Release Notes for Cisco UCS Central, Release 2.1

First Published: 2025-05-12

Last Modified: 2025-09-04

Introduction

Cisco UCS Central 2.1(1a) 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 2.1(1a). 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
2.1(1a)	May 12, 2025	Created release notes for Cisco UCS Central Release 2.1 (1a).
	June 17, 2025	Updated the following sections: • Behavior Changes in Release 2.1(1a) • Feature Support Matrix
	August 12, 2025	Updated the following section: Open Caveats in Release 2.1(1a)
2.1(1b)	July 28, 2025	Updated the following sections: • Behavior Changes in Release 2.1(1b) • Feature Support Matrix • Upgrade Paths
	August 12, 2025	Updated the following section: Open Caveats in Release 2.1(1b)

Release	Date	Description
2.1(1c)	August 13, 2025	Updated the following sections: • Feature Support Matrix • Resolved Caveats in Release 2.1(1c)
	September 4, 2025	Updated the following sections: • Feature Support Matrix • Behavior Changes in Release 2.1(1c) • Upgrade Paths • Open Caveats in Release 2.1(1c)

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 Getting Started Guide for Cisco UCS Central, Release 2.1.
- 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 Getting Started 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 Getting Started 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.

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 21 on Cisco.com for current information on Cisco UCS Central.

System Requirements

Supported Browsers

We recommend using the most recent version of one of the following supported browsers for Windows, Linux RHEL, and MacOS:

- Microsoft Edge
- Mozilla Firefox
- Google Chrome
- Apple Safari

Note The browser page refresh rate has been adjusted to an auto-trigger mode with a maximum interval of 1 minute, moving away from an event-based trigger. This means you may need to wait for a short period for the browser to refresh and display updated data automatically.

To address GUI malfunctions, clearing the browser cache is recommended.

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 ESXi 7.x, ESXi 8.0 and later

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

- Microsoft Hyper-V Server 2022, Microsoft Hyper-V Server 2025, and later
- KVM Hypervisor on Red Hat Enterprise Linux 8.7 and later

The released OVA is supported by VMware ESXi 7.x, ESXi 8.0 and later.

Support for Transport Layer Security

Support for TLS 1.2 and TLS 1.3

Cisco UCS Central 2.1(1a) supports TLS 1.2 and TLS 1.3 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 2.1(1a) 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 2.1

Behavior Changes in Release 2.1(1c)

Cisco UCS Central 2.1(1c) has added support for the following:

- Cisco UCS 6664 Fabric Interconnect—The Cisco UCS 6664 Fabric Interconnect is a 2-rack unit (RU), fixed-port system designed for Top-of-Rack deployment in data centers. The fabric interconnect has both Ethernet and unified ports. Unified ports provide Fibre Channel over Ethernet (FCoE), Fibre Channel, NVMe over Fabric, and Ethernet. By supporting these different protocols, you can use a single multi-protocol Virtual Interface Card (VIC) in your servers.

  The Cisco UCS 6664 Fabric Interconnect supports an array of Gigabit Ethernet (GbE), Fibre Channel (FC), and Fibre Channel over Ethernet (FCoE) ports to offer connectivity to peer data center devices. This device is also ideal for high-performance, scalable, and secure networking in modern data centers.
- Support for UCSX-X10C-PTE3 Pass Controller on Cisco UCS X215c M8 Compute Node.
- Cisco UCS X-Series Direct (Fabric Interconnect 9108 100G) now supports Cisco UCS C-Series rack servers, enabling unified management of both UCS X-Series compute nodes and C-Series servers in one domain. It also adds secondary chassis support, allowing deployment of a second UCS X9508 chassis and up to 20 servers in a single X-Direct domain. These enhancements improve scalability and simplify data center hardware management. This is applicable through CLI only for release 2.1(1c).

Behavior Changes in Release 2.1(1b)

Deprecation Announcements

- Deprecation of Smart Licensing through Smart Call Home. Cisco Smart Transport is now used as the default method for Smart Licensing communication with the Cisco Smart Software Manager (CSSM) server.
- Deprecation of Online help file launch as PDF.

