Cisco Unified Computing System (UCS), version 4.0(4b)

Common Criteria Operational User Guidance and Preparative Procedures

Version 2.0

12 December 2019

EDCS-16371159

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Table of Contents

DOCUMENT INTRODUCTION

This document provides supporting evidence for an evaluation of a specific Target of Evaluation (TOE), the Cisco Unified Computing System with Cisco UCS Manager, version 4.0 (4b). This Operational User Guidance with Preparative Procedures addresses the administration of the TOE software and hardware and describes how to install, configure, and maintain the TOE in the Common Criteria evaluated configuration.

1. Introduction

This Operational User Guidance with Preparative Procedures documents the administration of the Cisco Unified Computing System with Cisco UCS Manager, version 4.0(4b) TOE certified under Common Criteria.

1.1. Audience

This document is written for administrators configuring the TOE. This document assumes that you are familiar with the basic concepts and terminologies used in internetworking, and understand your network topology and the protocols that the devices in your network can use, that you are a trusted individual, and that you are trained to use the operating systems on which you are running your network.

1.2. Purpose

This document is the Operational User Guidance with Preparative Procedures for the Common Criteria evaluation. It was written to highlight the specific TOE configuration and administrator functions and interfaces that are necessary to configure and maintain the TOE in the evaluated configuration. This document is not meant to detail specific actions performed by the administrator but rather is a road map for identifying the appropriate locations within Cisco documentation to get the specific details for configuring and maintaining UCS operations.

1.3. Document References

This document makes reference to several Cisco Systems documents. The documents used are shown below.

Link to all configuration guides: http://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-manager/products-installation-and-configuration-guides-list.html

Table 1: Document References

	UCS Manager
[1]	Cisco UCS **Site Preparation** Guide http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/hw/site-prep-guide/ucs_site_prep.pdf
[2]	**Release Notes** for Cisco UCS Manager, Release 4.0 https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/release/notes/CiscoUCSManager-RN-4-0.html
[3]	Cisco UCS Manager **Getting Started** Guide, Release 4.0 https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/GUI-User-Guides/Getting-Started/4-0/b_UCSM_Getting_Started_Guide_4_0.html
[4]	Cisco UCS Manager **Administration Management** Guide 4.0 https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/GUI-User-Guides/Admin-Management/4-0/b_Cisco_UCS_Admin_Mgmt_Guide_4-0.html Cisco UCS Manager **Administration Management Using the CLI**, Release 4.0

	https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/CLI-User-Guides/Admin-Management/4-0/b_Cisco_UCS_Manager_CLI_Administration_Mgmt_Guide_4-0.html
[5]	Cisco UCS Manager **Firmware Management** Guide, Release 4.0 https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/GUI-User-Guides/Firmware-Mgmt/4-0/b_UCSM_GUI_Firmware_Management_Guide_4-0.html Cisco UCS Manager **Firmware Management Using the CLI**, Release 4.0 https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/CLI-User-Guides/Firmware-Mgmt/4-0/b_UCSM_CLI_Firmware_Management_Guide_4-0.html
[6]	Cisco UCS Manager **Infrastructure Management** Guide, Release 4.0 https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/GUI-User-Guides/Infrastructure-Mgmt/4-0/b_UCSM_GUI_Infrastructure_Management_Guide_4_0.html Cisco UCS Manager **Infrastructure Management Using the CLI**, Release 4.0 https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/CLI-User-Guides/Infrastructure-Mgmt/4-0/b_UCSM_CLI_Infrastructure_Management_Guide_4_0.html
[7]	Cisco UCS Manager **Network Management** Guide, Release 4.0 https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/GUI-User-Guides/Getting-Started/4-0/b_UCSM_Getting_Started_Guide_4_0.htmlCisco UCS Manager **Network Management Guide Using the CLI**, Release 4.0 https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/CLI-User-Guides/Network-Mgmt/4-0/b_CLI_UCSM_Network_Management_Guide_4_0.html
[8]	Cisco UCS Manager **Server Management** Guide, Release 4.0 https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/GUI-User-Guides/Server-Mgmt/4-0/b_Cisco_UCS_Manager_Server_Mgmt_Guide_4_0.html Cisco UCS Manager **Server Management Using the CLI**, Release 4.0 https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/CLI-User-Guides/Server-Mgmt/4-0/b_Cisco_UCS_Manager_Server_Mgmt_CLI_Guide_4_0.html
[9]	Cisco UCS Manager **Storage Management** Guide, Release 4.0 https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/GUI-User-Guides/Storage-Mgmt/4-0/b_UCSM_GUI_Storage_Management_Guide_4_0.html Cisco UCS Manager **Storage Management Guide using the CLI**, Release 4.0 https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/CLI-User-Guides/Storage-Mgmt/4-0/b_CLI_UCSM_Storage_Management_Guide_4_0.html
[10]	Cisco UCS Manager **System Monitoring** Guide, Release 4.0 https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/GUI-User-Guides/System-Monitoring/4-0/b_UCSM_GUI_System_Monitoring_Guide_4-0.html Cisco UCS Manager **System Monitoring Guide Using the CLI**, Release 4.0

