Release Notes for Cisco UCS Manager, Release 6.0

First Published: 2025-09-02

Cisco UCS Manager

Cisco UCS™ Manager, Release 6.0 provides unified, embedded management of all software and hardware components of the Cisco Unified Computing System™ (Cisco UCS) across multiple chassis, Cisco UCS servers, and thousands of virtual machines. Cisco UCS Manager manages Cisco UCS as a single entity through an intuitive GUI, a command-line interface (CLI), or an XML API for comprehensive access to all Cisco UCS Manager functions. For more information on Cisco UCS Manager, see Cisco UCS Manager on Cisco.com.

This document contains information on new features, resolved caveats, open caveats, and workarounds for Cisco UCS Manager, Release 6.0. This document also includes the following:

- Current information that became available after the technical documentation was published
- Related firmware and BIOS on blade and rack servers and other Cisco Unified Computing System (UCS) components associated with the release

Revision History

Table 1: Release 6.0(1)

Release	Date	Description
6.0(1b)	September 02, 2025	Created release notes for Cisco UCS Manager Release 6.0(1b).

What's New

New Hardware Features

- New Hardware in Release 6.0(1b), on page 1

New Software Features

- New Software Feature in Release 6.0(1b), on page 2

New Hardware in Release 6.0(1b)

- 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.
- Support for 30TB 2.5 inch pTLC Micron 6550 NVMe drive on Cisco UCS C225 M8 servers
- Cisco UCS Manager introduces dual support for the Cisco Tri-Mode M1 24G RAID (UCSC-RAID-M1L16) controllers on Cisco UCS C240 M8 Servers, enabling independent configuration and management of two controllers within the same server environment.

New Software Feature in Release 6.0(1b)

Support for the following software features:

- Fabric Interconnect Audit Log support using the Linux Audit Framework (auditd), providing comprehensive monitoring and tracking of user and system activities on Cisco UCS 6600, 6500, and 6400 Series Fabric Interconnects. This feature enables enhanced security and compliance by recording activities into Fabric Interconnect Audit Log files.
- 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.
- iSCSI boot support using Internet Protocol version 6 (IPv6) for Cisco UCS servers, enabling seamless integration into IPv6-capable IP networks. This addresses IPv4 limitations and offers improved scalability and management for next-generation infrastructure deployments.
- Support for AES master key and MACsec (Type-6 [AES], Type-0, and Type-7 encryption) for Ethernet uplink ports is now available on Cisco UCS 6664 Fabric Interconnects and Cisco UCS X-Series Direct (Cisco UCS Fabric Interconnects 9108 100G).
- Support for ERSPAN on Cisco UCS X-Series Direct (Cisco UCS Fabric Interconnects 9108 100G).
- Migration support for Cisco UCS 6600 Series Fabric Interconnect, including:
  - UCS-FI-6454 to UCS-FI-6664
  - UCS-FI-64108 to UCS-FI-6664
  - UCS-FI-6536 to UCS-FI-6664
- Added warning message for Native VLAN Configuration changes on vNICs, highlighting the requirement for a port flap and a brief connectivity impact (approximately 20–40 seconds) when the Native VLAN is modified. This enhancement helps administrators better plan for and manage VLAN changes.
- Support for KVM direct access over inband on Cisco UCS C-Series M8, M7, and M6 servers, enabling administrators to securely access and manage server consoles directly over the inband network and improving operational efficiency and flexibility for Cisco UCS C-Series servers.

- Support for secure deletion of all data on Cisco UCS 6400, 6500, 6600 Series, and X-Series Direct Fabric Interconnect using the Command Line Interface (CLI). This enhancement ensures customer data privacy by permanently deleting all data, eliminating the possibility of data retrieval or recovery.
- Enhanced Login Profile security with configurable rules for user login attempts, enabling administrators to monitor and audit access. The system can block further logins for a set time after a specified number of failed attempts to prevent unauthorized access. Additionally, Cisco UCS Manager now generates syslog messages for authentication failures, including details such as user ID, domain ID, IP address, and account status.

Security Fixes

Security Fixes in Release 6.0(1b)

Defect ID - CSCwm98102

The Cisco products UCS B-Series Blade Servers, UCS C-Series Rack Servers and UCS X-Series Compute Nodes may include an optional Trusted Platform Module (TPM) 2.0 that is affected by the vulnerability identified by the following Common Vulnerability and Exposures (CVE) ID:

- CVE-2025-2884—TCG TPM2.0 Reference implementation's CryptHmacSign helper function is vulnerable to Out-of-Bounds read due to the lack of validation the signature scheme with the signature key's algorithm. See Errata Revision 1.83 and advisory TCGVRT0009 for TCG standard TPM2.0

Cisco UCS servers equipped with one of the following optional TPM modules:

- UCSX-TPM2-002
- UCSX-TPM-002C
- UCS-TPM-002D
- UCSX-TPM-002D

The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.

Defect ID - CSCwb83414

Cisco UCS Manager includes Third-party Software that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-2009-5155—The glob implementation in the GNU C Library (glibc) does not properly handle long patterns, which may allow context-dependent attackers to cause a denial of service or possibly execute arbitrary code via a crafted pattern.
- CVE-2010-3192—The GNU C Library (glibc) does not properly restrict the use of the LD_AUDIT environment variable for setuid/setgid binaries, which allows local users to gain privileges by executing setuid programs with this variable set.
- CVE-2013-0242—The iconv program in GNU C Library (glibc) does not properly handle certain invalid multi-byte input sequences, which could allow remote attackers to cause a denial of service or possibly execute arbitrary code.

- CVE-2014-4043—The wordexp function in GNU C Library (glibc) allows context-dependent attackers to bypass intended restrictions via shell metacharacters, which are not properly handled in certain cases.
- CVE-2014-9402—The __hcreate_r function in GNU C Library (glibc) does not properly check for integer overflows, which could allow attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2014-9761—The gethostbyname function in GNU C Library (glibc) does not properly handle long hostnames, which allows remote attackers to cause a denial of service or possibly have unspecified other impact.
- CVE-2015-5180—The iconv function in GNU C Library (glibc) does not properly handle certain input sequences, which allows attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2015-8776—The catopen function in GNU C Library (glibc) does not properly handle negative values, which could allow local users to cause a denial of service or possibly execute arbitrary code.
- CVE-2015-8777—The regcomp function in GNU C Library (glibc) may allow context-dependent attackers to cause a denial of service or possibly execute arbitrary code via a crafted regular expression.
- CVE-2015-8778—The getnetbyname function in GNU C Library (glibc) does not properly handle long network names, which could allow attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2015-8779—The getaliasbyname function in GNU C Library (glibc) does not properly handle long alias names, which could allow attackers to cause a denial of service or potentially execute arbitrary code.
- CVE-2015-8982—The nan, nanf, and nanl functions in GNU C Library (glibc) do not properly handle certain malformed strings, which could allow attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2015-8983—The strftime function in GNU C Library (glibc) does not properly handle certain format strings, which could allow attackers to cause a denial of service or potentially execute arbitrary code.
- CVE-2015-8984—The fnmatch function in GNU C Library (glibc) does not properly handle certain patterns, which could allow attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2015-8985—The glob function in GNU C Library (glibc) does not properly handle certain patterns, which could allow attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2016-10228—The iconv program in GNU C Library (glibc) does not properly handle certain malformed input sequences, which could allow attackers to cause a denial of service or potentially execute arbitrary code.
- CVE-2016-10739—The getaddrinfo function in GNU C Library (glibc) does not properly handle large AF_INET6 responses, which could allow remote attackers to cause a denial of service or potentially execute arbitrary code.
- CVE-2016-1234—The send_dg function in the resolver in GNU C Library (glibc) does not properly handle certain responses, which could allow remote attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2016-4429—The resolver in GNU C Library (glibc) does not properly handle crafted DNS responses, which could allow remote attackers to cause a denial of service or possibly execute arbitrary code.

- CVE-2017-1000366—The dynamic linker in GNU C Library (glibc) does not properly handle certain environment variables, which could allow local attackers to gain privileges or bypass security restrictions.
- CVE-2017-12132—The _dl_init_paths function in GNU C Library (glibc) does not properly process certain environment variables, which could allow local users to gain elevated privileges or bypass security restrictions.
- CVE-2017-15670—The glob function in GNU C Library (glibc) does not properly handle certain patterns, which could allow attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2017-15671—The glob function in GNU C Library (glibc) does not properly handle memory allocation failures, which could allow attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2017-15804—The glob function in GNU C Library (glibc) does not properly handle certain file system conditions, which could allow attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2018-1000001—The realpath function in GNU C Library (glibc) does not properly handle long paths, which could allow attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2018-11236—The GNU C Library (glibc) does not properly restrict stack pointer usage in certain conditions, which could allow local attackers to execute arbitrary code or cause a denial of service.
- CVE-2018-11237—The GNU C Library (glibc) may allow attackers to cause a denial of service or possibly execute arbitrary code via crafted input that triggers incorrect handling of certain memory operations.
- CVE-2018-19591—The getcwd function in GNU C Library (glibc) does not properly handle very long directory names, which could allow local attackers to cause a denial of service or potentially execute arbitrary code.
- CVE-2018-20796—The glob function in GNU C Library (glibc) does not properly handle crafted patterns, which could allow attackers to cause a denial of service or potentially execute arbitrary code.
- CVE-2018-6485—The _dl_map_object_from_fd function in GNU C Library (glibc) does not properly handle certain ELF files, which could allow local attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2019-25013—The iconv function in GNU C Library (glibc) does not properly handle certain input sequences, which could allow attackers to cause a denial of service or potentially execute arbitrary code.
- CVE-2019-6488—The glob function in GNU C Library (glibc) does not properly handle memory allocation failures, which could allow attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2019-7309—The glob function in GNU C Library (glibc) does not properly handle crafted patterns in certain conditions, which could allow attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2019-9169—The __libc_open function in GNU C Library (glibc) does not properly handle file descriptors in certain situations, which could allow local attackers to cause a denial of service or potentially execute arbitrary code.
- CVE-2020-10029—The memmem function in GNU C Library (glibc) on 32-bit systems may read out of bounds, which could allow attackers to cause a denial of service or possibly execute arbitrary code.

- CVE-2020-1751—The nss_dns module in GNU C Library (glibc) does not properly handle crafted DNS responses, which could allow remote attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2020-1752—The getaddrinfo function in GNU C Library (glibc) does not properly handle certain crafted responses, which could allow remote attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2020-27618—The iconv function in GNU C Library (glibc) does not properly handle certain input sequences, which could allow attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2020-29573—The qsort function in GNU C Library (glibc) does not properly check for pointer overflows, which could allow attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2020-6096—The x86-64 memcpy function in GNU C Library (glibc) does not properly handle overlapping memory regions, which could allow attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2021-3326—The mq_notify function in GNU C Library (glibc) does not properly handle certain parameters, which could allow local attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2021-35942—The wordexp function in GNU C Library (glibc) does not properly handle crafted patterns, which could allow attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2021-38604—The iconv function in GNU C Library (glibc) does not properly handle certain input sequences, which could allow attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2022-23218—The iconv function in GNU C Library (glibc) does not properly handle certain malformed input sequences, which could allow attackers to cause a denial of service or potentially execute arbitrary code.
- CVE-2022-23219—The iconv function in GNU C Library (glibc) does not properly handle certain malformed input sequences, which could allow attackers to cause a denial of service or potentially execute arbitrary code.

