- **Cisco UCS C220 M6 Server**—The Cisco UCS C220 M6 Server is a one-rack unit server that can be used as standalone, or as part of Cisco UCS, which unifies computing, networking, management, virtualization, and storage access into a single integrated architecture.
- **Cisco UCS C240 M6 Server**—The Cisco UCS C240 M6 Server is a 2 rack-unit, rack server chassis that can operate in both standalone environments and as part of Cisco UCS. Cisco UCS C240 M6 Servers support a maximum of two 3rd Gen Intel® Xeon® Scalable Processors, in either one or two CPU configurations.

Behavior Changes in Release 2.0(1l)

Cisco UCS Central 2.0(1l) supports the following hardware:

- **Cisco UCS C240 SD M5 Rack Server**—The new UCS C240 SD M5 is a purpose-built server aimed to address the use cases such as edge computing in space-constrained environments. This 2RU server has been redesigned to a 22” (55.9 cm) chassis-depth and enables fully front-accessible peripherals, including PCIe slots, drives and mLOM slots.
- **CSCvv10016**—Cisco UCS Central 2.0(1l) supports additional BIOS tokens that are supported by Cisco UCS Manager release 4.1(2a).

Behavior Changes in Release 2.0(1k)

Cisco UCS Central 2.0(1k) supports the following hardware:

- **High density Fourth Generation Fabric Interconnect**—The Cisco UCS 64108 Fabric Interconnect is a core part of the Cisco Unified Computing System, providing both network connectivity and management capabilities for the system. Cisco UCS 64108 Fabric Interconnects support 96 10/25-Gbps ports, 16 10/25-Gbps unified ports, and 12 40/100-Gbps uplink ports.
- Cisco UCS Central 2.0(1k) supports additional BIOS tokens that are supported by Cisco UCS Manager release 4.1(1a). For a complete and up to date list of all supported BIOS tokens, defaults, and their values, see the UCS Server BIOS Tokens guide.

Behavior Changes in Release 2.0(1j)

- Cisco UCS Central now supports 100 locales.

Behavior Changes in Release 2.0(1i)

- Cisco UCS Central does not allow changing the initial power state of a global service profile or a service profile template. The initial power state will not be pushed to Cisco UCS Manager as part of the Service profile association. However, you can continue to perform normal power operations on the servers as before. This behavior change is introduced as a fix for the defect CSCvp40200. For more information on the resolved Caveats in Cisco UCS Central 2.0(1i), see Resolved Caveats in Release 2.0(1i), on page 28.
- Cisco UCS Central 2.0(1i) supports additional BIOS tokens that are supported by Cisco UCS Manager release 4.0(4a). For a complete and up to date list of all supported BIOS tokens, defaults, and their values, see the UCS Server BIOS Tokens guide.
- You will no longer be able to download the Hardware Compatibility Catalog stored in *https:// ucshclserver.cloudapps.cisco.com/ fetch/ current.tar.gz* from Cisco.com. Cisco recommends that you run the following command to download the HCL catalog and then import it into Cisco UCS Central from the UI.

Attention Before you run the command, ensure that you have internet connectivity.

```
curl -k -f --connect-timeout 30 --dump-header "hcl_download_header" -o current.tar.gz
https://ucshclserver.cloudapps.cisco.com/fetch/current.tar.gz -u CCOusername:CCOPassword'
```

Behavior Changes in Release 2.0(1g)

- Cisco UCS Central 2.0(1g) supports Cisco UCS C 480 ML M5 Servers.
- Cisco UCS Central does not support High Availability for new installations.

Behavior Changes in Release 2.0(1f)

Cisco UCS Central 2.0(1f) supports the following hardware:

- Cisco UCS 6454 Fabric Interconnects
- Cisco UCS VIC 1400 series adapter cards on Cisco UCS M5 servers
- New SIOC and Cisco UCS VIC 1400 adapter cards with S3260 storage servers

Cisco UCS Central 2.0(1f) supports BIOS tokens for Cisco UCS Manager release 4.0(1a). For a complete, and up to date list of supported BIOS tokens, defaults, and values, see M5 Server BIOS Tokens in the Cisco UCS M5 Server BIOS Tokens guide.

Note Cisco UCS Central does not support Cisco UCS C-125 M5 Servers.

Behavior Changes in Release 2.0(1d)

Cisco UCS Central 2.0(1d) supports additional BIOS tokens for Cisco UCS S3260M5 servers that are supported by Cisco UCS Manager release 3.2(3). For a complete, and up to date list of supported BIOS tokens, defaults, and values, see M5 Server BIOS Tokens in Release 3.2(3) in the Cisco UCS M5 Server BIOS Tokens guide.

The following table lists the Cisco UCS Central and Cisco UCS Manager releases that support the BIOS tokens in the M5 server models:

Table 1: Supported M5 Server Models

Cisco UCS Central Release	Cisco UCS Manager Release	Server Models
2.0(1d)	3.2(3)	S3260 M5 B200 M5 B480 M5 C220 M5 C240 M5 C480 M5

Behavior Changes in Release 2.0(1c)

Cisco UCS Central 2.0(1c) supports additional BIOS tokens for Cisco UCS B480M5 and C480M5 servers that are supported by Cisco UCS Manager release 3.2(2). For a complete, and up to date list of supported BIOS tokens, defaults, and values, see M5 Server BIOS Tokens in Release 3.2(2) in the Cisco UCS M5 Server BIOS Tokens guide.