	https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/CLI-User-Guides/System-Monitoring/4-0/b_UCSM_CLI_System_Monitoring_Guide_4-0.html
	Fabric Interconnect
[11]	Cisco UCS **6454** Fabric Interconnect Hardware Installation Guide https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/hw/6454-install-guide/6454/6454_chapter_0111.html Cisco UCS **6300 Series** Fabric Interconnect Hardware Installation Guide https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/hw/6300-install-guide/6300_Series_HIG/6300_Series_HIG_chapter_01.html
	B-Series Servers
[12]	Cisco UCS **B-Series Blade Servers**: Install and Upgrade Guides http://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-b-series-blade-servers/products-installation-guides-list.html
	C-Series Servers
[13]	Cisco UCS **C-Series Rack Servers**: Install and Upgrade Guides http://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-c-series-rack-servers/products-installation-guides-list.html
	Troubleshooting and Other References
[14]	Cisco UCS Manager **Troubleshooting** Reference Guide https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ts/guide/UCSTroubleshooting.html
[15]	Cisco UCS Manager **XML API** Programmer's Guide https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/api/b_ucs_api_book.html
[16]	**Intelligent Platform Management Interface** Specification Second Generation v2.0 http://www.intel.com/content/dam/www/public/us/en/documents/product-briefs/second-gen-interface-spec-v2.pdf
[17]	Cisco UCS **Faults and Error Messages** Reference Guide 4.0 https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/Reference-Docs/Faults-Error-Msgs/4-0/b_Cisco_UCS_Faults_and_Error_Messages_Reference-4-0.html
	S-Series Servers
[18]	Cisco UCS **S3260 Server Integration with Cisco UCS Manager**, Release 4.0 https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/GUI-User-Guides/Dense-Storage-Server-Integ-Mgmt/4-0/b_UCSM_3260_Integration_Guide_4_0.html Cisco UCS **S3260 Server Integration with Cisco UCS Manager Using the CLI**, Release 4.0 https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/CLI-User-Guides/Dense-Storage-Server-Integ-Mgmt/4-0/b_CLI_UCSM_3260_Integration_Guide_4_0.html
[19]	Cisco UCS **S-Series Storage Servers**: Install and Upgrade Guides https://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-s-series-storage-servers/products-installation-guides-list.html

1.4. Supported Hardware and Software

Only the following hardware and software listed below is compliant with the Common Criteria EAL2 evaluation. Using hardware not specified invalidates the secure configuration. Likewise, using any software version other than the evaluated software listed below will invalidate the secure configuration.