The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.

Defect ID - CSCwb84351

Cisco UCS Manager includes Third-party Software that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-2015-5602—sudo before 1.8.14 does not properly parse sudoers rules, which could allow local users to bypass intended restrictions and execute arbitrary commands via a user specification containing a netgroup that is followed by an exclusion (exclamation mark) operator.
- CVE-2016-7076—sudo before 1.8.18 does not properly manage the TZ environment variable, allowing local users to bypass security restrictions or possibly execute arbitrary code via a specially crafted value of TZ in the environment of a sudo command.
- CVE-2017-1000367—In Sudo before 1.8.20, an attacker with sudo privileges may be able to run arbitrary commands as root due to an unsafe library search path, potentially resulting in privilege escalation.

- CVE-2017-1000368—Sudo before 1.8.20 improperly handles certain command line arguments, allowing local users to obtain unintended access or execute arbitrary commands as another user by leveraging a race condition.
- CVE-2019-14287—A flaw in Sudo before 1.8.28 allows a user with permission to run commands as any user except root to execute commands as root by specifying the user ID -1 or 4294967295.
- CVE-2019-18634—Sudo before 1.8.26 does not properly handle the pwfeedback option, which can allow a local user to cause a stack-based buffer overflow and potentially execute arbitrary code or escalate privileges.
- CVE-2021-23239—Sudo before 1.9.5p2 incorrectly handles certain sudoers rules for Runas user specifications, which could allow users to bypass security policies and execute commands as unintended users.
- CVE-2021-23240—Sudo before 1.9.5p2 may allow a local user to bypass Runas user restrictions due to incorrect parsing of sudoers files, enabling the execution of commands as a user other than the one intended by policy.
- CVE-2021-3156—A heap-based buffer overflow vulnerability in Sudo before 1.9.5p2, known as "Baron Samedit," allows local users to gain root privileges by triggering improper handling of command line arguments.

The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.

Defect ID - CSCwf97363

Cisco UCS Manager includes Third-party Software that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-2012-0876—OpenSSL before 1.0.0h and 1.0.1-beta before 1.0.1-beta3 allows remote attackers to cause a denial of service via a crafted record that triggers an out-of-bounds read.
- CVE-2012-2135—Python before 2.7.3 and 3.x before 3.2.3 does not properly handle Unicode strings in the urllib module, which could allow remote attackers to conduct cross-site scripting (XSS) attacks or obtain sensitive information.
- CVE-2013-1753—Python before 2.7.5 and 3.x before 3.3.2 allows remote attackers to cause a denial of service via crafted input to the SSL module, resulting in excessive CPU consumption.
- CVE-2013-2099—Multiple integer overflow vulnerabilities in Python, including in the buffer and unicodeobject modules, could allow remote attackers to execute arbitrary code or cause a denial of service.
- CVE-2013-4238—OpenSSL before 1.0.1e does not properly handle certain DTLS retransmissions, which allows remote attackers to cause a denial of service via crafted DTLS packets.
- CVE-2013-7040—Python 2.7 before 2.7.7 and 3.x before 3.3.3 does not properly handle certain SSL certificate attributes, which could allow remote attackers to spoof SSL servers via crafted certificates.
- CVE-2013-7338—Python 2.7 before 2.7.7 and 3.x before 3.3.3 allows remote attackers to cause a denial of service via crafted input that triggers an infinite loop in the SSL module.
- CVE-2013-7440—The Python CGIHTTPServer module before 2.7.9 and 3.x before 3.4.3 allows remote attackers to execute arbitrary code via crafted HTTP requests that inject shell commands.

- CVE-2014-0224—OpenSSL before 1.0.1h allows man-in-the-middle attackers to decrypt and modify traffic via a flaw in the SSL/TLS handshake process when both client and server are vulnerable.
- CVE-2014-1912—Python 2.7 before 2.7.7 and 3.x before 3.3.3 allows remote attackers to cause a denial of service via crafted input to the socket module, which can trigger memory corruption.
- CVE-2014-2667—The urllib3 library before version 1.8 does not properly handle subjectAltName fields in X.509 certificates, which could allow remote attackers to spoof SSL servers via crafted certificates.
- CVE-2014-4616—OpenSSL before 1.0.1i does not properly restrict processing of DTLS packets, which allows remote attackers to cause a denial of service via crafted DTLS handshake messages.
- CVE-2014-4650—The ssl module in Python before 2.7.8 and 3.x before 3.4.2 does not properly handle certain TLS handshake messages, which could allow remote attackers to cause a denial of service.
- CVE-2014-7185—Python before 2.7.9 and 3.x before 3.4.3 allows remote attackers to execute arbitrary code via crafted pickle data that triggers unsafe loading.
- CVE-2014-9365—The Python email module before 2.7.9 and 3.x before 3.4.3 does not properly handle certain headers, which could allow remote attackers to conduct header injection attacks.
- CVE-2015-1283—Integer overflow in the zipimport module in Python before 2.7.9 and 3.x before 3.4.3 could allow attackers to execute arbitrary code or cause a denial of service via a crafted ZIP archive.
- CVE-2015-20107—Python 3.10.0 through 3.10.6 and 3.11.0a1 through 3.11.0b3 allows command injection via the mailcap module when parsing certain files, potentially allowing attackers to execute arbitrary commands.
- CVE-2015-5652—OpenSSL before 1.0.2d and 1.0.1p does not properly validate certain ASN.1 structures, which could allow remote attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2016-0718—The _json module in Python before 2.7.11 and 3.x before 3.4.4 allows context-dependent attackers to cause a denial of service via a crafted JSON document that triggers an incorrect exception.
- CVE-2016-0772—The ssl.match_hostname function in Python before 2.7.10 and 3.x before 3.4.4 does not properly match IP addresses in hostnames, which could allow attackers to spoof SSL servers.
- CVE-2016-1000110—The urllib3 and requests libraries, before urllib3 1.23 and requests 2.20.0, do not properly handle certain HTTP headers, which could allow remote attackers to conduct CRLF injection attacks via crafted headers.
- CVE-2016-2183—The SWEET32 attack affects 64-bit block ciphers in TLS, such as 3DES and Blowfish, allowing remote attackers to recover plaintext data via a birthday attack against long-duration encrypted sessions.
- CVE-2016-3189—Python before 2.7.12 and 3.x before 3.5.2 does not properly validate certificates when using the ssl.match_hostname function, which could allow remote attackers to spoof SSL servers.
- CVE-2016-4472—Python before 2.7.13 and 3.x before 3.5.2 does not properly handle certain HTTP responses in the httplib module, which could allow remote attackers to conduct HTTP header injection attacks.
- CVE-2016-5636—OpenSSL before 1.0.2i and 1.0.1u does not properly validate certain certificate fields, which could allow remote attackers to conduct impersonation attacks or cause a denial of service.
- CVE-2016-5699—Python before 2.7.13 and 3.x before 3.5.2 does not properly handle certain HTTP responses in urllib, which could allow attackers to conduct HTTP response splitting attacks.

- CVE-2016-9063—The DES and Triple DES ciphers, as used in OpenSSL and NSS, have a birthday bound of approximately four billion blocks, allowing remote attackers to recover plaintext data via a birthday attack (SWEET32).
- CVE-2017-1000158—Python 2.7 before 2.7.13 and 3.x before 3.6.1 does not properly handle certain Unicode strings in the urllib and http libraries, which could allow remote attackers to conduct CRLF injection attacks.
- CVE-2017-9233—The _strxfrm function in Python before 2.7.14 and 3.x before 3.6.2 does not properly validate certain input, which could allow attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2018-1000030—Python before 2.7.14 and 3.x before 3.6.4, when using shutil.rmtree with symlinks, may allow local attackers to delete arbitrary files via a race condition.
- CVE-2018-1000802—Python 2.7, 3.4, 3.5, and 3.6 allow local users to execute arbitrary code as root via a Trojan horse module in a local directory, which is searched before system directories when running scripts with elevated privileges.
- CVE-2018-1060—Python 2.7 before 2.7.15 and 3.x before 3.4.6 and 3.5.x before 3.5.3 does not properly handle certain regular expressions in the difflib and poplib modules, which could allow attackers to cause a denial of service.
- CVE-2018-1061—Python 2.7 before 2.7.15 and 3.x before 3.4.6 and 3.5.x before 3.5.3 allows remote attackers to cause a denial of service via a crafted email address to the email.utils.parseaddr function.
- CVE-2018-14647—The PyYAML library in versions before 4.1 allows remote attackers to execute arbitrary code via crafted YAML input, due to unsafe use of the yaml.load function.
- CVE-2018-20406—Python 2.7 before 2.7.16 and 3.x before 3.4.10, 3.5.x before 3.5.7, and 3.6.x before 3.6.9 does not properly handle certain regular expressions in the difflib module, which may allow attackers to cause a denial of service.
- CVE-2018-20852—Python 3.7.x before 3.7.4 and 3.8.x before 3.8.1 does not properly handle certain inputs in the urllib.parse module, which could allow attackers to bypass URL parsing restrictions.
- CVE-2018-25032—zlib through 1.2.11 has a memory corruption issue related to the inflateMark function, which could allow attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2019-10160—Python 2.7 before 2.7.16 and 3.x before 3.7.3 does not properly handle certain regular expressions in the difflib module, which could allow attackers to cause a denial of service.
- CVE-2019-12900—zlib through 1.2.11 has a memory corruption issue in the inflate function, which could allow remote attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2019-15903—Python 2.7 before 2.7.17 and 3.x before 3.7.5 does not properly validate input in the tarfile module, which could allow remote attackers to write files outside of the intended directory via a crafted TAR archive.
- CVE-2019-16056—Python 2.7 before 2.7.17 and 3.x before 3.7.5 does not properly handle certain inputs in the http.client module, which could allow attackers to conduct HTTP header injection attacks.
- CVE-2019-16935—Python 2.7 before 2.7.18 and 3.x before 3.7.6 has an issue in the XML parsing modules (xmlrpc), which could allow remote attackers to cause a denial of service via crafted XML data.

