Release Notes for Cisco UCS E-Series M6 Servers, Release 4.15.x

First Published: 2024-09-27

Last Modified: 2025-08-28

Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright $^{©}$ 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Release Notes for Cisco UCS E-Series M6 Servers, Release 4.15.x

Overview

The Cisco UCS E-Series M6 Servers are size-, weight-, and power-efficient blade servers that can be housed within the Cisco Catalyst 8300 Series Edge platforms. These servers provide a general-purpose compute platform for branch-office applications deployed either as bare-metal on operating systems, such as Linux, or as virtual machines on hypervisors, such as VMware vSphere Hypervisor.

The Cisco UCS E-Series M6 Servers are available in the following form-factors:

- UCS-E1100D-M6: Double-wide service module, 10-cores CPU, 3.0 -GHz clock speed

System Requirements

The following system requirements apply to the UCS E-Series M6 Servers:

Hardware Requirements

Note The UCS E-Series M6 Servers can be installed in the following Cisco Catalyst 8300 Series Edge platforms:

- C8300-2N2S-4T2X

- C8300-2N2S-6T

The following E-Series M6 Servers are supported:

- UCS-E1100D-M6

Note For details about the E-Series M6 Servers, see the "Hardware Requirements" section in the Hardware Installation Guide for Cisco UCS E-Series M6 Servers .

Software Requirements

The UCS E-Series M6 Servers require three major software systems:

CIMC Firmware

Cisco Integrated Management Controller (CIMC) is a management module, which is built into the motherboard. A dedicated processor, separate from the main server CPU, runs the CIMC firmware. CIMC is the management service for the UCS E-Series M6 Servers. You can use CIMC to access, configure, administer, and monitor the server.

The system ships with a running version of the CIMC firmware. You can update the CIMC firmware, but no initial installation is needed.

✎

Note   The table below lists the minimum CIMC versions required for the UCS E-Series M6 Servers.

Table 1: Minimum CIMC Versions Required

Server Name	CIMC Version
UCS-E1100D-M6	4.11.1

BIOS Firmware

BIOS initializes the hardware in the system, discovers bootable devices, and boots them in the provided sequence. It boots the operating system and configures the hardware for the operating system to use. BIOS manageability features allow you to interact with the hardware and use it. In addition, BIOS provides options to configure the system, manage firmware, and create BIOS error reports.

The system ships with a running version of the BIOS firmware. You can update the BIOS firmware, but no initial installation is needed.

Operating System or Hypervisor

The main server CPU runs on an operating system, or a hypervisor. You can purchase an E-Series M6 Server with a preinstalled hypervisor.

The following table lists the supported hypervisors for CIMC releases:

Table 2: Supported Hypervisors for CIMC Releases

Release	Supported Hypervisors
4.15.1	VMware ESXi 7.0U3g RHEL 8.3
4.15.2	VMware ESXi 7.0U3g ESXI 8.0U2

GUI Requirements

The UCS E-Series M6 servers GUI is supported on the following browsers:

- Google Chrome
- Microsoft Edge
- Mozilla Firefox
- Safari

Upgrading to a New Software Release

To upgrade the BIOS or CIMC image on your UCS E-Series M6 server, obtain the package (image) from https://software.cisco.com/download/home, and follow the instructions in chapter "*Firmware Management*" in the CLI Configuration Guide for UCS E-Series M6 Servers.

Cisco Catalyst 8300 Series Edge Platforms, E-Series M6 Server, and Cisco IOS-XE Software Release Compatibility

Table 3: Minimum Release Compatibility for Cisco Catalyst 8300 Series Edge Platforms, E-Series M6 Server, CIMC, Cisco SD-WAN, and Cisco IOS-XE Software

Cisco Catalyst 8300 Series	UCS E-Series M6 Server(s)	Cisco IOS-XE Software Release	CISCO SD-WAN Release	CIMC
C8300-2N2S-4T2X	UCS-E1100D-M6	Cisco IOS-XE 17.11.1a	Cisco SD-WAN Release 20.11.1	4.11.1
C8300-2N2S-6T	UCS-E1100D-M6	Cisco IOS-XE 17.11.1a	Cisco SD-WAN Release 20.11.1	4.11.1

New Features for CIMC Release 4.15.1

There are no new features in this release.

> **Note** Documentation is sometimes updated after original publication; therefore, for updated content, review the documentation on Cisco.com.

Resolved and Open Bugs

Access the Bug Search tool at Bug Search Tool. Enter the bug identifier in the **Search For** field, and then press **Enter**.

Open Bugs in Release 4.15.2

There are no open bugs in this release.

Resolved Bugs in Release 4.15.2

The table below lists the bugs that are resolved in release 4.15.2.

Bug ID	Description
CSCwo77400	UCSE M6: The vKVM login page uses a URL parameter for redirection.
CSCwm28576	M6: The size of the `nohup.out` file continues to grow.
CSCwm14253	The VMD Enable option should be configurable through both the CIMC CLI and GUI.
CSCwo65440	M6: Implement a CLI command to display the hardware version.

Bug ID	Description
CSCwn09356	TABEI-M: FAN failures are not being reported in CIMC.

Open Bugs in Release 4.15.1

There are no open bugs in this release.

Resolved Bugs in Release 4.15.1

The table below lists the bugs that are resolved in release 4.15.1:

Bug ID	Description
CSCwh53326	Last reboot reason after bios active is 'Hard reset' instead of 'Flash Reset'.
CSCwi29799	Cisco Integrated Management Controller Command Injection Vulnerability for UCS E-Series M6.
CSCwi36034	TabeiM: PSU1 name is not showing for **show psu info** command.
CSCwi06421	Image mapping failed through CIFS on CIMC Vmedia mapping.
CSCwi18006	NFVIS ISO image is not unmapped after NFVIS installation is done
CSCwi42996	UCSE-M6 Cisco IMC Web-Based Management Interface Command Injection Vulnerability.

Related Documentation

For more information, see the following Cisco UCS E-Series M6 Server documents:

- Hardware Installation Guide for Cisco UCS E-Series M6 Servers

- CLI Configuration Guide for Cisco UCS E-Series M6 Servers

- GUI Configuration Guide for Cisco UCS E-Series M6 Servers

- Cisco Network Modules, Server Modules, and Interface Cards Regulatory Compliance and Safety Information

- Troubleshooting Guide for Cisco UCS E-Series M6 Servers

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.

- To get the business results you're looking for with the technologies that matter, visit Cisco Services.

- To submit a service request, visit Cisco Support.

- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco DevNet.

- To obtain general networking, training, and certification titles, visit Cisco Press.

• To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

Troubleshooting

For the most up-to-date, detailed troubleshooting information, see the Cisco TAC website at https://www.cisco.com/en/US/support/index.html.

Go to **Products by Category** and choose your product from the list, or enter the name of your product. Look under **Troubleshoot and Alerts** to find information for the issue that you are experiencing.