The table below lists the Cisco UCS Central and Cisco UCS Manager releases that support the BIOS tokens in the M5 server models:

Table 2: Supported M5 Server Models

Cisco UCS Central Release	Cisco UCS Manager Release	Server Models
2.0(1c)	3.2(2)	B200 M5 B480 M5 C220 M5 C240 M5 C480 M5

Behavior Changes in Release 2.0(1b)

Cisco UCS Central 2.0(1b) extends support for the new BIOS tokens for Cisco UCS B200M5, C220M5, and C240M5 servers that are supported by Cisco UCS Manager release 3.2(1). For a complete, and up to date list of supported BIOS tokens, defaults, and values, see M5 Server BIOS Tokens in Release 3.2(1) in the Cisco UCS M5 Server BIOS Tokens guide.

The **Reboot on BIOS Settings Change** property in the BIOS Policy is set to **Disabled** by default after an upgrade to Cisco UCS Central 2.0(1b). As a best practice, Cisco recommends that you retain this default setting.

The table below lists the Cisco UCS Central and Cisco UCS Manager releases that support the BIOS tokens in the M5 server models:

Table 3: Supported M5 Server Models

Cisco UCS Central Release	Cisco UCS Manager Release	Server Models
2.0(1b)	3.2(1)	B200 M5 C220 M5 C240 M5

Behavior Changes in Release 2.0

Deprecation Announcements

- Cisco UCS Central no longer includes the Flex-based UI. The HTML5 UI is the only graphical interface available.
- The Statistics Management feature is deprecated and is no longer supported in Cisco UCS Central.
- 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.

Feature Support

Behavior Changes Based on Design

- The Spotlight search bar replaces the search bar, and allows you to search for profiles, policies, pools, VLANs/VSANs, templates, domains, orgs, domain groups etc by their names, descriptions, and labels. Spotlight auto-completes the search field with suggestions as you type and displays the top 10 potential matches to the term you type.
- Icons in the Sidebar navigation menu enable direct and easy access to all objects in Cisco UCS Central. Browse tables, Organization navigation, and Domain group navigation are now part of Sidebar navigation.
- From the Organizations tree view, you can directly navigate to that org's Profiles, Templates, Pools, Policies, and Permitted VLANs. The corresponding tab in the selected org is highlighted and opened when you click these objects.
- Cisco UCS Central 2.0 prevents you from deleting critical objects such as service profiles, domain groups, organizations, and service profile templates from the Cisco UCS Central GUI and the command line. When you attempt to delete any of these items from Cisco UCS Central, an error message with the potential impact displays.
- You must create the global service profile template before you can create a service profile.
- 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.
- Only the configuration export (all-config) and backup (full-state) options are used in Cisco UCS Central. Other backup types such as config logical and config system are not supported.

Feature Support Matrix

The following table lists the compatible versions of Cisco UCS Central and Cisco UCS Manager.

Cisco UCS Central	Supported Versions of Cisco UCS Manager
2.0(1u)	2.2, 3.1, 3.2, 4.0, 4.1 up to 4.1(3), 4.2 up to 4.2(3), 4.3(2), 4.3(3)
2.0(1t)	2.2, 3.1, 3.2, 4.0, 4.1 up to 4.1(3), 4.2 up to 4.2(3), 4.3(2)
2.0(1s)	2.2, 3.1, 3.2, 4.0, 4.1 up to 4.1(3), 4.2 up to 4.2(3)
2.0(1r)	2.1, 2.2, 3.0, 3.1, 3.2, 4.0, 4.1 up to 4.1(3), 4.2 up to 4.2(3)
2.0(1q)	2.1, 2.2, 3.0, 3.1, 3.2, 4.0, 4.1 up to 4.1(3), 4.2(1), 4.2(2)
2.0(1p)	2.1, 2.2, 3.0, 3.1, 3.2, 4.0, 4.1 up to 4.1(3), 4.2(1)
2.0(1o)	2.1, 2.2, 3.0, 3.1, 3.2, 4.0, 4.1 up to 4.1(3), 4.2(1)
2.0(1n)	2.1, 2.2, 3.0, 3.1, 3.2, 4.0, 4.1 up to 4.1(3)
2.0(1m)	2.1, 2.2, 3.0, 3.1, 3.2, 4.0, 4.1 up to 4.1(3)
2.0(1l)	2.1, 2.2, 3.0, 3.1, 3.2, 4.0, 4.1 up to 4.1(2)
2.0(1k)	2.1, 2.2, 3.0, 3.1, 3.2, 4.0, 4.1 up to 4.1(1)
2.0(1j)	2.1, 2.2, 3.0, 3.1, 3.2, and 4.0 up to 4.0(4)
2.0(1i)	2.1, 2.2, 3.0, 3.1, 3.2, and 4.0 up to 4.0(4)
2.0(1h)	2.1, 2.2, 3.0, 3.1, 3.2, and 4.0 up to 4.0(2)
2.0(1g)	2.1, 2.2, 3.0, 3.1, 3.2, and 4.0 up to 4.0(2)
2.0(1f)	2.1, 2.2, 3.0, 3.1, 3.2, and 4.0(1)
2.0(1e)	2.1, 2.2, 3.0, 3.1, and 3.2
2.0(1d)	2.1, 2.2, 3.0, 3.1, and 3.2
2.0(1c)	2.1, 2.2, 3.0, 3.1, and 3.2 up to 3.2(2)
2.0(1b)	2.1, 2.2, 3.0, 3.1, and 3.2(1)
2.0(1a)	2.1, 2.2, 3.0, and 3.1
1.5	2.1, 2.2, 3.0, 3.1 up to 3.1(2)

Cisco UCS Central	Supported Versions of Cisco UCS Manager
1.4	2.1, 2.2 up to 2.2(8), 3.0, 3.1 up to 3.1(1)
1.3	2.1, 2.2 up to 2.2(6)