  Cisco UCS Central Help is now directly accessible as an integrated HTML help system.

Behavior Changes in Release 2.1(1a)

Cisco UCS Central 2.1(1a) has added support for the following:

- Single Root I/O Virtualization (SR-IOV) support.
- Operating system and security upgrades.
- Upgrading Cisco UCS Central using CLI.
- OVA installation is now supported only through vCenter.
- The GRUB menu includes options for Reset Password, Reboot, and Reinstall.
- An online PDF version launches, replacing the HTML help format.
- Cisco UCS Central 2.1 will be compatible with Cisco UCS Manager versions 4.1.3 and later.

  For more information, see Feature Support Matrix.
- Cisco UCS Central supports the following hardware:
  - Cisco UCS C220 M8 Server
  - Cisco UCS C240 M8 Server
  - Cisco UCS X210c M8 Compute Node

Deprecation Announcements

- Depreciation of PAK licenses.

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
2.1(1c)	4.1(3), 4.2 up to 4.2(3), 4.3(2), 4.3(3), 4.3(4), 4.3(5), 4.3(6), 6.0(1)
2.1(1b)	4.1(3), 4.2 up to 4.2(3), 4.3(2), 4.3(3), 4.3(4), 4.3(5), 4.3(6)
2.1(1a)	4.1(3), 4.2 up to 4.2(3), 4.3(2), 4.3(3), 4.3(4), 4.3(5), 4.3(6)
2.0(1w)	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), 4.3(4), 4.3(5), 4.3(6)
2.0(1v)	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), 4.3(4), 4.3(5)
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

Cisco UCS Central	Supported Versions of Cisco UCS Manager
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)
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 2.1 (1a)

For details on the supported UCS Manager features in Cisco UCS Central 2.1(1a), see Cisco UCS Manager Release Notes.

Cisco UCS Central Features	Supported Cisco UCS Manager Versions
SR-IOV support	4.3(2b)
Password Encryption Key to enhance security for backup configuration files.	4.2(3d)
UCS Manager supports TLS 1.3	4.2(3o)
BIOS tokens to improve RAS memory setting for UCS M5 servers	4.1(3a)
Support for Cisco UCS X215c M8 Compute Node	4.3(5a)
Support for Cisco UCS C225 M8 Server	4.3(5a)
Support for Cisco UCS C245 M8 Rack Server	4.3(4b)
Support for Cisco UCS X-Series Direct	4.3(4b)
Support for Tri-Mode 24G SAS RAID Controller	4.3(4a)
Support for Cisco UCSX-440P PCIe Node	4.3(4a)
Support for Cisco UCS X410c M7	4.3(2c)
Support for Cisco UCSX-9508 Chassis	4.3(2b)

Cisco UCS Central Features	Supported Cisco UCS Manager Versions
Support for Cisco UCS X210c M7	4.3(2b)
Support for Cisco UCS X210c M6	4.3(2b)
Support for Cisco UCS 9108 25G IFMs	4.3(2b)
Support for Cisco UCS 9108 100G IFMs	4.3(2b)
Support for Cisco UCS C220 M7 Server	4.3(2b)
Support for Cisco UCS C240 M7 Server	4.3(2b)

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

Upgrading Cisco UCS Central 2.1

You can upgrade Cisco UCS Central 2.1 to any other later release through ISO only:

Base Version	Upgradable Version	Upgrade Mode
2.1(1a)	2.1(1b) and later	CLI
2.1(1b)	2.1(1c) and later	CLI

For 2.1(1c)

- You can directly upgrade from Cisco UCS Central release 2.1(1a) and 2.1(1b) to Cisco UCS Central release 2.1(1c).
- Backup restoration to Cisco UCS Central Release 2.1(1c) is supported from Cisco UCS Central release version 2.0(1s) and later.

For information on the behavior changes introduced in Release 2.1(1c), refer to the Changes in Cisco UCS Central, Release 2.1(1c) section.