1.4.1. Supported Configurations

- Cisco UCS Manager (UCSM) components
    - One or more Cisco UCS Fabric Interconnects [6332, 6332-16UP or 6454 (for use with S-Series, or C-Series Servers), or 6324 (for use in the 5108 Blade Server Chassis)]
        - Cisco UCS Manager release 4.0(xx)
- Server and Fabric Extenders (with software loaded from the UCSM bundle)
    - Blade server configurations:
        - One or more Cisco UCS 5108 Chassis with:
            - One or more Cisco UCS Fabric Extenders (2204XP, 2208XP, 2304, 2408)
            - One or more Cisco UCS Blade Servers (B200 M5, or B480 M5)
    - Rack-Mount Server configurations:
        - One or more Cisco Nexus Fabric Extenders (2232 PP, 2232TM-E and 2348UPQ)
        - One or more Cisco UCS Rack Servers:
            - Any of: C220 M5, C240 M5, C480 M5 or C480 ML M5
        - And/or: Cisco UCS C4200 Chassis with one or more C125 M5
    - Storage Server configurations:
        - One or more Cisco Nexus Fabric Extenders (2232 PP, 2232TM-E and 2348UPQ)
        - One or more Cisco UCS Storage Servers (S3260 M5)

1.4.2. Compatible network adapters for Blade Servers

- Cisco UCS VIC 1340
- Cisco UCS VIC 1440
- Cisco UCS VIC 1480

1.4.3. Compatible network adapters for Rack Mount Servers

- Cisco UCS VIC 1225
- Cisco UCS VIC 1225T
- Cisco UCS VIC 1385
- Cisco UCS VIC 1387
- Cisco UCS VIC 1455
- Cisco UCS VIC 1457

1.4.4. Compatible network adapters for Rack Mount Servers

- Cisco UCS VIC 1227
- Cisco UCS VIC 1455
- Cisco UCS VIC 1387

1.5. Operational Environment

1.5.1. Required software for the operational environment

- The GUI client applet of the Cisco UCS Manager (UCSM) is a Java-based application that allows remote administration of UCSM over TLS. The applet, which is part of the TOE, requires Sun JRE 1.7 or later, which is part of the IT environment. Note that that UCS Manager runs on the Fabric Interconnect component of the UCS system and the management workstation is used to connect to the UCS and run the UCSM client applet (the Java-based GUI). The UCS Manager uses web start[1] to present the GUI and supports the following web browsers:
  - Microsoft Internet Explorer 11 or higher
  - Mozilla Firefox 45 or higher
  - Google Chrome 57 or higher
  - Apple Safari version 9 or higher
  - Opera version 35 or higher
- The UCS system must be separated from public/untrusted networks by an application-aware firewall such that remote access to the TOE's management interface is prohibited from untrusted networks and only allowed from trusted networks.

1.5.2. Optional software/components for the operational environment:

- SSHv2 Client: UCSM can be managed remotely via SSHv2.
- SNMPv3 Client: UCSM can be managed remotely via SNMPv3.
- Remote Authentication Server: A RADIUS, TACACS+, or LDAP server is an optional component for use with the TOE.
- SNMPv3 Server: An SNMPv3 server is an optional component for use with the TOE.
- Syslog Server: A syslog server is required for receiving and reviewing audit messages of failed administrative actions. Successful actions are logged to the local audit logs as well as to the remote syslog server. Failed authentication attempts are not logged to the local audit log, but are sent to a remote syslog server.
- NTP Server: An NTP server is an optional component of the operational environment that would allow for synchronizing the TOE clocks with an external time source.

[1] Java Web Start is a network deployment method for standalone Java applications. Note that although the deployment to the administrator's browser is dynamic, the version deployed is a static version associated with the TOE.

1.6. Excluded Functionality

Stand-alone configuration of the C-Series (Rack Mount) Servers and S-Series Storage Servers are not supported; C-Series servers must be managed by UCS Manager.

Direct admin interfaces to CIMC (on B-Series, C-Series servers and S-Series Storage servers) is disabled when the servers are integrated with the fabric and will be managed via UCSM.

IPMI management of CIMC is disabled by default and remains disabled in the evaluated configuration.

Telnet is disabled by default and must remain disabled in the evaluated configuration, SSH must be used instead.

CIM XML is disabled by default, and must remain disabled in the evaluated configuration.

All other functionality is supported in the evaluated configuration.