The following table provides a list of specific features in Cisco UCS Central, and the 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 2.0

Cisco UCS Central Features	Supported Cisco UCS Central Versions	Supported Cisco UCS Manager Versions			
		2.1	2.2	3.0	3.1 /3.2/4.0
Support for Second RAID Controller in the IO Expander on Cisco UCS S3260 Storage Server (UCS-C3K-M4RAID)	2.0(1a)	No	No	No	3.1(3) and later
Support for Dual HBA Controller on Cisco UCS S3260 Storage Server (UCS-S3260-DHBA)	2.0(1a)	No	No	No	3.1(3) and later
Support for Dual SIOC	2.0(1a)	No	No	No	3.1(3) and later
Globalization of Service Profiles	2.0(1a)	No	2.2(8f)	No	3.1(2) and later
BIOS Asset Tag	2.0(1a)	No	No	No	3.1(3) and later
Hot patching/ Lightweight Upgrades	2.0(1a)	No	No	No	3.1(3) and later
User-Defined Zone Profiles	2.0(1a)	No	No	No	3.1(3) and later
Integrated Server Diagnostics	2.0(1a)	No	No	No	3.1(3) and later

Cisco UCS Central Features	Supported Cisco UCS Central Versions	Supported Cisco UCS Manager Versions			
		2.1	2.2	3.0	3.1 /3.2/4.0
SED Security Policies, Smart SSD, and KMIP Support	2.0(1a)	No	No	No	3.1(3) and later
Automatic Configuration of FI-Server Ports	2.0(1a)	No	No	No	3.1(3) and later
Set KVM IP on physical servers	2.0(1a)	No	No	No	3.1(3) and later
Fabric Evacuation in Firmware Auto Install	2.0(1a)	No	No	No	3.1(3) and later
Direct Fabric Interconnect Evacuation	2.0(1a)	No	2.2(4) and later	No	3.1(1) and later
Launch HTML5 KVM Client	2.0(1a)	No	No	No	3.1(3) and later
Multicast Policy	2.0(1a)	No	No	No	3.1(3) and later
Power Sync Policy	2.0(1a)	No	2.2(8)	No	3.1(2) and later
Statistics Threshold Policy	2.0(1a)	No	No	No	3.1(3) and later
Graphics Card Policy	2.0(1a)	No	No	No	3.1(3) and later
QoS System Class	2.0(1a)	No	No	No	3.1(3) and later
Hardware Change Discovery Policy	2.0(1a)	No	No	No	3.1(3) and later
Port Auto-Discovery Policy	2.0(1a)	No	No	No	3.1(3) and later
KMIP Certification Policy	2.0(1a)	No	No	No	3.1(3) and later
Server Reboot Logs	2.0(1a)	No	No	No	3.1(3) and later
Delete Decommissioned Rack Server, Chassis, FEX	2.0(1a)	Yes	Yes	No	3.1(1) and later

Cisco UCS Central Features	Supported Cisco UCS Central Versions	Supported Cisco UCS Manager Versions			
		2.1	2.2	3.0	3.1 /3.2/4.0
VLAN Group	2.0(1b)	No	No	No	3.1(2) and later

Feature Support for Release 1.5

Cisco UCS Central Features	Supported Cisco UCS Central Versions	Supported Cisco UCS Manager Versions			
		2.1	2.2	3.0	3.1
Cisco UCS S3260 Storage Server support	1.5(1a)	No	No	No	3.1(2) and later
vNIC/vHBA pairing	1.5(1a)	No	2.2(7) and later	No	3.1(2) and later
Traffic monitoring	1.5(1a)	No	2.2(7) and later	No	3.1(1) and later
UUID sync	1.5(1a)	No	2.2(7) and later	No	3.1(2) and later
Admin host port for PCI placement	1.5(1a)	No	No	No	3.1(1e) and later
Support for 160 LDAP group maps	1.5(1a)	No	2.2(8) and later	No	3.1(2) and later

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

Cisco UCS Central Features	Supported Cisco UCS Central Versions	Supported Cisco UCS Manager Versions				
		2.1	2.2	2.5	3.0	3.1
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	No	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 upgrade Cisco UCS Central to release 2.0 from any of the following releases:

- From 1.4 to 2.0

- From 1.5 to 2.0
- If you want to upgrade Cisco UCS Central from release 2.0(1d) or 2.0(1e) to 2.0(1m), you must first upgrade to release 2.0(1l) and then to 2.0(1m).

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
CSCwj08579	In Cisco UCS X9508 Chassis, Power Extended Policy does not get pushed to IFM when the policy value is modified from Cisco UCS Central. This issue occurs when the Policy Extended Policy Resolution control is Global and the updated value of the policy is displayed in Cisco UCS Manager GUI.	Change the Power Extended Policy Resolution control to Local and update the values from Cisco UCS Manager.
CSCwf75644	The background image does not load properly in the Cisco UCS Central GUI for Microsoft Internet Explorer browser. A white background is displayed as the background image.	The background image loads properly in the Cisco UCS Central GUI login page for other web browsers. Microsoft Edge browser can be used for Windows OS.
CSCwh32835	When a Cisco UCS X-series chassis is connected to the domain, the fan details of IFM modules for X-series chassis are not displayed in Cisco Central GUI Chassis page.	You can view the fan details for IFM using Cisco UCS Central CLI.

CSCuy37428
CSCuv32055
	When registering a Cisco UCS domain immediately after installation, you may see one of the following issues:
	• After installing Cisco UCS Central on RHEL 7.2 KVM, domain registration fails.
	• 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`

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 1.5. • 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.