- CVE-2019-18348—The urllib3 library before 1.25.3 does not properly remove the authorization header when a redirect to a different host occurs, which could allow remote attackers to obtain sensitive information by intercepting redirected requests.
- CVE-2019-20907—Python 3.4.x through 3.8.x mishandles certain regular expressions in the re module, which could allow attackers to cause a denial of service via a crafted regex pattern.
- CVE-2019-5010—Python before 2.7.16 and 3.x before 3.7.2 mishandles null bytes in certain inputs to the xmlrpc.client and xmlrpc.server modules, which could allow remote attackers to cause a denial of service.
- CVE-2019-9636—Python 3.x before 3.7.3 does not properly sanitize input in the urlsplit and urlparse functions, which could allow attackers to bypass security restrictions or conduct attacks such as URL spoofing.
- CVE-2019-9674—Python 3.0 through 3.7.2 mishandles certain crafted ZIP archives in the zipfile module, which could allow attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2019-9947—Python 2.7 before 2.7.16 and 3.x before 3.7.3 mishandle certain newline characters in the urllib module, which could allow attackers to conduct HTTP header injection attacks.
- CVE-2019-9948—Python 2.7 before 2.7.16 and 3.x before 3.7.3 mishandle certain inputs in the urllib module, which could allow attackers to conduct HTTP header injection attacks.
- CVE-2020-10735—Python 3.7 through 3.10 mishandles int to string conversions for large integers, which could allow attackers to cause a denial of service via excessive CPU usage.
- CVE-2020-14422—Python 2.7 before 2.7.18 and 3.x before 3.7.7 mishandles certain inputs in the http.client module, which could allow attackers to conduct HTTP header injection attacks.
- CVE-2020-15523—Python 2.7 before 2.7.18 and 3.x before 3.8.4 mishandles certain regular expressions in the difflib and poplib modules, which could allow attackers to cause a denial of service.
- CVE-2020-15801—Python 3.8.x before 3.8.5 mishandles certain inputs in the tarfile module, which could allow remote attackers to write files outside of the intended directory via a crafted TAR archive.
- CVE-2020-26116—Python 3.x before 3.9.0 mishandles certain regular expressions in the difflib module, which could allow attackers to cause a denial of service via excessive CPU consumption.
- CVE-2020-27619—Python 3.8.x before 3.8.6 mishandles certain inputs in the http.client module, which could allow attackers to conduct HTTP header injection attacks.
- CVE-2020-8315—Python 2.7 before 2.7.18 and 3.x before 3.8.3 mishandles certain inputs in the urllib module, which could allow attackers to conduct HTTP header injection attacks.
- CVE-2020-8492—Python 2.7 before 2.7.18 and 3.x before 3.8.2 mishandles certain inputs in the urllib.parse module, which could allow attackers to bypass security restrictions or conduct attacks such as URL spoofing.
- CVE-2021-23336—Python 3.6.x through 3.8.x mishandles certain URLs in the urllib.parse module, which could allow attackers to bypass security restrictions or conduct attacks such as URL spoofing.
- CVE-2021-3177—Python 3.x before 3.9.2 has a buffer overflow in the PyCArg_repr function in the ctypes module, which could allow attackers to execute arbitrary code or cause a denial of service.
- CVE-2021-3426—Python 3.7.x before 3.7.10, 3.8.x before 3.8.8, and 3.9.x before 3.9.2 mishandle certain regular expressions in the re module, which could allow attackers to cause a denial of service via excessive CPU usage.

- CVE-2021-3733—Python 3.6.x through 3.9.x mishandles certain inputs in the urllib.parse module, which could allow attackers to bypass security restrictions or conduct attacks such as URL spoofing.
- CVE-2021-3737—Python 3.6.x through 3.9.x mishandles certain inputs in the urllib.parse module, which could allow attackers to bypass security restrictions or conduct attacks such as URL spoofing.
- CVE-2021-4189—Python 3.6.x through 3.9.x mishandles certain inputs in the urllib.request module, which could allow attackers to bypass security restrictions or conduct attacks such as URL spoofing.
- CVE-2022-0391—Python 3.7.x through 3.9.x mishandles certain inputs in the urllib.parse module, which could allow attackers to bypass security restrictions or conduct attacks such as URL spoofing.
- CVE-2022-26488—Python 2.7 before 2.7.18 and 3.x before 3.8.10 mishandles certain inputs in the http.client module, which could allow attackers to conduct HTTP header injection attacks.
- CVE-2022-37454—The Python 'random' module, as used in PyCryptodome before 3.15, may generate predictable random numbers under certain conditions, which could weaken cryptographic operations and allow attackers to guess secret values.
- CVE-2022-45061—Python 3.9.x before 3.9.16, 3.10.x before 3.10.9, and 3.11.x before 3.11.1 mishandle certain regular expressions in the urllib module, which could allow attackers to cause a denial of service via excessive CPU usage.
- CVE-2023-24329—The urllib.parse module in Python 3.x before 3.10.10 and 3.11.x before 3.11.2 does not properly parse URLs containing whitespace characters, which could allow attackers to bypass security checks or conduct spoofing attacks.
- CVE-2023-27043—Python 3.7.x through 3.11.x mishandles certain inputs in the urllib.parse module, which could allow attackers to conduct HTTP header injection or other attacks by bypassing input validation.

The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.

Defect ID - CSCwf97368

Cisco UCS Manager includes Third-party Software that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-2011-2939—Perl before 5.14.2 and 5.12.4 allows context-dependent attackers to execute arbitrary code or cause a denial of service via a crafted regular expression that triggers a heap-based buffer overflow.
- CVE-2012-5195—The Perl CGI module before 3.63 allows remote attackers to inject HTTP headers via newline characters in the values of certain CGI parameters.
- CVE-2012-6329—The Encode module in Perl before 5.16.1 does not properly handle certain UTF-8 input, which could allow context-dependent attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2013-1667—The CGI module in Perl before 5.14.3 and 5.16.x before 5.16.3 does not properly handle special characters in MIME headers, which could allow remote attackers to inject arbitrary HTTP headers.
- CVE-2014-4330—Perl before 5.20.1 mishandles certain crafted regular expressions, which could allow context-dependent attackers to cause a denial of service or possibly execute arbitrary code.

- CVE-2015-8853—The File::Temp module in Perl before 2.26 does not properly check permissions for temporary files, which could allow local users to obtain sensitive information or modify data via a symlink attack.
- CVE-2016-1238—Perl before 5.24.1 does not properly search for library paths, which could allow local users to execute arbitrary code via a Trojan horse module in an insecure directory.
- CVE-2016-2381—The DB_File module in Perl before 5.24.0 allows context-dependent attackers to execute arbitrary code or cause a denial of service via crafted input that triggers memory corruption.
- CVE-2017-12814—The XSLoader module in Perl before 5.24.3 and 5.26.x before 5.26.1 does not properly handle certain input, which could allow attackers to execute arbitrary code or cause a denial of service.
- CVE-2017-12837—Perl before 5.26.2 mishandles certain crafted regular expressions, which could allow context-dependent attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2017-12883—Perl before 5.26.2 mishandles certain crafted regular expressions, which could allow context-dependent attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2018-12015—The Archive::Tar module in Perl before 2.24 allows remote attackers to overwrite arbitrary files via a symlink attack in a TAR archive.
- CVE-2018-18311—Perl before 5.28.1 mishandles certain crafted regular expressions, which could allow context-dependent attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2018-18312—Perl before 5.28.1 mishandles certain crafted regular expressions, which could allow context-dependent attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2018-18313—Perl before 5.28.1 mishandles certain crafted regular expressions, which could allow context-dependent attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2018-18314—Perl before 5.28.1 mishandles certain crafted regular expressions, which could allow context-dependent attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2018-6913—The Encode module in Perl before 5.26.2 allows context-dependent attackers to cause a denial of service via crafted input that triggers a buffer overflow.
- CVE-2020-10543—Perl before 5.30.3 mishandles certain crafted regular expressions, which could allow context-dependent attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2020-10878—Perl before 5.30.3 mishandles certain crafted regular expressions, which could allow context-dependent attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2020-12723—Perl before 5.30.3 mishandles certain crafted regular expressions, which could allow context-dependent attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2023-31486—The Archive::Tar module in Perl before 2.40 does not properly validate file paths in TAR archives, which could allow attackers to write files outside of the intended directory via a crafted archive.

The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.

Defect ID - CSCwb84668

Cisco UCS Manager includes Third-party Software that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-2014-9471—The chfn and chsh utilities in util-linux before 2.26 do not properly check for newline characters in user input, which could allow local users to bypass security restrictions or inject malicious content into configuration files.
- CVE-2015-4042—The su utility in util-linux before 2.26.2 does not properly clear environment variables, which could allow local users to gain privileges or bypass security restrictions via a crafted environment.
- CVE-2016-2781—The chroot utility in GNU coreutils before 8.25 does not properly drop supplementary groups before executing commands, which could allow local users to bypass intended security restrictions.
- CVE-2017-18018—runuser in util-linux before 2.30.2 does not properly clear environment variables, which could allow local users to gain privileges or bypass security restrictions via a crafted environment.

The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.

Resovled Caveats

Resolved Caveats in Release 6.0(1b)

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwo62993	Secure LDAP authentication fails intermittently on some Cisco UCS Manager domains after trustpoint configuration changes. The issue manifests as **TLS start failed** errors and **unknown CA** alerts, indicating certificate validation problems. Affected domains show **unable to get local issuer certificate** errors during SSL verification despite network connectivity to the LDAP server. This issue is resolved	4.3(3a)	6.0(1b)

Open Caveats

Open Caveats in Release 6.0(1b)

The following caveats are open in Release 6.0(1b).

Defect ID	Symptom	Workaround	First Bundle Affected
CSCwq17020	After installing U3 Micron drives with capacities of 3.8TB or larger in JBOD mode behind the UCSX-X10C-RAIDF controller, Linux OS fails to boot due to BIOS errors related to loading the EFI boot image. This issue occurs specifically on Cisco UCS M8 servers equipped with Intel® processors and affects multiple Linux distributions. The problem does not occur when the drives are configured in RAID 0. Microsoft Windows® and Linux OS boot successfully on smaller capacity drives or when using RAID 0.	Install the OS on drive configured in RAID.	4.3(6a)
CSCwq34720	Re-association of the Cisco UCS X210c M7 compute node, running Windows 2022 Server with **Secure Boot** enabled, fails with the following error:`SBAT self-check failed: Security Policy Violation`	Remove the SBAT variable from the BIOS token and then perform a CMOS clear. After this, the service profile association will complete successfully with Secure Boot enabled, allowing the system to boot normally. Cisco recommends that you contact TAC for further assistance.	4.3(5c)B

Defect ID	Symptom	Workaround	First Bundle Affected
CSCwq94580	After upgrading the infrastructure A bundle to release 6.0(1b), server maintenance operations on Cisco UCS C Series M5 rack servers may fail due to unsupported hardware or software configurations detected during the upgrade. This issue occurs in setups equipped with Cisco UCS FI models 6400 series, 6536, and UCSX-S9108-100G.	You must reboot the FIs sequentially starting with secondary role FI first. **Note** Rebooting the FIs is a disruptive operation that will result in a temporary service interruption. It is recommended to perform this task during a planned maintenance window. Cisco recommends that you contact TAC for further assistance.	6.0(1b)

Known Behavior and Limitations

Known Behavior and Limitations in Release 6.0(1b)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCwq41000	Broadcom AERO RAID controller (UCSX-X10C-RAIDF) for Cisco UCS X210c server and Cisco 12G Modular Raid controller with 4GB Cache (UCSC-RAID-M6T) do not transition drives from **Unconfigured Good (UG)** to **Online** state when **Auto Configuration Mode (ACM)** is set to RAID0 after storage profile redeploy and server reboot. As a result, RAID0 LUNs are not created. This issue affects drive state transitions and RAID0 LUN creation on Cisco Tri-Mode 24G SAS RAID Controller w/4GB Cache (UCSC-RAID-HP).	There is no known workaround.	6.0(1b)

Compatibility

Cisco UCS Manager and Cisco UCS C-Series Release Compatibility Matrix for C-Series Rack-Mount Servers

Cisco UCS C-Series Rack-Mount Servers are managed by built-in standalone software— Cisco Integrated Management Controller (Cisco IMC). However, when a C-Series Rack-Mount Server is integrated with Cisco UCS Manager, the Cisco IMC does not manage the server anymore.