For 2.1(1b)

- You can directly upgrade from Cisco UCS Central release 2.1(1a) to Cisco UCS Central release 2.1(1b).
- The ISO upgrade is applicable starting from Cisco UCS Central release 2.1(1b), ensuring compatibility and support for systems running this version and later.
- Backup restoration to Cisco UCS Central Release 2.1(1b) is supported from Cisco UCS Central release version 2.0(1s) and later.

For information on the behavior changes introduced in Release 2.1(1b), refer to the Changes in Cisco UCS Central, Release 2.1(1b) section.

For 2.1(1a)

- There is no direct upgrade path supported to Cisco UCS Central release 2.1(1a) from earlier releases.
- Backup restoration to Cisco UCS Central Release 2.1(1a) is supported from version 2.0(1s) and later.

Note For information about how to upgrade from previous releases of Cisco UCS Central, see the Cisco UCS Central Getting Started Guide, Release 2.1.

For information on the behavior changes introduced in Release 2.1(1a), refer to the Changes in Cisco UCS Central, Release 2.1(1a) section. For details on hardware compatibility in Release 2.1, see compatible Cisco UCS Manager Release Notes.

Known Limitations and Behaviors Release 2.1

Known Limitations and Behaviors in Release 2.1(1c)

The Cisco UCS 6664 Fabric Interconnect infrastructure firmware cannot be added through the Cisco UCS Central GUI or CLI.

Known Limitations and Behaviors in Release 2.1(1b)

There are no known behavior and limitations in Release 2.1(1b).

Known Limitations and Behaviors in Release 2.1(1a)

There are no known behavior and limitations in Release 2.1(1a).

Security Fixes

The following security fixes are resolved:

Release	Defect ID	CVE ID	Symptom
2.1(1a)	CSCwe78970	CVE-2014-0050, CVE-2013-0248, CVE-2014-0050, CVE-2016-1000031, CVE-2016-3092, CVE-2023-24998	Critical CVE in component commons-file upload. Upgrade to latest version.
2.1(1a)	CSCwf28668	CVE-2018-15473, CVE-2021-41617, CVE-2007-2768, CVE-2008-3844, CVE-2010-4478, CVE-2012-0814, CVE-2014-2653, CVE-2015-5352, CVE-2015-5600,CVE-2015-6563, CVE-2015-6564, CVE-2016-0777, CVE-2016-0778, CVE-2016-10009, CVE-2016-10010, CVE-2016-10011, CVE-2016-10012, CVE-2016-10708, CVE-2016-1908, CVE-2016-3115, CVE-2016-6210, CVE-2017-15906, CVE-2018-15473, CVE-2018-15919, CVE-2018-20685, CVE-2019-16905, CVE-2019-6109, CVE-2019-6110, CVE-2019-6111, CVE-2020-14145, CVE-2021-28041, CVE-2021-41617	Critical CVE in component openssh. Upgrade to latest version.