Security Fixes

The following security fixes are resolved:

Release	Defect ID	CVE ID	Symptom
2.0(1r)	CSCwd59106	CVE-2021-44228	Removal of older version of Log4j in SOLR component.
2.0(1q)	CSCwa33066	CVE-2021-40438	Evaluation of ucs-cloud for vulnerabilities resolved in Apache httpd 2.4.49
	CSCwa54646	CVE-2021-45105	Evaluation of ucs-central for Log4j 2.x DoS vulnerability fixed in 2.17 and 2.17.1

Release	Defect ID	CVE ID	Symptom
2.0(1p)	CSCwa47303	CVE-2021-44228	Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021
2.0(1m)	CSCvw35850	N/A	API null digest authorization issue in Cisco UCS Central release 2.0(1j) has been addressed and fixed.
2.0(1l)	CSCvt27767	CVE-2020-1938	The Apache Tomcat vulnerability in Cisco UCS Central has been addressed and fixed.
2.0(1k)	CSCvq70837	CVE-2017-1000486	Primefaces vulnerabilities in Cisco UCS Central have been addressed and fixed.
2.0(1j)	CSCvp38294	CVE-2015-0228, CVE-2015-0253, CVE-2015-3183, CVE-2015-3185, CVE-2016-0736, CVE-2016-2161, CVE-2016-5387, CVE-2016-8740, CVE-2016-8743, CVE-2017-15710, CVE-2017-15715, CVE-2017-3167, CVE-2017-3169, CVE-2017-7659, CVE-2017-7668, CVE-2017-7679, CVE-2018-0113, CVE-2018-1283, CVE-2018-1301, CVE-2018-1302, CVE-2018-1303, CVE-2018-1312, CVE-2018-1333, CVE-2018-8011	Apache vulnerabilities in Cisco UCS Central have been addressed and fixed.
2.0(1h)	CSCm91751	CVE-2016-2107	Open SSL Oracle padding vulnerability in Cisco UCS Central has been addressed and fixed.

Release	Defect ID	CVE ID	Symptom
2.0(1f)	CSCvh74209	CVE-2015-5600, CVE-2015-6563, CVE-2015-6564, CVE-2016-10009, CVE-2016-10010, CVE-2016-10011, CVE-2016-10012, CVE-2016-8858, CVE-2016-3115, CVE-2007-6750	Open SSH and Apache HTTP Server Vulnerabilities in Cisco UCS Central have been addressed and fixed.
2.0(1d)	CSCvg47507	CVE-2017-1000100, CVE-2017-1000254, CVE-2017-1000257, CVE-2017-7407	Multiple **curl** vulnerabilities have been addressed.
	CSCvf85637	Weak SSH Ciphers in Cisco UCS Central	Cisco UCS Central has now disabled weak SSH ciphers for all versions.
	CSCvh62085	Spectre and Meltdown vulnerabilities	Spectre and Meltdown-related vulnerabilities have been addressed and fixed.
2.0(1c)	CSCvf71978	Cisco UCS Central Cross-Site Scripting vulnerability	A vulnerability in Cisco UCS Central Cross-Site Scripting has been addressed.
	CSCvf71986	Cisco UCS Central Session Fixation vulnerability	A Session Fixation vulnerability in Cisco UCS Central has been addressed.
	CSCvf85660	Cisco UCS Central Apache weak cipher vulnerabilities	Cisco UCS Central now supports SHA2 for default signed certificate.

Release	Defect ID	CVE ID	Symptom
2.0(1a)	CSCvb48578	CVE-2016-6304 CVE-2016-6305 CVE-2016-2183 CVE-2016-6303 CVE-2016-6302 CVE-2016-2182 CVE-2016-2180 CVE-2016-2177 CVE-2016-2178 CVE-2016-2179 CVE-2016-2181 CVE-2016-6306 CVE-2016-6307 CVE-2016-6308 CVE-2016-6309 CVE-2016-7052	A vulnerability in OpenSSL and the TLS protocol has been addressed.
	CSCvc90364	CVE-2016-0736 CVE-2016-2161 CVE-2016-5387 CVE-2016-8740 CVE-2016-8743	A vulnerability in remote web server has been addressed.
	CSCvb85545	CVE-2016-5195	DIRTY CoW vulnerability has been addressed.
	CSCvc23477 CSCvd72180	Evaluation of Cisco UCS Central for NTP November 2016 and March 2017	Vulnerabilities in NTP server have been addressed.

Resolved Caveats

Resolved Caveats in Release 2.0(1u)

The following caveats have been resolved in Cisco UCS Central release 2.0(1u):

Defect ID	Description
CSCwi33551	Unable to edit multiple options in the power policy in the sub-domain in the Web UI. The configuration changes fails with an exception.

Resolved Caveats in Release 2.0(1t)

The following caveats have been resolved in Cisco UCS Central release 2.0(1t):

Defect ID	Description
CSCwf96008	The domain group is deleted successfully from the Web UI. However, the deleted domain group appears in the Web UI as a major fault after deletion. **Note** This issue occurs in Cisco UCS Central 2.0(1r) and 2.0.(1s) as well.