1.7. Modes of Operation

UCSM has two categories of operation: booting; and normal operation.

- When booting, the UCSM normal boot sequence can be interrupted by the Authorised Administratorwith direct local access to the serial console port. When the boot sequence is interrupted, UCSM presents a loader prompt, allowing the administrator to enter the image to be booted, then UCSM presents a boot prompt that allows the administrator to perform basic maintenance tasks like resetting the admin password. None of the network ports are operational while UCSM is booting. For further detail, refer to "Troubleshoot Firmware" in **[5]**.
    - The booting mode is the initial setup, which provides prompts for basic setup information such as IP address. Setup mode is entered automatically on a switch which has no configuration. Setup mode is accessible initially only via the serial console port, and can be completed through the serial connection via CLI, or can be completed through HTTPS (TLS1.2) via GUI after providing basic network configuration for the management port (an IP address, subnet, etc.). No other network services are operational during setup. For further information, refer to "Console Setup - Configure Fabric Interconnects" in **[3]**.
- There are two forms of normal operation: standalone; and clustered. For further information, refer to "Configuration Options" section in **[3]**.
    - In a standalone configuration, only one IP address and the subnet mask are used for the single management port on the single fabric interconnect running a single instance of UCSM.

- In a cluster configuration, a pair of clustered fabric interconnects use the following three IP addresses in the same subnet: Management port IP address for fabric interconnect A; Management port IP address for fabric interconnect B; and the Cluster IP address. Both fabric interconnects in a cluster configuration must go through the initial setup process. The first fabric interconnect to be set up must be enabled for a cluster configuration. Then, when the second fabric interconnect is set up, it detects the first fabric interconnect as a peer fabric interconnect in the cluster. To use the cluster configuration, the two fabric interconnects must be directly connected together using Ethernet cables between the L1 (L1-to-L1) and L2 (L2-to-L2) high availability ports, with no other fabric interconnects in between. This allows the two fabric interconnects to continuously monitor the status of each other and quickly know when one has failed. The two instances of Cisco UCS Manager communicate across a private network between the L1 and L2 Ethernet ports on the fabric interconnects. Configuration and status information is communicated across this private network to ensure that all management information is replicated.

2. Secure Acceptance of the TOE

In order to ensure the correct TOE is received, the TOE should be examined to ensure that that is has not been tampered with during delivery.

Verify that the TOE software and hardware were not tampered with during delivery by performing the following actions:

Step 1 Before unpacking the TOE, inspect the physical packaging the equipment was delivered in. Verify that the external cardboard packing is printed with the Cisco Systems logo and motifs. If it is not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 2 Verify that the packaging has not obviously been opened and resealed by examining the tape that seals the package. If the package appears to have been resealed, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 3 Verify that the box has a white tamper-resistant, tamper-evident Cisco Systems bar coded label applied to the external cardboard box. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). This label will include the Cisco product number, serial number, and other information regarding the contents of the box.

Step 4 Note the serial number of the TOE on the shipping documentation. The serial number displayed on the white label affixed to the outer box will be that of the device. Verify the serial number on the shipping documentation matches the serial number on the separately mailed invoice for the equipment. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 5 Verify that the box was indeed shipped from the expected supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). This can be done by verifying with the supplier that they shipped the box with the courier company that delivered the box and that the consignment note number for the shipment matches that used on the delivery. Also verify that the serial numbers of the items shipped match the serial numbers of the items delivered. This verification should be performed by some mechanism that was not involved in the actual equipment delivery, for example, phone/FAX or other online tracking service.