Release	Defect ID	CVE ID	Symptom
2.1(1a)	CSCwf62171	CVE-2015-0235, CVE-2012-3406, CVE-2012-4412, CVE-2012-4424, CVE-2012-6656, CVE-2013-1914, CVE-2013-2207, CVE-2013-4237, CVE-2013-4332, CVE-2013-4458, CVE-2013-4788, CVE-2013-7423, CVE-2013-7424, CVE-2014-0475, CVE-2014-4043, CVE-2014-5119, CVE-2014-6040, CVE-2014-8121, CVE-2014-9402, CVE-2014-9761, CVE-2014-9984, CVE-2015-1472, CVE-2015-1473, CVE-2015-1781, CVE-2015-5180, CVE-2015-5277, CVE-2015-7547, CVE-2015-8776, CVE-2015-8777, CVE-2015-8778, CVE-2015-8779, CVE-2015-8982, CVE-2015-8983, CVE-2015-8984, CVE-2015-8985, CVE-2016-10228, CVE-2016-10739, CVE-2016-1234, CVE-2016-3075, CVE-2016-3706, CVE-2016-4429, CVE-2016-5417, CVE-2016-6323, CVE-2017-1000366, CVE-2017-12132, CVE-2017-12133, CVE-2017-15670, CVE-2017-15671, CVE-2017-15804, CVE-2018-1000001, CVE-2018-11236, CVE-2018-11237, CVE-2018-19591, CVE-2018-20796, CVE-2018-6485, CVE-2019-25013, CVE-2019-6488, CVE-2019-7309, CVE-2019-9169, CVE-2020-10029, CVE-2020-1751, CVE-2020-1752, CVE-2020-27618, CVE-2020-29573, CVE-2020-6096, CVE-2021-3326, CVE-2021-35942, CVE-2021-38604, CVE-2021-3999, CVE-2022-23218, CVE-2022-23219	Critical CVE in component glibc. Upgrade to latest version.
2.1(1a)	CSCwf97383	CVE-2017-8779, CVE-2018-14622, CVE-2021-46828	Critical CVE in component libtirpc. Upgrade to latest version.
2.1(1a)	CSCwf97385	CVE-2010-2061, CVE-2010-2064, CVE-2017-8779	Critical CVE in component rpcbind. Upgrade to latest version.
2.1(1a)	CSCwk79854	CVE-2023-48795, CVE-2023-48795	UCS Central
2.1(1a)	CSCwj22476	CVE-2020-9484, CVE-2020-11996, CVE-2016-5425	Mandatory upgrade of high-risk tomcat component.

Release	Defect ID	CVE ID	Symptom
2.1(1a)	CSCwd29488	CVE-2020-2754,CVE-2020-2755,CVE-2020-2756, CVE-2020-2757,CVE-2020-2767,CVE-2020-2773, CVE-2020-2778,CVE-2020-2781, CVE-2020-2800,CVE-2020-2803,CVE-2020-2805,CVE-2020-2816, CVE-2020-2830,CVE-2021-2161,CVE-2021-2163,CVE-2022-21248, CVE-2022-21282,CVE-2022-21283,CVE-2022-21293,CVE-2022-21294, CVE-2022-21296,CVE-2022-21299,CVE-2022-21305, CVE-2022-21340,CVE-2022-21341,CVE-2022-21349,CVE-2022-21360, CVE-2022-21365,CVE-2022-21426,CVE-2022-21434,CVE-2022-21443, CVE-2022-21476, CVE-2022-21496,CVE-2022-21540,CVE-2022-21541, CVE-2022-34169	Vulnerabilities in openjdk 1.8.0u121.
2.1(1a)	CSCwj22465	CVE-2020-11984, CVE-2021-26691, CVE-2021-44790, CVE-2022-22720, CVE-2022-23943, CVE-2022-31813, CVE-2023-25690, CVE-2024-38474, CVE-2024-38476, CVE-2022-22721, CVE-2022-28615, CVE-2022-36760, CVE-2021-44224, CVE-2006-20001, CVE-2019-10081, CVE-2019-9517, CVE-2020-11993, CVE-2020-9490, CVE-2021-26690, CVE-2022-22719, CVE-2022-26377, CVE-2022-29404, CVE-2022-30556, CVE-2023-27522, CVE-2023-31122, CVE-2023-38709, CVE-2024-24795, CVE-2024-27316, CVE-2024-38472, CVE-2024-38477, CVE-2024-40898, CVE-2020-1927, CVE-2023-45802, CVE-2019-10082, CVE-2019-10098, CVE-2019-17567, CVE-2020-1934, CVE-2021-30641, CVE-2022-28330, CVE-2022-28614, CVE-2022-37436, CVE-2019-10092	Mandatory upgrade of high-risk apache-http-server component
2.1(1a)	CSCwj22471	CVE-2018-16839, CVE-2018-16840, CVE-2019-5481, CVE-2019-5443, CVE-2019-5436, CVE-2018-1000300, CVE-2019-5482, CVE-2019-15601, CVE-2021-3450, CVE-2021-3449, CVE-2018-1000301, CVE-2018-16842, CVE-2018-0500, CVE-2019-1547, CVE-2019-1551, CVE-2019-1552, CVE-2019-1559, CVE-2019-1563, CVE-2020-1968, CVE-2020-1971, CVE-2021-23840, CVE-2021-23841, CVE-2021-3711, CVE-2021-3712, CVE-2021-4160, CVE-2022-0778, CVE-2022-1292, CVE-2022-2068	Mandatory upgrade of high-risk openssl component
2.1(1a)	CSCwf28668	CVE-2007-2768, CVE-2008-3844, CVE-2010-4478, CVE-2012-0814,CVE-2014-2653, CVE-2015-5352, CVE-2015-5600, CVE-2015-6563, CVE-2015-6564, CVE-2016-0777, CVE-2016-0778, CVE-2016-10009, CVE-2016-10010, CVE-2016-10011, CVE-2016-10012, CVE-2016-10708, CVE-2016-1908, CVE-2016-3115, CVE-2016-6210, CVE-2017-15906, CVE-2018-15473,CVE-2018-15919, CVE-2018-20685, CVE-2019-16905, CVE-2019-6109,CVE-2019-6110, CVE-2019-6111, CVE-2020-14145, CVE-2021-28041, CVE-2021-41617	Critical CVE in component openssh. Upgrade to the latest version.