Resolved Caveats in Release 2.0(1s)

The following caveats have been resolved in Cisco UCS Central release 2.0(1s):

Defect ID	Description
CSCwe74020	Unable to launch Avocent KVM for Cisco UCS B-series M5 Servers through UCS Central for releases up to 4.2(1).
CSCwd52410	FC aggregate ports were not displayed accurately for 5th Gen FI in UCS Central; Ports were displayed as Scalability port 0/1 to 0/4 instead of 31/1 to 31/4.
CSCwd66816	Kickstart file missing from the UCS 6332 Fabric Interconnects Infrastructure Software Bundle imported to UCS Central causing the Fabric Interconnects upgrade failure through UCS Central.
CSCwe91955	Unable to launch Avocent KVM for Cisco UCS S3260 M5 server through UCS Central for releases 4.2(2) and later.
CSCwe18667	Cisco UCS C-series M6 servers unable to upgrade BIOS firmware through Global Host Firmware Package Policy from UCS Central due to the failure to extract the UCS M6 BIOS images.
CSCwd03694	vSAN names and IDs check validation have been added in UCS Central to avoid any overlaps or duplicates across SAN or Storage.
CSCwe23344	Maximum Data LUNs Per Target has been increased from [1-1024] to [1-4096] for FC adapter policies in UCS Central. Note: This capability is supported only for UCS Manager releases 4.2(3d) and later.

Resolved Caveats in Release 2.0(1r)

The following caveats are resolved in Cisco UCS Central release 2.0(1r):

Defect ID	Description
CSCwd24159	Unable to set the **Power Profiling** option through UCS Central for certain Cisco UCS B200 M6 server having configurations with high-end CPU and 32 DIMMS. The **Power Profiling** option is mandatory to be able to power on the blades.

Defect ID	Description
CSCwc80714	In Cisco UCS Central 2.01(g), when you assign a Cisco UCS Manager domain to a domain group and remove it, you might not be able to access Cisco UCS Central GUI. From **pmon** state, **resource-mgr** is displayed as failed.

Resolved Caveats in Release 2.0(1q)

The following caveats are resolved in Cisco UCS Central release 2.0(1q):

Release	Description
CSCwa19412	Cisco UCS Central now supports ASD v4 version.
CSCwa68949	Cisco UCS Central supports the download for firmware packages larger than 2 GB.
CSCwb32036	Smart License registration for Cisco UCS Central with Cisco Smart Software Licensing Manager portal no longer fails due to CA certificate changes.

Resolved Caveats in Release 2.0(1p)

The following caveats are resolved in Cisco UCS Central release 2.0(1p):

Release	Description	
CSCwa47303	Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021	
CSCvz56004	After upgrading a blade to the 4.2(1d)B, HTML KVM does not launch.	
CSCvy86072	A vulnerability in OpenSSH could allow an unauthenticated, remote attacker to access sensitive information on a targeted system.	
CSCvz44944	When changing a domain IP for domains registered for Fully Qualified Domain Name (FQDN), duplicate domains incorrectly display.	

Resolved Caveats in Release 2.0(1o)

The following caveats are resolved in Cisco UCS Central release 2.0(1o):

Release	Description
CSCvy67473	Existing UCS Central images that you download from Cisco CCO for installation now work properly. Previously, the images did not run properly because of errors associated with an unavailable locator service.

Resolved Caveats in Release 2.0(1n)

The following caveats are resolved in Cisco UCS Central release 2.0(1n):

Release	Description
CSCvw18010	BIOS policies are now displayed correctly in the Cisco UCS Central. As a result, the BIOS values can be edited from the interface.
CSCvx18078	A VMMQ policy can now be configured from Cisco UCS Central and pushed to the UCS Manager as part of the Service Profile configuration. .

Resolved Caveats in Release 2.0(1m)

The following caveats are resolved in Cisco UCS Central release 2.0(1m):

Release	Description
CSCvv60698	GENEVE encapsulation acceleration option in the Ethernet Adapter Policy is now enabled in Cisco UCS Central.
CSCvs41517	NVMe option for UEFI boot policy is now supported in Cisco UCS Central.
CSCvw38152	Cisco UCS Central 2.0(1m) supports additional BIOS tokens that are supported by Cisco UCS Manager release 4.1(3a).

Resolved Caveats in Release 2.0(1l)

The following caveats are resolved in Cisco UCS Central release 2.0(1l):

Release	Description
CSCvt45036	VSAN globalization fails with the following error, "Wait for Globalization".
CSCvt12270	Upgrade from Cisco UCS Central release 2.0(1d) or 2.0(1e) to release 2.0(1k) could fail due to boot partition getting full.
CSCvu44028	After an upgrade to Cisco UCS Central release 2.0(1k), UI displays memory RAS Settings as "platform default" although the CLI displays the right information.
CSCvt00346	A DME crash may occur when the ucsCentral_messages log file exceeds the limit.

Resolved Caveats in Release 2.0(1k)

The following caveats are resolved in Cisco UCS Central release 2.0(1jk):

Release	Description
CSCvr02845	Cisco UCS Central can now successfully download firmware bundles of the Cisco UCS 6454 and 64108 Fabric Interconnects.
CSCvr09400	The Cisco UCS 6454 ports 49-54 can now be configured as Network Uplink or FCoE uplink ports from Cisco UCS Central.

Release	Description
CSCvr56397	Disk Group Policy now supports values 253 and 254 for Disk Slot IDs to configure RAID1 for UCS M.2-HWRAID from Cisco UCS Central.

Resolved Caveats in Release 2.0(1j)

The following caveats are resolved in Cisco UCS Central release 2.0(1j):

Release	Description
CSCvp76562	Infrastructure firmware upgrade profiles can now be created for 4GFI in Cisco UCS Central and infra upgrade can be successfully completed.
CSCvp47201	The downloaded infrastructure firmware packages are now uniquely named to avoid name conflict among platform bundles. The infra firmware upgrade process in Cisco UCS Central now picks up the images based on the appropriate platform.
CSCvq94753	Restore using SCP/SFTP in Cisco UCS Central is fixed.