Each Cisco UCS Manager release incorporates its corresponding C-Series Standalone release. For example, Cisco UCS Manager Release 4.3(6) includes the 4.3(6) server bundle for all the M8, M7, M6 and S3260 M5 servers, and the 4.3(2) server bundle for all other M5 servers. This ensures support for all M8, M7, M6, and M5 servers listed in the C-Series Standalone releases.

Cisco UCS Equivalency Matrix for Cisco Intersight, Cisco IMC, and Cisco UCS Manager outlines the release timeline for Cisco Intersight, Cisco Integrated Management Controller (IMC), and Cisco UCS Manager (UCSM). It includes essential information such as the date each patch was posted, the specific patch version, and the platforms that are supported by each release. By referring to this matrix, you can identify the appropriate firmware and software versions required for your servers before migrating them to Cisco Intersight. This ensures that your server infrastructure remains supported and operates efficiently during and after the transition.

The following table lists the Cisco UCS Manager and C-Series software standalone releases for C-Series Rack-Mount Servers:

Table 2: Cisco UCS Manager and C-Series Software releases for C-Series Servers

Cisco UCS Manager Release	C-Series Standalone Releases Included	C-Series Servers Supported by the C-Series Standalone Releases
6.0(1)	6.0(1)	All M8, M7, M6, and S3260 M5
	4.3(2)	All M5
4.3(6)	4.3(6)	All M8, M7, M6, and S3260 M5
	4.3(2)	All M5
4.3(5)	4.3(5)	All M8, M7, and M6
	4.3(4)	S3260 M5
	4.3(2)	All M5
4.3(4)	4.3(4)	C245 M8 All M7, M6, and S3260 M5
	4.3(2)	All M5
4.3(3)	4.3(3)	All M7, M6, and S3260 M5
	4.3(2)	All M5
4.3(2)	4.3(2)	All M7, M6, and M5

Cisco UCS Manager Release	C-Series Standalone Releases Included	C-Series Servers Supported by the C-Series Standalone Releases
4.2(3)	4.2(3)	All M6, M5, and S3260 M4
	4.1(3)	All M5 and S3260 M4
	4.1(2)	C220 M4, C240 M4, and C460 M4
4.2(2)	4.2(2)	All M6, M5, and S3260 M4
	4.1(3)	S3260 M4, All M5
	4.1(2)	C220 M4, C240 M4, C460 M4
4.2(1)	4.2(1)	All M6
	4.1(3)	S3260 M4, All M5
	4.1(2)	C220 M4, C240 M4, C460 M4
4.1(3)	4.1(3)	S3260 M4, All M5
	4.1(2)	C220 M4, C240 M4, C460 M4
	3.0(4)	All M3
4.1(2)	4.1(2)	C220 M5, C240 M5, C240 SD M5, C480 M5, S3260 M5, C480 M5 ML, C125 M5, C220 M4, C240 M4, C460 M4, S3260 M4
	3.0(4)	All M3
4.1(1)	4.1(1)	C220 M5, C240 M5, C480 M5, S3260 M5, C125 M5, C480 M5 ML only
	4.0(2)	C220 M4, C240 M4, C460 M4, S3260 M4, C125 M5 only
	3.0(4)	All M3
4.0(4)	4.0(4)	C220 M5, C240 M5, C480 M5, S3260 M5, C480 M5 ML only
	4.0(2)	C220 M4, C240 M4, C460 M4, S3260 M4, C125 M5 only
	3.0(4)	All M3

Cisco UCS Manager Release	C-Series Standalone Releases Included	C-Series Servers Supported by the C-Series Standalone Releases
4.0(2)	4.0(2)	C220 M4, C240 M4, C460 M4, C220 M5, C240 M5, C480 M5, S3260 M4, S3260 M5, C125 M5, C480 M5 ML only
	3.0(4)	All M3
4.0(1)	4.0(1)	C220 M4, C240 M4, C460 M4, C220 M5, C240 M5, C480 M5, S3260 M4, S3260 M5, C125 M5 only
	3.0(4)	All M3

Cross-Version Firmware Support

The Cisco UCS Manager A bundle software (Cisco UCS Manager, Cisco NX-OS, IOM and FEX firmware) can be mixed with previous B or C bundle releases on the servers (host firmware [FW], BIOS, Cisco IMC, adapter FW and drivers). To help you quickly verify valid combinations, this release includes an interactive compatibility tool, available here:

Cisco UCS Manager Cross Version Firmware Matrix

By selecting a Fabric Interconnect model along with the desired Infrastructure (A Bundle) and Host Firmware (B and C Bundles) releases, the tool dynamically displays whether each combination is a supported configuration.

Note Beginning with Cisco UCS Manager Release 6.0(1b), Cisco UCS 6300 Series FI and Cisco UCS 6332 FI are not supported.

Table 3: Mixed Cisco UCS Releases Supported on Cisco UCS 6664, 6536, and 6400 series Fabric Interconnects

	Infrastructure Versions (A Bundles)								
Host FW Versions (B or C Bundles)	4.2(1)	4.2(2)	4.2(3)	4.3(2)	4.3(3)	4.3(4)	4.3(5)	4.3(6)	6.0(1)
6.0(1)	—	—	—	—	—	—	—	—	6664, 6536, 6454, 64108
4.3(6)	—	—	—	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6664, 6536, 6454, 64108

	Infrastructure Versions (A Bundles)								
4.3(5)	—	—	—	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6664, 6536, 6454, 64108
4.3(4)	—	—	—	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6664, 6536, 6454, 64108
4.3(3)	—	—	—	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6664, 6536, 6454, 64108
4.3(2)	—	—	—	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6664, 6536, 6454, 64108
4.2(3)	6200, 6332, 6332-16UP, 6454, 64108	6200, 6332, 6332-16UP, 6454, 64108	6200, 6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6664, 6536, 6454, 64108
4.2(2)	6200, 6332, 6332-16UP, 6454, 64108	6200, 6332, 6332-16UP, 6454, 64108	6200, 6332, 6332-16UP, 6454, 64108	6332, 6332-16UP, 6454, 64108	6332, 6332-16UP, 6454, 64108	6332, 6332-16UP, 6454, 64108	6332, 6332-16UP, 6454, 64108	6332, 6332-16UP, 6454, 64108	—
4.2(1)	6200, 6332, 6332-16UP, 6454, 64108	6200, 6332, 6332-16UP, 6454, 64108	6200, 6332, 6332-16UP, 6454, 64108	6332, 6332-16UP, 6454, 64108	6332, 6332-16UP, 6454, 64108	6332, 6332-16UP, 6454, 64108	6332, 6332-16UP, 6454, 64108	6332, 6332-16UP, 6454, 64108	—

Table 4: Mixed Cisco UCS Releases Supported on Cisco UCS X-Series Direct

Host FW Versions (B Bundles)	Infrastructure Versions (A Bundles)			
	4.3(4)	4.3(5)	4.3(6)	6.0(1)
6.0(1)	—	—	—	UCSX-S9108-100G
4.3(6)	UCSX-S9108-100G	UCSX-S9108-100G	UCSX-S9108-100G	UCSX-S9108-100G

Host FW Versions (B Bundles)	Infrastructure Versions (A Bundles)			
4.3(5)	UCSX-S9108-100G	UCSX-S9108-100G	UCSX-S9108-100G	UCSX-S9108-100G
4.3(4)	UCSX-S9108-100G	UCSX-S9108-100G	UCSX-S9108-100G	UCSX-S9108-100G

You may also view the extended version of the Mixed Cisco UCS Releases Supported on Cisco UCS Fabric Interconnects at Cisco UCS Manager Cross-Version Firmware Support 6.0.

For reference, the Cisco UCS Equivalency Matrix for Cisco Intersight, Cisco IMC, and Cisco UCS Manager outlines the release timeline for Cisco Intersight, Cisco Integrated Management Controller (Cisco IMC), and Cisco UCS Manager. It includes essential information such as the date each patch was posted, the specific patch version, and the platforms that are supported by each release. By referring to this matrix, you can identify the appropriate firmware and software versions required for your servers before migrating them to Cisco Intersight. This ensures that your server infrastructure remains supported and operates efficiently during and after the transition.

Upgrade and Downgrade Guidelines

To get a complete overview of all the possible upgrade paths in Cisco UCS Manager, see Cisco UCS Manager Upgrade/Downgrade Support Matrix.

Upgrade and Downgrade to Release 6.0(1)

- If your setup is equipped with Cisco UCS 6664 Fabric Interconnect, you cannot downgrade Infrastructure Firmware Version (A Bundle) to any release earlier than 6.0(1b).
- If your setup is equipped with Cisco UCS X-Series Direct (Fabric Interconnect 9108 100G) and Cisco UCS C-Series rack servers or a secondary chassis, then you cannot downgrade to any release earlier than 6.0(1b).
- If your setup includes Cisco Tri-Mode M1 24G RAID (UCSC-RAID-M1L16) controllers on Cisco UCS C240 M8 Servers, then you can not downgrade to any release earlier than 6.0(1b).
- Once you enable any of the following features, then you cannot downgrade to any release earlier than 6.0(1b). You must first disable these features before downgrading to any earlier release:
  - **Fabric Interconnect Audit Log** support using the Linux Audit Framework (auditd) on Cisco UCS 6600, 6500, or 6400 Series Fabric Interconnects
  - iSCSI boot support using Internet Protocol version 6 (IPv6) for Cisco UCS servers
  - Support for AES master key and MACsec (Type-6 [AES], Type-0, and Type-7 encryption) for Ethernet uplink ports on Cisco UCS 6664 Fabric Interconnects and Cisco UCS X-Series Direct (Cisco UCS Fabric Interconnects 9108 100G)
  - Support for ERSPAN on Cisco UCS X-Series Direct (Cisco UCS Fabric Interconnects 9108 100G)

Table 5: Upgrade Paths to Release 6.0(1)

Upgrade from Release	Recommended Upgrade Path
Upgrade from any 4.3(6) release	Direct upgrade or downgrade to release 6.0(1).