Step 6 Once the TOE is unpacked, inspect the unit. Verify that the serial number displayed on the unit itself matches the serial number on the shipping documentation and the invoice. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). Also verify that the unit has the following external identification:

Table 2: Evaluated Products and their External Identification

Product Name	External Identification
Cisco UCS 5108 Server Chassis	UCSB-5108
Cisco UCS B200 M5 Blade Server	UCSB-B200-M5

Cisco UCS B480 M5 Blade Server	UCSB-B480-M5
Cisco UCS C4200 Rack Server Chassis	UCSC-C4200-SFF
Cisco UCS C125 M5 Rack Server	UCS-C125
Cisco UCS C220 M5 Rack Server	UCSC-C220-M5SX UCSC-C220-M5SN
Cisco UCS C240 M5 Rack Server	UCSC-C240-M5SX UCSC-C240-M5S UCSC-C240-M5SN
Cisco UCS C480 M5 Rack Server	UCSC-C480-M5
Cisco UCS C480 ML M5 Rack Server	UCSC-C480-M5ML8
Cisco UCS S3260 M5 Rack Server	UCSS-S3260-M5
Cisco UCS 6454 Fabric Interconnect	UCS-FI-6454-U
Cisco UCS 6332 Fabric Interconnect	UCS-FI-6332-U
Cisco UCS 6332-16UP Fabric Interconnect	UCS-FI-6332-16UP-U
Cisco UCS 6324 Fabric Interconnect	UCS-FI-M-6324
Cisco UCS 2204XP Fabric Extender	UCS-IOM-2204XP
Cisco UCS 2208XP Fabric Extender	UCS-IOM-2208XP
Cisco UCS 2304 Fabric Extender	UCS-IOM-2304
Cisco UCS 2408 Fabric Extender	UCS-IOM-2408
Cisco Nexus 2232PP Fabric Extender	N2K-C2232PP
Cisco Nexus 2232TM-E Fabric Extender	N2K-C2232TM-E
Cisco Nexus 2348UPQ Fabric Extender	N2K-C2348UPQ

Step 7 Approved methods for obtaining a Common Criteria evaluated software images:

- Download the Common Criteria evaluated software image file from Cisco.com onto a trusted computer system. Software images are available from Cisco.com at the following: http://www.cisco.com/cisco/web/download/index.html.
- The TOE ships with software images preinstalled. However, this may not be the evaluated version. If this is the case, then the Common Criteria evaluated software image file must be downloaded from Cisco.com.

Step 8 Once the file is downloaded, verify that it was not tampered with by using an SHA512 checksum utility (such as 'sha512sum' on Linux) to compute the SHA512 checksum for the downloaded file and comparing this with the checksum for the image listed in Table 5 below. If the checksums do not match, contact Cisco Technical Assistance Center (TAC) http://tools.cisco.com/ServiceRequestTool/create/launch.do.

Step 9 The end-user must confirm once the TOE has booted that they are indeed running the evaluated version.

- For all Fabric Interconnect models, use the "**show version**" command to display which image is "Active". Refer to "Manage Firmware through Cisco UCS Manager" in **[5]**. Example:
  - connect local-management
    - show version
    - exit
  - connect nxos
    - show version
    - exit
- For all Fabric Extender models, use "**show version**". Example:
  - scope chassis [chassis number]
    - scope iom [a or b]
      - show version
- For the 5108 chassis, use the "**show firmware**" command. Example:
  - scope chassis [chassis number]
    - show firmware
- For B-Series servers, use the UCS Manager GUI to determine the active version, or use the "**show firmware**" command from via the CLI to display which image is "Active". Refer to "Manage Firmware through Cisco UCS Manager" in **[5]**. Example:
  - [Start from "scope chassis" listed above.]
    - scope server [server number]
      - show firmware
- For C-Series servers, use the "**show server firmware**" command to ensure the correct firmware version is running. If the correct firmware version is not loaded, or not active refer to "Manage Firmware through Cisco UCS Manager" in **[5]**. Example:
  - show server firmware
- For S-Series servers, use the "**show firmware**" command to ensure the correct firmware version is running. If the correct firmware version is not loaded, or not active refer to "Firmware Management" in **[19]**. Example:
  - scope chassis [chassis id]
    - scope sioc {1|2}
      - Scope cmc
        - show firmware

Table 3: Software Image Bundle for UCS Manager (infrastructure bundles)