Resolved Caveats in Release 2.0(1i)

The following caveats are resolved in Cisco UCS Central release 2.0(1i):

Release	Description
CSCvo21755	Cisco UCS Central no longer has a high memory consumption across processes with SNMP polling.
CSCvp13960	You can simultaneously apply a server pool and a vMedia policy to a global service profile in Cisco UCS Central 2.0(x).
CSCvp21297	VLANs added to a VLAN group in Cisco UCS Central 2.0(1d) and 2.0(1h) no longer get deleted when they are pushed to Cisco UCS Manager.
CSCvp40200	Servers associated with Cisco UCS Central 2.0 no longer reload unexpectedly triggered by **hard-reset**.

Resolved Caveats in Release 2.0(1h)

The following caveats are resolved in Cisco UCS Central release 2.0(1h):

Release	Description
CSCvm81056	VLAN Group is no longer deleted from the uplink port-channel when a new VLAN is added to an existing VLAN group, or when the same VLAN is added to a vNIC template with Cisco UCS Central 2.0(1d).
CSCvo45661	VSANs with FCOE ID 4011 and 4012 can now be created from Cisco UCS Central 2.0(1g) on the following: • Cisco UCS 6332 Fabric Interconnect running Cisco UCS Manager 4.0(2b) • Cisco UCS 6248 Fabric Interconnect running Cisco UCS Manager3.2(3i)

Release	Description
CSCvo62782	Configuring Cisco.com credentials with Cisco UCS Central GUI no longer fails. The credentials can now be saved.

Resolved Caveats in Release 2.0(1g)

The following caveats are resolved in Cisco UCS Central release 2.0(1g):

Release	Description
CSCvm81311	Cisco UCS Manager Data Management Engine (DME) no longer crashes due to mismatched `adminvCon` values passed by Cisco UCS Centralfor dynamic and static vNICs.
CSCvd51108	Cisco UCS Central virtual machine no longer becomes unresponsive due to growing SNMP Memory consumption upon persistent polling.

Resolved Caveats in Release 2.0(1f)

The following caveats are resolved in Cisco UCS Central release 2.0(1f):

Release	Description
CSCvk12385	`svc_server_DME` logs no longer observe memory leaks due to faults in Cisco UCS Manager.
CSCvi75816	Unassociated Global Service Profile (GSP) no longer prevents a Cisco UCS domain move to a new domain group.
CSCvi85023	Fault F10000035 (fltStorageItemCapacityWarning - For Disk Usage for /boot Partition exceeding 90%) no longer appears during an upgrade to Cisco UCS Central 2.0(1d) from any of the previous versions.
CSCvi86491	Renaming a service profile in Cisco UCS Central no longer causes the configuration settings to revert to the original template settings.
CSCvj12410	UEFI Boot parameters for the M.2 controller are now available in Cisco UCS Central.
CSCvk06781	Option to disable VLAN Port Count Optimization for non-root domain groups is now available in Cisco UCS Central.
CSCvk38338	Fault F14533382 is no longer raised when QOS System Class policy is applied.
CSCvd39239	Cisco UCS Central can now clear Stale/Orphaned Faults that are related to domain registration.

Resolved Caveats in Release 2.0(1e)

The following caveats are resolved in Cisco UCS Central release 2.0(1e):

Release	Description
CSCvj44960	Cisco UCS Central no longer causes the servers to reboot when Inband profile is configured for the UCS domain, and the domain FIs are restarted.

Resolved Caveats in Release 2.0(1d)

The following caveats are resolved in Cisco UCS Central release 2.0(1d):

Defect ID	Symptom
CSCvg81832	Cisco UCS Central now launches the HTML5 KVM for Cisco UCS C-Series Rack Servers.
CSCvh05008	You can now create an IP Pool under a domain group from the Cisco UCS Central GUI.
CSCvh11135	Cisco UCS Central no longer hangs, and functions normally in a large-scale deployment.
CSCvg91479	Spotlight search on Cisco UCS Central now works for users with multiple locales.
CSCvh88028	LDAP users using CLI do not get password expiry errors during log-in.
CSCvi32682	Estimate impact upon activating Cisco UCS Central subscription on a UCS domain no longer times out.
CSCvi05444	Cisco UCS Central Spotlight search displays correct ownership for service profiles.

Resolved Caveats in Release 2.0(1c)

The following caveats are resolved in Cisco UCS Central release 2.0(1c):

Defect ID	Symptom
CSCvf 37185	Cisco UCS Central SNMP Managed Information Base (MIB) library now loads in Cisco UCS Central 2.0, and the snmpwalk on Cisco UCS Central specific MIB does not fail.
CSCve51309	Outband IP on the server now gets assigned when you select **Reapply Configuration** in **Domain Settings.**
CSCve88234	The Cisco UCS Central spotlight search now displays results for Local Service Profiles.
CSCvg48615	Cisco UCS Central now supports more BIOS tokens that are supported in Cisco UCS Manager, Release 3.2(2b).
CSCvf64818	Call Home alerts that are part of Call Home monitoring do not stay in the **Enabled** status anymore after you disable them through Cisco UCS Central Release 1.5 or 2.0.
CSCvf83421	After a VLAN change, **Estimate Impact** in Cisco UCS CentralHTML GUI does not display **Server needs reboot** status anymore.

Defect ID	Symptom
CSCvf84627	Cisco UCS Central no longer shows Faults F11000491 and F10017451 while using an Inband KVM IP in the Domain Profile.
CSCvf57811	Global Service Profiles in Cisco UCS Central 1.5(1b) no longer move to **Ungrouped** state after un-associating from a Blade or Rack server on occasion.
CSCvg11782	Globalization of Service Profiles no longer fails in Cisco UCS Central 2.0(1a), when rack servers are present in the server pool.
CSCve31096	Globalization of Service Profiles no longer fails in Cisco UCS Central 2.0(1a), due to VLAN permission issues.