Upgrade from Release	Recommended Upgrade Path
Upgrade from any 4.3(5) release	Direct upgrade or downgrade to release 6.0(1).
Upgrade from any 4.3(4) release	Direct upgrade to release 6.0(1). Downgrade: **1.** First downgrade from release 6.0(1) to release 4.3(5). **2.** Downgrade to release 4.3(4).
Upgrade from any 4.3(3) release	Direct upgrade to release 6.0(1). Downgrade: **1.** First downgrade from release 6.0(1) to release 4.3(5). **2.** Downgrade to release 4.3(3).
Upgrade from any 4.3(2) release	Direct upgrade to release 6.0(1). Downgrade: **1.** First downgrade from release 6.0(1) to release 4.3(5). **2.** Downgrade to release 4.3(2).
Upgrade from any 4.2(3) release	Direct upgrade to release 6.0(1). Downgrade: **1.** First downgrade from release 6.0(1) to release 4.3(5). **2.** Downgrade to release 4.2(3).

Upgrade from Release	Recommended Upgrade Path
Any other older release	Upgrade: 1. Upgrade to release 4.2(3) or later. **Note** Refer Release Notes for Cisco UCS Manager, Release 4.2 to identify the recommended upgrade path to release 4.2(3). 2. Download and upgrade to release 6.0(1). Downgrade: 1. First downgrade from release 6.0(1) to release 4.3(5). 2. Downgrade to any other older release. **Note** Refer to the Cisco UCS Manager Release Notes for the specific version you plan to downgrade to.

UCS Manager Health and Pre-Upgrade Check Tool

The UCS Manager Health and Pre-Upgrade Check Tool provides automated health and pre-upgrade checks that are designed to ensure your clusters are healthy before you upgrade. It is imperative that this healthcheck is not just performed, but that you take corrective action on any cluster that is found to be unhealthy. Correct all issues reported by the UCS Manager health check before continuing.

Internal Dependencies

This section explains the interdependencies between Cisco UCS hardware and Cisco UCS Manager versions, including the following considerations:

- Version dependencies for Server FRU items such as DIMMs depend on the server type.
- Chassis items such as fans and power supplies work with all versions of Cisco UCS Manager.

In this release, an interactive compatibility lookup tool is available to help you quickly determine supported combinations of Infrastructure Releases, Fabric Interconnects, servers, VICs, and IOM modules based on the selected release.

Cisco UCS Manager Internal Dependencies Matrix

Full version of the Internal Dependencies tables is also available for reference: Cisco UCS Manager Internal Dependencies, Release 6.0

Cisco UCS NVMeoF Support Matrix for 3rd Party Storage Vendors

Table 6: Cisco UCS NVMeoF Support Matrix for 3rd Party Storage Vendors

Storage Vendor	Feature	Storage Array	Cisco UCS FI	Cisco UCS VIC	Operating System
NetApp Inc.®	NVMe-FC	ONTAP 9.7 onwards	6400 series 6536	1400 14000 15000	ESXi 7.0U3+ ESXi 8.0+ RHEL 8.6+ RHEL 9.0+ SLES 15SP3+
	NVMe-FC	ONTAP 9.13 onwards	UCSX-S9108-100G	15000	ESXi 7.0U3+ ESXi 8.0U2+ RHEL 8.9+ RHEL 9.3+ SLES 15SP4+
	NVMe-FC	ONTAP 9.16 onwards	6664	15000 14000	ESXi 8.0 U3+ ESXi 9.0+ RHEL 9.6+ RHEL 10+ SLES 15SP5+
	NVMe-TCP	ONTAP 9.10 onwards	6400 series 6536	1400 14000 15000	ESXi 7.0U3+ ESXi 8.0+ RHEL 9.0+ SLES 15SP3+
	NVMe-TCP	ONTAP 9.13 onwards	UCSX-S9108-100G	15000	ESXi 7.0U3+ ESXi 8.0U2+ RHEL 9.3+ SLES 15SP4+
	NVMe-TCP	ONTAP 9.16 onwards	6664	15000 14000	ESXi 8.0 U3+ ESXi 9.0+ RHEL 9.6+ RHEL 10+ SLES 15SP5+

Storage Vendor	Feature	Storage Array	Cisco UCS FI	Cisco UCS VIC	Operating System
Note Cisco UCS VIC 1300 series is supported only with RHEL 8.6+. Refer https://hwu.netapp.com/ for latest Storage Array support details. A valid NetApp® account is required to access the compatibility information. Not tested with NetApp E-Series or SolidFIre Storage Models.					

Storage Vendor	Feature	Storage Array	Cisco UCS FI	Cisco UCS VIC	Operating System
Pure Storage, Inc.®	NVMe-FC	Purity//FA 6.1 onwards	6300 6400	1300	RHEL 8.6+
	NVMe-FC	Purity//FA 6.1 onwards	6300 6400 6536	1400 14000 15000	ESXi 7.0U3+ ESXi 8.0+ RHEL 8.6+ RHEL 9.0+ SLES 15SP1+
	NVMe-FC	Purity//FA onwards 6.6.3	UCSX-S9108-100G	15000	ESXi 7.0U3+ RHEL 8.6+ SLES 15SP3+ ESXi 8.0 RHEL 9.0+
	NVMe-FC	Purity//FA onwards 6.8.7	6664	15000 14000	ESXi 8.0 U3+ ESXi 9.0+ RHEL 9.6+ RHEL 10+ SLES 15SP5+
	NVMe-ROCEv2	Purity//FA 5.2 onwards	6300 6400 6536	1400 14000 15000	RHEL 7.2+ RHEL 8.0+ RHEL 9.0+
	NVMe-ROCEv2	Purity//FA 5.2 onwards	6400 6536	1400 14000 15000	ESXi 7.0U3 ESXi 8.0
	NVMe-ROCEv2	Purity//FA onwards 6.6.3	UCSX-S9108-100G	15000	ESXi 7.0U3+ ESXi 8.0U2+ RHEL 8.9+ RHEL 9.3+
	NVMe-ROCEv2	Purity//FA onwards 6.8.7	6664	15000 14000	

Storage Vendor	Feature	Storage Array	Cisco UCS FI	Cisco UCS VIC	Operating System
					ESXi 8.0 U3+ ESXi 9.0+ RHEL 9.6+ RHEL 10+ SLES 15SP5+
	NVMe-TCP	Purity//FA 6.4.2 onwards	6300 6400 6536	1400 14000 15000	ESXi 7.0U3+ RHEL 9.0+ SLES 15SP3+
	NVMe-TCP	Purity//FA onwards 6.6.3	UCSX-S9108-100G	15000	ESXi 7.0U3+ ESXi 8.0U2+ RHEL 8.9+ RHEL 9.3+ SLES 15SP4+
	NVMe-TCP	Purity//FA onwards 6.8.7	6664	15000 14000	ESXi 8.0 U3+ ESXi 9.0+ RHEL 9.6+ RHEL 10+ SLES 15SP5+

Storage Vendor	Feature	Storage Array	Cisco UCS FI	Cisco UCS VIC	Operating System
Dell Inc.®	NVMe-FC	PowerStore PowerMax	6300 6400 6536	1400 14000 15000	ESXi 7.0U3+ RHEL 8.6+ SLES 15SP3+
	NVMe-FC	PowerStore PowerMax	UCSX-S9108-100G	15000	ESXi 7.0U3+ ESXi 8.0U2+ RHEL 8.9+ RHEL 9.3+ SLES 15SP4+
	NVMe-FC	PowerStore PowerMax	6664	15000 14000	ESXi 8.0 U3+ ESXi 9.0+ RHEL 9.6+ RHEL 10+ SLES 15SP5+
	NVMe-TCP	PowerStore PowerMax	6300 6400 6536	1400 14000 15000	ESXi 7.0U3+ RHEL 8.6+ SLES 15SP3+
	NVMe-TCP	PowerStore PowerMax	UCSX-S9108-100G	15000	ESXi 7.0U3+ ESXi 8.0U2+ RHEL 8.9+ RHEL 9.3+ SLES 15SP4+
	NVMe-TCP	PowerStore PowerMax	6664	15000 14000	ESXi 8.0 U3+ ESXi 9.0+ RHEL 9.6+ RHEL 10+ SLES 15SP5+

Storage Vendor	Feature	Storage Array	Cisco UCS FI	Cisco UCS VIC	Operating System
IBM	NVMe-FC	IBM FlashSystem 9500	6400 6500	1400 14000 15000	ESXi 8.0U2 ESXi 7.0U3 RHEL 8.8 RHEL 9.2
		IBM FlashSystem 9200/R	6400 6500	1400 14000 15000	ESXi 8.0U2 ESXi 7.0U3 RHEL 8.8 RHEL 9.2
		IBM FlashSystem 9100	6400 6500	1400 14000 15000	ESXi 8.0U2 ESXi 7.0U3 RHEL 8.8 RHEL 9.2
		IBM FlashSystem 7300	6400 6500	1400 14000 15000	ESXi 8.0U2 ESXi 7.0U3 RHEL 8.8 RHEL 9.2
		IBM FlashSystem 7200/H	6400 6500	1400 14000 15000	ESXi 8.0U2 ESXi 7.0U3 RHEL 8.8 RHEL 9.2
		IBM FlashSystem 5300	6400 6500	1400 14000 15000	ESXi 8.0U2 ESXi 7.0U3 RHEL 8.8 RHEL 9.2
		IBM FlashSystem 5200	6400 6500	1400 14000 15000	ESXi 8.0U2 ESXi 7.0U3 RHEL 8.8 RHEL 9.2
		IBM FlashSystem 5045	6400 6500	1400 14000 15000	

Storage Vendor	Feature	Storage Array	Cisco UCS FI	Cisco UCS VIC	Operating System
					ESXi 8.0U2 ESXi 7.0U3 RHEL 8.8 RHEL 9.2
		IBM FlashSystem 5035	6400 6500	1400 14000 15000	ESXi 8.0U2 ESXi 7.0U3 RHEL 8.8 RHEL 9.2
		IBM FlashSystem 5015	6400 6500	1400 14000 15000	ESXi 8.0U2 ESXi 7.0U3 RHEL 8.8 RHEL 9.2
		IBM SAN Volume Controller SV3	6400 6500	1400 14000 15000	ESXi 8.0U2 ESXi 7.0U3 RHEL 8.8 RHEL 9.2
		IBM SAN Volume Controller SV2	6400 6500	1400 14000 15000	ESXi 8.0U2 ESXi 7.0U3 RHEL 8.8 RHEL 9.2

Note + under **OS Support** column refers to the newer release in that release train.

Cisco UCS FI Appliance Port Support Matrix

Table 7: Cisco UCS FI Appliance Port Support Matrix

Protocol	Vendor	Partner Support	Cisco support	Software version
Nvme-TCP	NetApp Inc.® (ONTAP)	Supported	Supported	ONTAP 9.10 onwards
	DELL EMC®	Supported	Supported	4.3(4) onwards
	Note PowerStore and PowerMax arrays support NVMeoF for TCP and FC.			
	Pure Storage Inc.®	Supported	Supported	4.3(4) onwards
RoceV2	NetApp Inc.® (ONTAP)	Not supported	Not supported	
	Note ROCEv2 is supported with the NetApp E-Series (Tier 2).			
	DELL EMC®	Not supported	Not supported	
	Pure Storage Inc.®	Supported	Supported	
ISCSI	NetApp Inc.® (ONTAP)	Supported	Supported	
	DELL EMC®	Supported	Supported	
	Pure Storage Inc.®	Supported	Supported	

Cisco UCS Fabric Interconnect and Switch Compatibility Matrix

Compatibility and Support Matrix for Cisco Fabric Interconnects and MDS Switches

Table 8: Cisco UCS Fabric Interconnect and MDS Release Support Matrix

Fabric Interconnect	Older Supported Release of MDS	Recommended release of MDS
Cisco UCS 6664 FI	9.2	9.4
Cisco UCS 6536 FI	9.2	9.4
Cisco UCS 6454 FI	9.2	9.4
Cisco UCS 64108 FI	9.2	9.4
Cisco UCS X-Series Direct	-	9.4

Note For older supported release only MDS recommended minor version are supported. See Recommended Releases for Cisco MDS 9000 Series Switches for more information.