Release	Defect ID	CVE ID	Symptom
2.1(1a)	CSCwf97384	CVE-2013-5211, CVE-2015-7705, CVE-2015-7850, CVE-2015-7976, CVE-2015-8158, CVE-2016-1549 , CVE-2016-2518, CVE-2016-4954, CVE-2016-4955, CVE-2016-4956, CVE-2016-7426, CVE-2016-7429, CVE-2016-7433, CVE-2016-9310, CVE-2016-9311, CVE-2017-6462, CVE-2017-6463, CVE-2017-6464, CVE-2018-7170, CVE-2018-7185, CVE-2019-11331, CVE-2020-11868, CVE-2020-13817	Critical CVE in component ntp. Upgrade to the latest version.
2.1(1a)	CSCwj22473	CVE-2017-1000486	Mandatory upgrade of high-risk primefaces component.

Resolved Caveats

Resolved Caveats in Release 2.1(1c)

The following caveats have been resolved in Cisco UCS Central release 2.1(1c):

Defect ID	Description
CSCwp10391	After deploying or upgrading Cisco UCS Central 2.1(1a) or 2.1(1b), you may encounter a completely blank white screen in the GUI's Chassis Profile section. The issue affects Cisco UCS Central versions 2.0(1v), 2.0(1w), 2.1(1a) and 2.1(1b).

Resolved Caveats in Release 2.1(1a)

The following caveats have been resolved in Cisco UCS Central release 2.1(1a):

Defect ID	Description
CSCwk79109	The registration process is unsuccessful, and the graphical user interface (GUI) fails to establish a connection with Cisco UCS Central when using an IPv6 address.
CSCwm60042	The request to obtain a domain display certificate failed after restoring Cisco UCS Central
CSCwm72373	The operations manager encountered a failure following the upgrade to UCS Central version 2.0(1v)
CSCwn02373	The synchronization issue with Cisco UCS Manager has led to the manual inventory refresh process being stuck
CSCwn98891	The Cisco UCS Central encounters an issue where it fails to upload an .iso image during the upgrade process for a Fabric Interconnect 6536.

Defect ID	Description
CSCwh37482	Unable to launch KVM using IPv6 in Cisco UCS Central.
CSCwh45850	Cisco UCS Central Online Help defects.
CSCwi23502	Error while creating the 40Gbps speed Port channel from Cisco UCS Central.
CSCwj77569	Cisco UCS Central is preventing the addition of comma-separated SAN values to a CSR.
CSCwj89003	Cisco UCS Central server power state is not in sync with Cisco UCS Manager.
CSCwk79854	The SSH transport protocol, including specific OpenSSH extensions, is available in OpenSSH versions prior to 9.6.
CSCwm96895	The Cisco UCS Central export configuration operation causes UCS Domains to lose visibility.
CSCwm33416	The SR-IOV feature enhancement is currently unavailable in Cisco UCS Central network policies.