Resolved Caveats in Release 2.0(1b)

The following caveats are resolved in Cisco UCS Central release 2.0(1b):

Defect ID	Symptom
CSCvf22068	The **User Label** option is now available on a global service profile derived from updating a template, on the Cisco UCS Central HTML5 GUI.
CSCvf16476	You can now activate virtual media when you launch the KVM console from a global service profile.
CSCve25720	VLAN membership now gets updated in Cisco UCS Manager when using VLAN groups.
CSCve39559	Global Chassis Profile association no longer fails when Storage Controller is selected as an Exclude Component in a global Chassis Firmware Pack.
CSCve70783	Arbitrary files in Cisco UCS Central can no longer be accessed by an authenticated local user.

Resolved Caveats in Release 2.0

The following caveats are resolved in Cisco UCS Central release 2.0(1a):

Defect ID	Symptom
CSCva84992	Httpd cores caused by invalid cookie no longer occur intermittently in Cisco UCS Central(1a).
CSCvb02359	SNMPD no longer crashes periodically after an upgrade from Cisco UCS Central 1.3 or earlier versions to version 1.4 or higher. This issue was caused due to log files getting filled up after the upgrade.
CSCvb05938	UCS Central Certificate Request now handles Organization (O) and Organization Unit (OU) Name fields correctly.
CSCvb26696	Policy reference related faults now get cleaned up in Cisco UCS Central Resource Manager.

Defect ID	Symptom
CSCvb38828	All Call Home settings can now be pushed down from *root* in Cisco UCS Central. You can go back to *root* settings after you make a change in the domain group.
CSCvb41775	Stale VLAN entry from Cisco UCS Central release 1.4(a) no longer exists after deleting the VLAN.
CSCvb46833	Suspended Cisco UCS domain can now be re-acknowledged and moved out of that state after an upgrade from Cisco UCS Central version 1.3(1a) to 1.5(1a). Cisco UCS Central no longer displays *No email is configured for profiles* while the Call Home policies are pushed down to the Cisco UCS domain.
CSCvb66577	Cisco UCS Central now displays a **Warning** message when you move domains from a domain group to another.
CSCvb76019	Unresolved VLAN name no longer exists in service profile templates in Cisco UCS Central release 1.4.
CSCvb81404	Domain Group syslog file size issues no longer exist in Cisco UCS Central 1.4.c.
CSCvb88419	VLANs are no longer missing from Port Channel configuration after an upgrade from Cisco UCS Central release 1.4b to release 1.5(1a).
CSCvc03633	Duplicate entries generated after Service Registry crash no longer exist in the *chassisversionholder.txt* file.
CSCvc34656	Remote operations on the LUNs under Global Service Profile definition no longer fail in Cisco UCS Central.
CSCvc42518	Cisco UCS Central policy names now match the policy names in Cisco UCS Manager.
CSCvc44482	Cisco UCS Central UI no longer shows incorrect Fabric ID for iSCSI vNICs on the service profiles.
CSCvc46131	HDD without Out of band capabilities no longer shows operability as **Not-supported**. It now displays **N/A**.
CSCvc64224	IP addresses in private scope no longer show as available when using IP pools with overlapping range.
CSCvc74991	Critical Fault with vNIC/vHBA Redundancy Pairs and using Global Server Pools no longer occurs in Cisco UCS Central.
CSCvc92353	Cisco UCS Central fails to download backup files to local desktop using PowerTools.
CSCvd01775	Cisco UCS Manager no longer runs a pretended upgrade when upgrade is done from Cisco UCS Central when the image is not available.
CSCvd13002	*Missing IPv4 Address* message can now be cleared from Cisco UCS Central.
CSCvd19031	Cisco UCS Central SFTP backup on-demand or schedule no longer fails.

Defect ID	Symptom
CSCvd60762	An outage of servers no longer occurs following a change to power policy in a service profile.
CSCvd72684	LDAP configuration on Cisco UCS Central is now pushed completely from Cisco UCS Central to lower-level Cisco UCS domains.
CSCvd91971	Primary vNIC in a redundancy pair now initially pushes VMQ Connection policies to Cisco UCS Manager.

Open Caveats

Open Caveats in Release 2.0(1t)

The following caveat is open in the Cisco UCS Central release 2.0(1t):

Defect ID	Symptom	Workaround
CSCwh70811	When the domain is registered to Cisco UCS Central and configuration import is triggered, the status is shown as **Work In Progress**, even after configuration import is completed.	The configuration import must be done from Cisco UCS Manager. The import status must be checked from Cisco UCS Manager.

Open Caveats in Release 2.0(1s)

The following caveat is open in the Cisco UCS Central release 2.0(1s):

Defect ID	Symptom	Workaround
CSCwe92425	**Schedule Domain Export** not working through UCS Central for local and remote copy with UCS Manager release 4.2(2) and above.	Set the **Backup and Export** policy to local and trigger the config backup from UCS Manager.

Open Caveats in Release 2.0(1r)

The following caveats are open in Cisco UCS Central release 2.0(1r):

Defect ID	Symptom	Workaround
CSCwd52410	When Cisco UCS-FI-6536 is registered to Cisco UCS Central and FC breakout ports are configured in Cisco UCS Manager, the FC aggregate ports in Cisco UCS Central display the value as 0. This is because FC breakout is not supported in Cisco UCS Central 2.0.1(r) release. In Cisco UCS Manager, if the port 33 is configured as FC breakout port, then in Cisco UCS Central, the FC breakout port displays the following values: 0/1, 0/2, 0/3 and 0/4 Actual values that the FC breakout port must display in Cisco UCS Central: 33/1, 33/2, 33/3, 33/4	There are no known workarounds.
CSCwe21986	FC breakout for Cisco UCS-FI-6536 is not supported in Cisco UCS Central 2.0.1(r) release. So, the FC breakout ports for Cisco UCS-FI-6536 cannot be configured in Cisco UCS Central.	The FC breakout ports must be configured and monitored from Cisco UCS Manager.