Compatibility and Support Matrix for Cisco Fabric Interconnects and Nexus Switches

Table 9: Compatibility and Support Matrix for Cisco Fabric Interconnects & Nexus Switches 6.0(1)

Fabric Interconnect	Older Supported Release of NX-OS	Recommended release of NX-OS
Cisco UCS 6664 FI	—	10.5(x)
Cisco UCS 6536 FI	—	10.5(x)
Cisco UCS 6454 FI	—	10.5(x)
Cisco UCS 64108 FI	—	10.5(x)
Cisco UCS X-Series Direct	—	10.5(x)

Compatibility and Support Matrix for Cisco Fabric Interconnects and Brocade Switches

Table 10: Cisco UCS Fabric Interconnect and Brocade Release Support Matrix

Cisco UCS Fabric Interconnect	Older Supported Release of Brocade	Recommended Release of Brocade
Cisco UCS 6664 FI	—	9.2
Cisco UCS 6536 FI	—	9.2
Cisco UCS 6454 FI	—	9.2
Cisco UCS 64108 FI	—	9.2
Cisco UCS X-Series Direct	—	9.2

Supported Hardware and Software

Supported Operating Systems

For detailed information about supported operating system, see the interactive UCS Hardware and Software Compatibility matrix.

Supported Web Browsers

To access the Cisco UCS Manager GUI, Cisco recommends 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 HTML-5 UI supports one user session per browser.

Default Open Ports

The following table lists the default open ports used in Cisco UCS Manager Release 6.0.

Port	Interface	Protocol	Traffic Type	Fabric Interconnect	Usage
22	CLI	SSH	TCP	UCS 6664 FI UCS 6400 Series FI UCS 6536 FI UCSX-S9108-100G	Cisco UCS Manager CLI access
80	XML	HTTP	TCP	UCS 6664 FI UCS 6400 Series FI UCS 6536 FI UCSX-S9108-100G	Cisco UCS Manager GUI and third party management stations. Client download
443	XML	HTTP	TCP	UCS 6664 FI UCS 6400 Series FI UCS 6536 FI UCSX-S9108-100G	Cisco UCS Manager login page access Cisco UCS Manager XML API access
743	KVM	HTTP	TCP	UCS 6664 FI UCS 6400 Series FI UCS 6536 FI UCSX-S9108-100G	CIMC Web Service / Direct KVM
7546	CFS	CFSD	TCP	UCS 6664 FI UCS 6400 Series FI UCS 6536 FI UCSX-S9108-100G	Cisco Fabric Service

Network Requirements

The *Cisco UCS Manager Administration Management Guide, Release 6.0* provides detailed information about configuring the Intersight Device Connector.

Cisco UCS Central Integration

For the complete list of compatible versions of Cisco UCS Central and Cisco UCS Manager, see *Feature Support Matrix* in Release Notes for Cisco UCS Central.

Supported Platforms in this Release

Release 6.0(1b)

The following servers are supported in this release and continue to receive support in subsequent releases within the same release train:

- Cisco UCS C240 M8 Server
- Cisco UCS C220 M8 Server
- Cisco UCS C225 M8 Server
- Cisco UCS C245 M8 Server
- Cisco UCS X210c M8 Compute Node
- Cisco UCS X215c M8 Compute Node
- Cisco UCS C240 M7 Server
- Cisco UCS C220 M7 Server
- Cisco UCS X410c M7 Compute Node
- Cisco UCS X210c M7 Compute Node
- Cisco UCS C220 M6 Server
- Cisco UCS C240 M6 Server
- Cisco UCS C245 M6 Server
- Cisco UCS C225 M6 Server
- Cisco UCS B200 M6 Server
- Cisco UCS X210c M6 Compute Node
- Cisco UCS B200 M5 Server
- Cisco UCS B480 M5 Server
- Cisco UCS S3260 M5 Server
- Cisco UCS C220 M5 Server
- Cisco UCS C240 M5 Server
- Cisco UCS C240 SD M5 Server

- Cisco UCS C480 M5 Server
- Cisco UCS C480 M5 ML Server
- Cisco UCS C125 M5 Server

Other Hardware

We recommend that you use the latest software version for all Chassis, Fabric Interconnects, Fabric Extenders, Expansion Modules and Power Supplies. To determine the minimum software version for your mixed environment, see Cross-Version Firmware Support, on page 18. The following is the list of other supported hardware:

Supported Hardware for UCS 6600 Series Fabric Interconnects

Table 11: Supported Hardware for UCS 6600 Series Fabric Interconnects

Type	Details
Chassis	Cisco UCSX-9508 Chassis (For Cisco UCS X-Series Servers)
Fabric Interconnects	UCS 6664
Fabric Extenders	93180YC-FX3 (25G server ports) UCSX-I-9108-25G or UCSX-I-9108-100G (Supported with Cisco UCS X-Series Servers)
Power Supplies	UCS-PSU-6600-AC UCSX-PSU-2800AC (For Cisco UCSX-9508 Chassis)

Supported Hardware for UCS 6500 Series Fabric Interconnects

Table 12: Supported Hardware for UCS 6500 Series Fabric Interconnects

Type	Details
Chassis	UCSB-5108-AC2 UCSB-5108-DC2 Cisco UCSX-9508 Chassis (For Cisco UCS X-Series Servers)
Fabric Interconnects	UCS 6500
Fabric Extenders	93180YC-FX3 (25G server ports) 93180YC-FX3 (10G server ports) 2408 UCSX-I-9108-25G or UCSX-I-9108-100G (Supported with Cisco UCS X-Series Servers)

Type	Details
Power Supplies	UCS-PSU-6536-AC UCSX-PSU-2800AC (For Cisco UCSX-9508 Chassis)

Supported Hardware for UCS 6400 Series Fabric Interconnects

Table 13: Supported Hardware for UCS 6400 Series Fabric Interconnects

Type	Details
Chassis	UCSC-C4200-SFF N20–C6508 UCSB-5108-DC UCSB-5108-AC2 UCSB-5108-DC2 UCSB-5108-HVDC Cisco UCSX-9508 Chassis (For Cisco UCS X-Series Servers)
Fabric Interconnects	UCS 64108 UCS 6454
Fabric Extenders	93180YC-FX3 (25G server ports) 93180YC-FX3 (10G server ports) 2408 UCSX-I-9108-25G
Power Supplies	UCS-PSU-6332-AC UCS-PSU-6332-DC UCS-PSU-64108-AC UCS-PSU-6332-DC

Supported Hardware for Cisco UCS X-Series Direct

Table 14: Supported Hardware for Cisco UCS X-Series Direct

Fabric Interconnects	Minimum Software Version	Suggested Software Version
Cisco UCS 9108-100G	4.3(4b)	6.0(1b)

GB Connector Modules, Transceiver Modules, and Cables

Following is the list of Gb connector modules, transceiver modules, and supported cables:

Note

- Transceiver modules and cables that are supported on a specific Fabric Interconnect are not always supported on all VIC adapters, IOMs, or FEXes that are compatible with that Fabric Interconnect. Detailed compatibility matrices for the transceiver modules are available here:https://www.cisco.com/c/en/us/support/interfaces-modules/transceiver-modules/products-device-support-tables-list.html
- S-Class transceivers, for example, QSFP-40G-SR4-S, do not support FCoE.

Table 15: Cisco UCS 6600 Series Fabric Interconnect

Gb Connector Modules	Transceiver Modules and Cables
FC SFP for UCS 6600 Series Fabric Interconnects	DS-SFP-FC16G-SW DS-SFP-FC32G-SW DS-SFP-FC64G-SW DS-SFP-FC16G-LW DS-SFP-FC32G-LW DS-SFP-FC64G-LW
10GbE on Unified Port for UCS 6600 Series Fabric Interconnects	SFP-H10GB-CU1M SFP-H10GB-CU2M SFP-H10GB-CU3M SFP-H10GB-CU5M SFP-H10GB-ACU7M SFP-H10GB-ACU10M SFP-10G-AOC1M SFP-10G-AOC10M
10GbE on 100G port (with QSA) for UCS 6600 Series Fabric Interconnects	SFP-10G-SR SFP-10G-SR-S SFP-10G-LR SFP-10G-LR-S

Gb Connector Modules	Transceiver Modules and Cables
25GbE on Unified Port for UCS 6600 Series Fabric Interconnects	SFP-25G-SR-S SFP-10/25G-LR-S SFP-10/25G-CSR-S SFP-25G-SL SFP-H25G-CU1M SFP-H25G-CU2M SFP-H25G-CU3M SFP-H25G-CU4M SFP-H25G-CU5M SFP-25G-AOC1M SFP-25G-AOC2M SFP-25G-AOC3M SFP-25G-AOC4M SFP-25G-AOC5M SFP-25G-AOC7M SFP-25G-AOC10M
25GbE on 100G port (with QSA28) for UCS 6600 Series Fabric Interconnects	SFP-25G-SR-S SFP-25G-SL
40GbE for UCS 6600 Series Fabric Interconnects	QSFP-40G-SR4 QSFP-40G-SR4-S QSFP-40G-LR4 QSFP-H40G-CU1M QSFP-H40G-CU3M QSFP-H40G-CU5M QSFP-H40G-ACU7M QSFP-H40G-AOC3M QSFP-H40G-AOC5M QSFP-H40G-AOC7M QSFP-H40G-AOC15M QSFP-H40G-AOC20M QSFP-H40G-AOC25M QSFP-H40G-AOC30M CVR-QSFP-SFP10G

Gb Connector Modules	Transceiver Modules and Cables
100GbE for UCS 6600 Series Fabric Interconnects	QSFP-100G-SR4-S QSFP-100G-PSM4-S QSFP-100G-SM-SR QSFP-100G-SL4 QSFP-40/100-SRBD QSFP-100G-DR-S QSFP-100G-FR-S QSFP-100G-SR1.2 QSFP-100G-CU1M QSFP-100G-CU2M QSFP-100G-CU3M QSFP-100G-CU5M QSFP-100G-AOC1M QSFP-100G-AOC2M QSFP-100G-AOC3M QSFP-100G-AOC5M QSFP-100G-AOC7M QSFP-100G-AOC10M QSFP-100G-AOC15M QSFP-100G-AOC20M QSFP-100G-AOC25M QSFP-100G-AOC30M