Release	4.0(4b)
Filename	ucs-k9-bundle-infra.4.0.4b.A.bin
Release Date	17-May-2019
Description	The UCS Infrastructure Software Bundle contains: - NX-OS software **for the UCS 6200 Fabric Interconnects** - Firmware for the fabric extenders and I/O modules - UCS Manager - Chassis Management Controller - UCSM Capability Catalog.
Size	953.64 MB
SHA512 Checksum	e23adec23e1ff6c4aa73626198cb742edd2a5ad0fc4a24a219f31c2cb2e68b740ad5becb80afd2ed0e972bd2914cb9fe9d5d434277582d1c51cc610fb11c3d72
Release	4.0(4b)
Filename	ucs-6300-k9-bundle-infra.4.0.4b.A.bin
Release Date	17-May -2019
Description	The UCS Infrastructure Software Bundle contains: - NX-OS software **for the UCS 6332 Fabric Interconnects** - Firmware for the fabric extenders and I/O modules - UCS Manager - Chassis Management Controller - UCSM Capability Catalog.
Size	1190.71 MB
SHA512 Checksum	c79f182d76437b8d2d0e4f1c3e571914b47044d309e9ba063ff6d6f23e1e8eee99d2c02f6ac7ea90ba4470df0421c1023b332cb7df18be68df26aafa8d2759c4
Release	4.0(4b)
Filename	ucs-mini-k9-bundle-infra.4.0.4b.A.bin
Release Date	17-May -2019
Description	The UCS Infrastructure Software Bundle contains: - NX-OS software **for the UCS 6324 Fabric Interconnects** - Firmware for the fabric extenders and I/O modules - UCS Manager - Chassis Management Controller - UCSM Capability Catalog.
Size	1000.52 MB
SHA512 Checksum	4b52e294f616123bc0f52fa42d9ad7e8bb1297069a7b448aec7e39c6eb16ff53c671ab19c5aada486bc45088da7bdfdda5231c9570b050e4b35e27cb7e761aa7
Release	4.0(4b)
Filename	ucs-6400-k9-bundle-infra.4.0.4b.A.bin
Release Date	17-May -2019

Description	The UCS Infrastructure Software Bundle contains: - NX-OS software **for the UCS 6454 Fabric Interconnects** - Firmware for the fabric extenders and I/O modules - UCS Manager - Chassis Management Controller - UCSM Capability Catalog.
Size	1923.24 MB
SHA512 Checksum	4fe6eaaf7674e221178c27f695b02f68f61989b6de971c2a2d81ecb33e4a84aa2ba15dde20016e32599b6161c7c9807b840f8e54feaa11557455aca937dc9b9c

Table 4: Software Image Bundle for UCS B-Series Servers and Adapters

Release	4.0(4b)
Filename	ucs-k9-bundle-b-series.4.0.4b.B.bin
Release Date	17-May -2019
Description	Software for the **UCS B-Series blade server** products.
Size	612.48 MB
SHA512 Checksum	9c5e1300c259dd419e1eef491667b97299e8a90b790dced5c6ad5f71ac884eac12760f319a0588113125007717cc85a71873b8cdb6510baea01d6876b72acdf3

Table 5: Software Image Bundle for UCS C-Series Servers and Adapters

Release	4.0(4b)
Filename	ucs-k9-bundle-c-series.4.0.4b.C.bin
Release Date	17-May -2019
Description	Software for the **UCS C-Series rack-mounted servers**. This is software for UCS Manager based C-Series management.
Size	1626.69 MB
SHA512 Checksum	3977ba2731980fcc7cc41b0b6bc5af93b196a34004e09b0caa4fa45210ae70582ead2c04cdcb06fa6d4f2a03ade403197b6ac99f02eb215d6a804ae3d811f203

Table 6: UCS C3260 (S3260) Rack Server Software

Release	4.0(4b)
Filename	ucs-s3260-huu-4.0.4b.iso
Release Date	29-April -2019
Description	Cisco UCS Host Upgrade Utility - For M4 and M5 Servers

Size	424.07 MB
SHA512 Checksum	a3e249ff0bd77a3438bde2246658bef2e45329ba2f67524c01ce25 a31fe9da525a05bd35178e27c89caa9004781c0484ecd13cae1740 726a085432d6b42b0212

Note: UCS C3260 name has changed to S3260.