Defect ID	Symptom	Workaround
CSCwd66816	After importing Cisco UCS firmware bundle to Cisco UCS Central, few files do not appear in the **Images** tab in the Cisco UCS Central GUI. Logs also confirm that there are missing files, irrespective of the imported firmware bundle version. You can also confirm this by checking the bundles from the library in Cisco UCS Central. Example: While importing Cisco UCS `A` bundle, Cisco UCS Central might display the following files: • `ucs-2200-6300.4.1.3g.bin` • `ucs-2300-6300.4.1.3g.bin` • `ucs-6300-ucs-manager-k9.4.1.3h.bin` • `ucs-6300-k9-system.5.0.3.N2.4.13g.bin` The missing file: `ucs-6300-k9-kickstart.5.0.3.N2.4.12b.bin` This issue occurs while using Cisco UCS Central to upgrade the Cisco UCS Manager domain.	Upgrade manually using Cisco UCS Manager.
CSCwe18667	Cisco UCS M6 servers unable to upgrade BIOS firmware when using a global Host Firmware Package from Cisco UCS Central. This issue is first seen in Cisco UCS Central 2.0(1p) and 2.0(1q) releases. This issue occurs when Cisco UCS B-series or C-series package is uploaded to Cisco UCS Central. And Cisco UCS Central fails to extract the Cisco UCS M6 BIOS image. This issue occurs when either the package uploaded is from a local file or downloaded from Cisco.com.	• Upload the Cisco UCS B-series or C-series 4.2(x) bundle directly to Cisco UCS Manager. • Create a new global Host Firmware Package in UCS Central and apply it to the server.

Open Caveats in Release 2.0(1p)

The following caveats are open in Cisco UCS Central release 2.0(1p):

Defect ID	Symptom	Workaround
CSCwa19415	UCS supports the latest BiosTokens.	

Open Caveats in Release 2.0(1k)

The following caveats are open in Cisco UCS Central release 2.0(1k):

Defect ID	Symptom	Workaround
CSCvt12270	Upgrade from Cisco UCS Central release 2.0(1d) or 2.0(1e) to release 2.0(1k) could fail due to boot partition getting full.	If you are upgrading to Cisco UCS Central 2.0(1k), you must first upgrade to Cisco UCS Central 2.0(1j) and then to 2.0(1k). If you are upgrading to Cisco UCS Central 2.0(1l) or later, you can upgrade directly without any intermediate upgrade.

Open Caveats in Release 2.0(1g)

The following caveats are open in Cisco UCS Central release 2.0(1g):

Defect ID	Symptom	Workaround
CSCvm81056	VLAN Group is deleted from the uplink port-channel when a new VLAN is added to an existing VLAN group or added the same VLAN to a vNIC template with Cisco UCS Central 2.0(1d).	Add the VLAN Group back to the uplink port-channel.

Open Caveats in Release 2.0

The following caveats are open in Cisco UCS Central release 2.0:

Defect ID	Symptom	Workaround
CSCvk21902	Upgrade from Cisco UCS Central 2.x to any other higher version fails with an **unknown exception** error.	From the console, select **Guest** > **Send Control+Alt+Delete** to reboot the VM. Once the reboot is complete, the upgrade request is reinitiated and completed.
CSCvm81311	Cisco UCS Manager Data Management Engine (DME) crashes due to mismatched `adminVcon` values passed by Cisco UCS Central for dynamic and static vNICs.	None

Defect ID	Symptom	Workaround
CSCvi33069	Cisco UCS Central fails to download firmware into the image library when uppercase characters are used for the Cisco Connection Online (CCO) account username.	Use lowercase characters for the CCO account username.
CSCve19522	Cisco UCS Domains in release 3.1(3a) moves to Lost Visibility status and fails to recover to the correct registration state.	Restart pmon on the Cisco UCS domain(s) from the Cisco UCS Manager CLI. **local mgmt # pmon stop** **local mgmt# pmon start** This defect is resolved in Cisco UCS Manager release 3.2(1a).
CSCve15708	In a Cisco UCS domain with 3.1(3a) firmware, registering Cisco UCS Manager to UCS Central using an IPv6 address fails with the following FSM error message: `Unable to resolve the UCS Central hostname. Please check the DNS entries.`	Downgrade to Cisco UCS Manager release 3.1(2). This defect is resolved in Cisco UCS Manager release 3.2(1a).
CSCvd47047	Creating Host Firmware Package Policy from different versions of Blade and Rack servers is successful from Cisco UCS Central, but fails in Cisco UCS Manager. This is due to Cisco UCS Central support for mixed versions of Blade and Rack servers for Cisco UCS Manager versions 3.1(1) and earlier.	Configure same versions of B and C bundles in the Host Firmware Package policy, if applied to Cisco UCS domain running Cisco UCS Manager version 3.1(2) or later.
CSCuz65590	If you change a WWXN pool to a static ID on an associated global service profile, Cisco UCS Manager will assign IDs to the vHBAs that are different from the IDs in Cisco UCS Central.	Assign new IDs to the vHBAs in Cisco UCS Central.
CSCve02287	Cisco UCS Central completes installation without a warning about inadequate system resources when you perform a fresh install using an *iso* image.	Check the System Requirements before you initiate the installation process.

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
- Cisco UCS Central Best Practices and Operations