Table 16: Cisco UCS 6500 Series Fabric Interconnects

Gb Connector Modules	Transceiver Modules and Cables
FC for UCS 6500 Series Fabric Interconnects	DS-SFP-4X32G-SW
1GbE for UCS 6500 Series Fabric Interconnects	GLC-TE (QSA), port 9, 10 GLC-SX-MMD (QSA)

Gb Connector Modules	Transceiver Modules and Cables
10GbE for UCS 6500 Series Fabric Interconnects	SFP-10G-SR (QSA) SFP-10G-SR-S(QSA) SFP-10G-LR (QSA) SFP-10G-LR-S (QSA) CVR-QSFP-SFP10G SFP-H10GB-CU1M
25GbE for UCS 6500 Series Fabric Interconnects	SFP-10/25G-LR-S SFP-10/25G-CSR-S SFP-25G-SL CVR-QSFP28-SFP25G SFP-H25G-CU1M (P1) SFP-H25G-CU2M (P1) SFP-H25GB-CU3M SFP-25G-AOC2M SFP-25G-AOC3M SFP-25G-SR-S

Gb Connector Modules	Transceiver Modules and Cables
40GbE for UCS 6500 Series Fabric Interconnects	QSFP-H40G-AOC1M QSFP-H40G-AOC2M QSFP-H40G-AOC3M QSFP-H40G-AOC5M QSFP-H40G-AOC15M QSFP-H40G-AOC25M QSFP-40G-CU1M QSFP-40G-CU2M QSFP-40G-CU3M QSFP-40G-CU5M QSFP-40G-SR4 QSFP-40G-SR4-S QSFP-40G-CSR4 QSFP-40G-LR4 QSFP-40G-LR4-S QSFP-4SFP10G-CU1M QSFP-4SFP10G-CU3M FET-40G **Note** FET-40G is supported only between FI and IOM/FEX QSFP-40G-ACU10M QSFP-40G-SR-BD QSFP-100G40G-BIDI **Note** QSFP-100G40G-BIDI is supported only on border ports/uplink ports in 40G mode.

Gb Connector Modules	Transceiver Modules and Cables
100GbE for UCS 6500 Series Fabric Interconnects	QSFP-100G-SR1.2 QSFP-100G-SR4-S QSFP-100G-LR4-S QSFP-100G-SM-SR QSFP-100G-SL4 QSFP-40/100-SRBD (or) QSFP-100G40G-BIDI **Note** QSFP-100G40G-BIDI is supported between FI and I9108-100G IOM/N9K-C93180YC-FX3 FEX/border ports in 100G mode. QSFP-100G-CU1M QSFP-100G-CU2M QSFP-100G-CU3M QSFP-100G-CU5M QSFP-4SFP25G-CU1M QSFP-4SFP25G-CU2M QSFP-4SFP25G-CU3M QSFP-4SFP25G-CU5M QSFP-100G-AOC1M QSFP-100G-AOC2M QSFP-100G-AOC3M QSFP-100G-AOC5M QSFP-100G-AOC7M QSFP-100G-AOC10M QSFP-100G-AOC15M QSFP-100G-AOC20M QSFP-100G-AOC25M QSFP-100G-AOC30M QSFP-100G-DR-S QSFP-100G-FR-S

Table 17: Cisco UCS 6400 Series Fabric Interconnects

Gb Connector Modules	Transceiver Modules and Cables
FC for UCS 6400 Series Fabric Interconnects	DS-SFP-FC8G-SW DS-SFP-FC8G-LW DS-SFP-FC16G-SW DS-SFP-FC16G-LW DS-SFP-FC32G-SW DS-SFP-FC32G-LW
100-Gb for UCS 6400 Series Fabric Interconnects	QSFP-100G-SR1.2 QSFP-40/100G-SRBD QSFP-100G-SR4-S QSFP-100G-LR4-S QSFP-100G-SM-SR QSFP-100G-CU1M QSFP-100G-CU2M QSFP-100G-CU3M QSFP-100G-AOC1M QSFP-100G-AOC2M QSFP-100G-AOC3M QSFP-100G-AOC5M QSFP-100G-AOC7M QSFP-100G-AOC10M QSFP-100G-AOC15M QSFP-100G-AOC20M QSFP-100G-AOC25M QSFP-100G-AOC30M QSFP-4SFP25G-CU1M QSFP-4SFP25G-CU2M QSFP-4SFP25G-CU3M QSFP-4SFP25G-CU5M

Gb Connector Modules	Transceiver Modules and Cables
40-Gb for UCS 6400 Series Fabric Interconnects	QSFP-40G-SR4 QSFP-40G-SR4-S QSFP-40G-SR-BD QSFP-40G-LR4 QSFP-40G-LR4-S QSFP-40G-ER4 WSP-Q40GLR4L QSFP-H40G-CU1M QSFP-H40G-CU3M QSFP-H40G-CU5M QSFP-H40G-ACU7M QSFP-H40G-ACU10M QSFP-H40G-AOC1M QSFP-H40G-AOC2M QSFP-H40G-AOC3M QSFP-H40G-AOC5M QSFP-H40G-AOC10M QSFP-H40G-AOC15M QSFP-4SFP10G-CU1M QSFP-4SFP10G-CU3M QSFP-4SFP10G-CU5M QSFP-4X10G-AC7M QSFP-4X10G-AC10M QSFP-4X10G-AOC1M QSFP-4X10G-AOC3M QSFP-4X10G-AOC5M QSFP-4X10G-AOC7M
32-Gb FC for UCS 6454 Fabric Interconnects	DS-SFP-FC32G-SW DS-SFP-FC32G-LW
25-Gb for UCS 6454 Fabric Interconnects	4x25GbE 10M[1]

Gb Connector Modules	Transceiver Modules and Cables
25-Gb for UCS 6400 Series Fabric Interconnects	SFP-25G-SR-S SFP-H25G-CU1M SFP-H25G-CU2M SFP-H25G-CU3M SFP-H25G-CU5M SFP-H25G-AOC1M SFP-H25G-AOC2M SFP-H25G-AOC3M SFP-H25G-AOC5M SFP-H25G-AOC7M SFP-H25G-AOC10M SFP-10/25G-LR-S SFP-10/25G-CSR-S
16-Gb for UCS 6454 Fabric Interconnects	DS-SFP-FC16G-LW DS-SFP-FC16G-SW

Gb Connector Modules	Transceiver Modules and Cables
10-Gb for UCS 6400 Series Fabric Interconnects	SFP-10G-SR SFP-10G-SR-S SFP-10G-LR SFP-10G-LR-S SFP-10G-ER SFP-10G-ER-S SFP-10G-ZR SFP-10G-ZR-S FET-10G **Note** FET-10G is only supported between Fabric Interconnects and IOMs/FEXs. SFP-10G-LRM SFP-H10GB-CU1M SFP-H10GB-CU2M SFP-H10GB-CU3M SFP-H10GB-CU5M SFP-H10GB-ACU7M SFP-H10GB-ACU10M SFP-10G-AOC1M SFP-10G-AOC2M SFP-10G-AOC3M SFP-10G-AOC5M SFP-10G-AOC7M SFP-10G-AOC10M
8-Gb FC for UCS 6400 Series Fabric Interconnects	DS-SFP-FC8G-SW DS-SFP-FC8G-LW
1-Gb for UCS 6400 Series Fabric Interconnects	GLC-TE GLC-SX-MMD SFP-GE-T

[1] Supported from Cisco UCS Manager, Release 4.1(2)

Table 18: Cisco UCS X-Series Direct Supported Gb Connector Modules

Gb Connector Modules	Cables
100-GbE	QSFP-100G-SR4-S QSFP-100G-SR4-S (Breakout) QSFP-100G-LR4-S QSFP-100G-SM-SR QSFP-100G-SL4 QSFP-100G-SL4 (Breakout) QSFP-100G-SR1.2 QSFP-40/100-SRBD QSFP-100G-DR-S QSFP-100G-FR-S QSFP-100G-CU1M QSFP-100G-CU2M QSFP-100G-CU3M QSFP-100G-CU5M QSFP-100G-AOC1M QSFP-100G-AOC2M QSFP-100G-AOC3M QSFP-100G-AOC5M QSFP-100G-AOC7M QSFP-100G-AOC10M QSFP-100G-AOC15M QSFP-100G-AOC20M QSFP-100G-AOC25M QSFP-100G-AOC30M
40GbE	QSFP-40G-SR4 QSFP-40G-SR4 (Breakout) QSFP-40G-SR4-S QSFP-40G-SR4-S (Breakout) QSFP-40G-CSR4 QSFP-40G-CSR4 (Breakout) QSFP-40G-SR-BD

Gb Connector Modules	Cables
4X25GbE	QSFP-4SFP25G-CU1M QSFP-4SFP25G-CU2M QSFP-4SFP25G-CU3M QSFP-4SFP25G-CU5M
4x10GbE	QSFP-4SFP10G-CU1M QSFP-4SFP10G-CU2M QSFP-4SFP10G-CU3M QSFP-4X10G-AOC3M QSFP-4X10G-AOC5M
25GbE via QSA28	SFP-25G-SR-S SFP-10/25G-LR-S SFP-10/25G-CSR-S SFP-25G-SL SFP-H25G-CU1M SFP-H25G-CU2M SFP-H25G-CU3M SFP-H25G-CU5M
10GbE/1GbE via QSA or QSA28	SFP-10G-SR SFP-10G-SR SFP-10G-SR-S SFP-10G-LR (With QSA) SFP-10G-LR SFP-10G-LR-S SFP-10G-LR-S CVR-QSFP-SFP10G+ GLC-T (ports 7, 8) CVR-QSFP-SFP28+ GLC-T (ports 7, 8)
8G, 16G, 32G FC	4x 8G FC breakout with 128G QSF 4x 16G FC breakoutwith 128G QSFP 4x 32G FC breakoutwith 128G QSFP

Supported GPU/GPU PCIe Node

Table 19: Supported GPU/GPU PCIe Node

GPU/GPU PCIe Node	PID	Supported Servers	Minimum Software Version	Suggested Software Version
NVIDIA A16 GPU on X440p: PCIE 250W 4X16GB, FHFL	UCSX-GPU-A16	Cisco UCS X210c M8 (with PCIe Node)	4.3(6a)	6.0(1b)
	UCSC-CGPU-A16	Cisco UCSX215c M8 (with PCIe Node)	4.3(5a)	6.0(1b)
AMD MI210 GPU; 300W 64GB, 2 slot FHFL	UCSX-GPU-MI210	Cisco UCS X215c M8	4.3(6a)	6.0(1b)
NVIDIA H100-NVL GPU 400W, 94GB, 2-slot FHFL	UCSX-GPU-H100-NVL	Cisco UCS X210c M8 (with PCIe Node)	4.3(6a)	6.0(1b)
	UCSC-GPU-H100-NVL	Cisco UCS C240 M8	4.3(6a)	6.0(1b)
		Cisco UCS X210c M7 Cisco UCS X215c M8 (with PCIe Node)	4.3(5a)	6.0(1b)
		Cisco UCS C245 M8	4.3(5a)	6.0(1b)
		Cisco UCS C240 M7	4.3(5a)	6.0(1b)
NVIDIA L4-Mezz GPU 70W, 24GB, 1-slot HHHL	UCSX-GPU-L4-Mezz	Cisco UCS X210c M7 Cisco UCS X215c M8	4.3(5a)	6.0(1b)
UCSX-440P-D GPU PCIe Node	UCSX-440P-D	Cisco UCS X210c M7, X210c M6, and X410c M7	4.3(4a)	6.0(1b)
Intel GPU Flex 140, Gen4x8, HHHL, 75W PCIe (Front Mezz)	UCSX-GPU-FLX140MZ	Cisco UCS X210c M7	4.3(2b)	6.0(1b)