Open Caveats

Open Caveats in Release 2.1(1c)

The following caveat is open in the Cisco UCS Central release 2.1(1c):

Defect ID	Symptom	Workaround
CSCwq95515	Server port configuration for X-Direct is not available through the Cisco UCS Central GUI.	Perform the following: • To configure an X-Direct port as a Server port through the UCS Central CLI, follow these steps: • UCSC# **connect resource-mgr** • UCSC(resource-mgr) # **scope domain-mgmt** • UCSC(resource-mgr) /domain-mgmt # **scope ucs-domain** <*domain_ID*> • UCSC(resource-mgr) /domain-mgmt/ucs-domain # **scope eth-server** • UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-server # **scope fabric {b}** • UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-server/fabric # **create interface** slot-id port-id • UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-server/fabric/interface # **commit-buffer** • UCSC(resource-mgr) /domain-mgmt/ucs-domain # • Configure from Cisco UCS Manager.

Defect ID	Symptom	Workaround
CSCwq99695	The Decommission Chassis option must be enabled for Extended chassis within X-Direct in the Cisco UCS Central GUI.	Perform the following: • You can decommision chassis option using the Cisco UCS Central CLI: • UCSC# **connect resource-mgr** • UCSC(resource-mgr) # **scope domain-mgmt** • UCSC(resource-mgr) /domain-mgmt # **scope ucs-domain** <*domain_ID*> • UCSC(resource-mgr) /domain-mgmt/ucs-domain # **decommision chassis** <*chassis_ID*> • UCSC(resource-mgr) /domain-mgmt/ucs-domain # **commit-buffer** • UCSC(resource-mgr) /domain-mgmt/ucs-domain # • Configure from Cisco UCS Manager.
CSCwq90038	Unable to use filter with Cisco UCS 6664 Fabric Interconnect while creating Maintenance Group Tag.	Add the Cisco UCS 6664 Fabric Interconnect domains for Maintenance Group Tag directly without using filter.
CSCwq90043	The Cisco UCS 6664 Fabric Interconnect infrastructure firmware cannot be added through the Cisco UCS Central GUI or CLI.	Configure the Cisco UCS 6664 Fabric Interconnect Infrastructure firmware update through Cisco UCS domain.

Open Caveats in Release 2.1 (1b)

The following caveat is open in the Cisco UCS Central release 2.1(1b):

Defect ID	Symptom	Workaround
CSCwq53304	The HCL Sync operation fails when both Firmware Image Download and HCL Sync are triggered simultaneously.	To download the HCL file, select only the HCL check box and uncheck the Firmware Image Download option. Alternatively, you can retry the HCL Sync after a failure.
CSCwp10391	After deploying or upgrading Cisco UCS Central 2.1(1a) or 2.1(1b), you may encounter a completely blank white screen in the GUI's Chassis Profile section. The issue affects Cisco UCS Central versions 2.1(1a) and 2.1(1b).	The GUI page shows no error message but fails to display any data. The problem begins with version 2.1(1a) and 2.1(1b). An alternative approach is to use the CLI.

Open Caveats in Release 2.1 (1a)

The following caveat is open in the Cisco UCS Central release 2.1(1a):

Defect ID	Symptom	Workaround
CSCwo48958	KVM launch from Cisco UCS Central fails for Cisco UCS Manager domains running on Cisco UCS Manager version 4.3(6).	Launch the KVM from the Cisco UCS Manager domain.
CSCwo72261	Network Manager failures and kernel messages related to *start dnf makecache failure* occur during the initial configuration of Cisco UCS Central.	Press Enter to proceed further with the user input or installation.
CSCwp10391	After deploying or upgrading Cisco UCS Central 2.1(1a) or 2.1(1b), you may encounter a completely blank white screen in the GUI's Chassis Profile section. The issue affects Cisco UCS Central versions 2.1(1a) and 2.1(1b).	The GUI page shows no error message but fails to display any data. The problem begins with version 2.1(1a) and 2.1(1b). An alternative approach is to use the CLI.

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 Central Configuration Guides
- Cisco UCS Central CLI Reference Manual
- Cisco UCS Central Faults Reference Manual