GPU/GPU PCIe Node	PID	Supported Servers	Minimum Software Version	Suggested Software Version
Intel GPU Flex 140, Gen4x8, HHHL, 75W PCIe	UCSX-GPU-FLEX140	Cisco UCS X410c M7 and X210c M7 (with PCIe Node)	4.3(4a)	6.0(1b)
	UCSC-GPU-FLEX140	Cisco UCS C220 M7 and C240 M7	4.3(4a)	6.0(1b)
Intel GPU Flex 170, Gen4x16, HHFL, 150W PCIe	UCSX-GPU-FLEX170	Cisco UCS X410c M7 and X210c M7 (with PCIe Node)	4.3(4a)	6.0(1b)
	UCSC-GPU-FLEX170	Cisco UCS C240 M7	4.3(4a)	6.0(1b)
NVIDIA TESLA A16 PCIE 250W 4X16GB	UCSX-GPU-A16-D	Cisco UCS X210c M7 and X210c M6 (with PCIe Node)	4.3(4a)	6.0(1b)
		Cisco UCS X410c M7 (with PCIe Node)	4.3(4a)	6.0(1b)
	UCSC-GPU-A16	Cisco UCS C240 M8	4.3(6a)	6.0(1b)
		Cisco UCS C240 M6	4.2(1d)	6.0(1b)
		Cisco UCS C245 M6	4.2(1i)	6.0(1b)
NVIDIA L4 Tensor Core, 70W, 24GB	UCSX-GPU-L4	Cisco UCS X210c M8 (with PCIe Node)	4.3(6a)	6.0(1b)
		Cisco UCS X210c M7 (with PCIe Node)	4.3(4a)	6.0(1b)
		Cisco UCS X410c M7 (with PCIe Node)	4.3(4a)	6.0(1b)

GPU/GPU PCIe Node	PID	Supported Servers	Minimum Software Version	Suggested Software Version
NVIDIA L40 300W, 48GB wPWR CBL	UCSX-GPU-L40	Cisco UCS X210c M7 (with PCIe Node)	4.3(4a)	6.0(1b)
		Cisco UCS X410c M7 (with PCIe Node)	4.3(4a)	6.0(1b)
	UCSC-GPU-L40	Cisco UCS C240 M7	4.3(2b)	6.0(1b)
		Cisco UCS X215c M8 (with PCIe Node)	4.3(5a)	6.0(1b)
NVIDIA L40S: 350W, 48GB, 2-slot FHFL GPU	UCSX-GPU-L40S	Cisco UCS X210c M8 (with PCIe Node)	4.3(6a)	6.0(1b)
		Cisco UCS X210c M7 (with PCIe Node) Cisco UCS X410c M7 (with PCIe Node)	4.3(4a)	
	UCSC-GPU-L40S	Cisco UCS C240 M8	4.3(6a)	6.0(1b)
		Cisco UCS C240 M7	4.3(4a)	6.0(1b)
		Cisco UCS X215c M8 (with PCIe Node)	4.3(5a)	6.0(1b)

GPU/GPU PCIe Node	PID	Supported Servers	Minimum Software Version	Suggested Software Version
NVIDIA T4 PCIE 75W 16GB	UCSX-GPU-T4-16	Cisco UCS X210c M6 (with PCIe Node)	4.3(4a)	6.0(1b)
	UCSC-GPU-T4-16	Cisco UCS C220 M6	4.3(2b)	6.0(1b)
		Cisco UCS C245 M6	4.2(1f)	6.0(1b)
		Cisco UCS C225 M6	4.2(1l)	6.0(1b)
		Cisco UCS C240 M5, C220 M5, and C480 M5	3.2(3a)	6.0(1b)
		Cisco UCS S3260 M5	3.1(2b)	6.0(1b)
NVIDIA T4 GPU PCIE 75W 16GB, MEZZ form factor (Front Mezz)	UCSX-GPU-T4-MEZZ	Cisco UCS X210c M7 and X210c M6	4.3(2b)	6.0(1b)
NVIDIA Hopper L4 70W, 24GB, 1-slot HHHL	UCSC-GPU-L4M6	Cisco UCS C220 M6, C240 M6	4.3(4a)	6.0(1b)
NVIDIA H100: 350W, 80GB, 2-slot FHFL GPU	UCSX-GPU-H100-80	Cisco UCS X210c M7 and X410c M7 (with PCIe Node)	4.3(4a)	6.0(1b)
	UCSC-GPU-H100-80	Cisco UCS C240 M7	4.3(4a)	6.0(1b)
NVIDIA L4:70W, 24GB, 1-slot HHHL GPU	UCSC-GPU-L4	Cisco UCS C240 M8 and C220 M8	4.3(6a)	6.0(1b)
		Cisco UCS C245 M8	4.3(5a)	6.0(1b)
		Cisco UCS C220 M7 and C240 M7	4.3(2b)	6.0(1b)
		Cisco UCS X215c M8 (with PCIe Node)	4.3(5a)	6.0(1b)
NVIDIA P4	UCSC-GPU-P4	Cisco UCS C220 M5	3.2(3a)	6.0(1b)

GPU/GPU PCIe Node	PID	Supported Servers	Minimum Software Version	Suggested Software Version
NVIDIA M10	UCSC-GPU-M10	Cisco UCS C240 M5 and C480 M5	3.2(3a)	6.0(1b)
NVIDIA GRID P6 Front Mezzanine	UCSB-GPU-P6-F	Cisco UCS B200 M5	3.2(1d)	6.0(1b)
		Cisco UCS B480 M5	3.2(2b)	6.0(1b)
NVIDIA GRID P6 Rear Mezzanine	UCSB-GPU-P6-R	Cisco UCS B200 M5	3.2(1d)	6.0(1b)
		Cisco UCS B480 M5	3.2(2b)	6.0(1b)
TESLA A30, PASSIVE, 180W, 24GB	UCSC-GPU-A30-D	Cisco UCS C240 M7	4.3(2b)	6.0(1b)
	UCSC-GPU-A30	Cisco UCS C240 M6	4.2(1d)	6.0(1b)
		Cisco UCS C245 M6	4.2(1i)	6.0(1b)
TESLA A40 RTX, PASSIVE, 300W, 48GB	UCSX-GPU-A40-D	Cisco UCS X210c M7 and X210c M6 (with PCIe Node)	4.3(4a)	6.0(1b)
		Cisco UCS X410c M7 (with PCIe Node)	4.3(4a)	6.0(1b)
	UCSC-GPU-A40-D	Cisco UCS C240 M7	4.3(2b)	6.0(1b)
	UCSC-GPU-A40	Cisco UCS C240 M6	4.2(1d)	6.0(1b)
		Cisco UCS C245 M6	4.2(1i)	6.0(1b)
		Cisco UCS C480 M5	3.2(3a)	6.0(1b)

GPU/GPU PCIe Node	PID	Supported Servers	Minimum Software Version	Suggested Software Version
TESLA A100, PASSIVE, 300W, 80GB12	UCSX-GPU-A100-80-D	Cisco UCS X210c M7 and X210c M6 (with PCIe Node)	4.3(4a)	6.0(1b)
		Cisco UCS X410c M7 (with PCIe Node)	4.3(4a)	6.0(1b)
	UCSC-GPUA100-80-D	Cisco UCS C240 M7	4.3(2b)	6.0(1b)
	UCSC-GPU-A100-80	Cisco UCS C240 M6	4.2(1d)	6.0(1b)
		Cisco UCS C245 M6	4.2(1i)	6.0(1b)
		All Cisco UCS C-Series M5	4.2(2c)	6.0(1b)
TESLA A10, PASSIVE, 150W, 24GB	UCSC-GPU-A10	Cisco UCS C240 M6	4.2(1d)	6.0(1b)
		Cisco UCS C245 M6	4.2(1i)	6.0(1b)
NVIDIA H200-NVL GPU	UCSC-GPU-H200-NVL	Cisco UCS C240 M8	4.3(6c)	6.0(1b)

Deprecated Hardware and Software in Cisco UCS Manager

Release 6.0(1b)

Beginning with Cisco UCS Manager Release 6.0(1b), the following hardware are no longer supported:

- Cisco UCS FI Models:
  - UCS-FI-6300-E6U16
  - UCS-FI-6300-E6-16UP
  - UCS-FI-6332-16UP
  - UCS-FI-6332
  - UCS-FI-M-6324
- IOM Models:
  - UCS-IOM-2208XP
  - UCS-IOM-2204XP

- UCS-IOM-2304
- UCS-IOM-2304V2

- FEX Models:
  - N2K-C2248TP-1GE
  - N2K-C2248T-1GE
  - N2K-C2148T-1GE
  - N2K-C2232PP-10GE
  - N2K-C2232TM-10GE
  - N2K-C2232TM-E-10GE
  - N2K-C2348UPQ-10GE

Capability Catalog

The Cisco UCS Manager Capability Catalog is a set of tunable parameters, strings, and rules. Cisco UCS uses the catalog to update the display and configurability of components such as newly qualified DIMMs and disk drives for servers.

The Capability Catalog is embedded in Cisco UCS Manager, but at times it is also released as a single image file to make updates easier.

The following table lists the PIDs added in this release and maps UCS software releases to the corresponding Capability Catalog file.

Table 20: Version Mapping

UCS Release	Catalog File Name	Additional PIDs in this Release
6.0(1b)	ucs-catalog.6.0.1c.T.bin	Cisco UCS Fabric Interconnect and Components: • FI: UCS-FI-6664-U • PSU and fan: UCS-PSU-6600-AC, UCS-FAN-6664 • Accessory and blank: UCS-ACC-6664 Controller: • UCSX-X10C-PTE3

Related Resources

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

- Release Bundle Contents for Cisco UCS Software
- Cisco UCS C-series Rack Server Integration Guides
- Cisco UCS C-series Software Release Notes
- Release Notes for Cisco Intersight Infrastructure Firmware
- Release Notes for Cisco UCS Central
- Cisco UCS Manager Upgrade/Downgrade Support Matrix Tool
- Cisco UCS Equivalency Matrix for Cisco Intersight, Cisco IMC, and Cisco UCS Manager Tool
- Cisco UCS Manager Internal Dependencies Matrix Tool
- Cisco UCS Manager Internal Dependencies, Release 6.0
- Cisco UCS Manager Cross Version Firmware Matrix Tool
- Cisco UCS Manager Cross-Version Firmware Support, Release 6.0