3. Secure Installation

3.1. Physical Installation

Follow the site preparation guide **[1]** for preparation of the physical site, and hardware installation guides **[11], [12],** and/or **[13]**, and/or **[19]+[18]** as applicable to the configuration of hardware components to be deployed.

3.2. Initial Setup via Direct KVM Access

C-Series Servers and S-Series Storage Servers must be given basic configuration via KVM prior to being connected to any network. The servers have a default user ID and password that would be accessible via the network, and must be changed via KVM prior to network connectivity.

Prior to connecting network interfaces of C-Series servers and S-Series Storage Servers, use a direct KVM connection to complete the steps outlined below:

3.2.1. Default Password Changes

Reset the admin password. During initial setup, the setup sequence via CLI prompts the user to set the admin password. To reset the password following initial setup, connect via CLI and reset the password following instructions in section, "Password Management," or "Locally Authenticated User Accounts," in **[4]** and 'Connecting the System and Opening the Setup Utility **[19]**.

3.2.2. IP Address Configuration

Set static IP address, or configure DHCP. Complete the steps described in the "Configuring Fabric Interconnects" in **[3]** and ''Setting Static CMC and BMC Internal IP Addresses' **[19]**.

3.2.3. Migrating from Standalone Cisco UCS S3260 to UCSM Managed Cisco UCS S3260

To configure the UCS S3260 to be managed by UCS Manager, complete the steps in Migration to UCSM- Managed Cisco UCS S3260 **[18].**

3.3. Network Connectivity for Servers

3.3.1. Port Configurations

For configuration options and procedures related to available port modes and port types, refer to "Port Modes" and "Port Types" within **[3]**.

3.3.2. Server Ports

For configuration options and procedures related to server ports, refer to "Configure Fabric Interconnect Server Ports in **[3]**.

3.3.3. Protected Management Network

The IT Environment in which the TOE components reside will need to provide a protected network for interconnects from the UCS Manager to remote

authentication servers, remote time servers (NTP), and remote log servers (syslog). An option for sufficient isolation of the protected management network would be to isolate it from Ethernet traffic of hosted OS instances by assigning separate VLAN(s) from the VLANs assigned to vNICs of any hosted OS, except where the hosted OS is an OS trusted by the TOE to provide remote authentication, time, or logging service. For configuration options and procedures, refer to "Configure LAN Connectivity" in **[3]**.

3.3.3.1. Reserved VLAN Ranges

VLAN IDs 4030-4047 inclusive, and 4094-4098 inclusive are permanently reserved for internal system use, and thus cannot be used for user traffic.

By default, a broader range of 128 VLAN IDs (3915-4042 inclusive, partially overlapping 4030-4047) is defined as reserved. If an administrator wants to be able to use VLAN IDs 3915-4029 for user traffic, the default reserved range can be set to any contiguous range of 128 unused VLAN IDs starting from 2-3915 inclusive. For example, changing the reserved range to 3787-3914 inclusive would allow VLANs 3915-4029 to be used.

Whenever the range of reserved VLANs is changed, all Fabric Interconnects and Fabric Extenders must be rebooted. If an Fabric Interconnect or Fabric Extender boots and its reserved VLAN range does not match what's defined by UCSM, the Fabric Interconnect or Fabric Extender will be updated and rebooted automatically. For VLANs, refer to "VLANs" in **[7]**.

Procedure To configure VLAN IDs

- **Step 1** In the Navigation pane, click LAN.
- **Step 2** In the Work pane, click the Global Policies tab.
- **Step 3** Specify a new value in the Reserved VLAN Start ID field. The reserved VLAN range ID can be specified from 2-3915.
- **Step 4** Click Save Changes.

3.4. Network Protocols and Cryptographic Settings

3.4.1. Remote Administration Protocols

- Telnet is disabled by default and must remain disabled in the evaluated configuration.
- SSHv2 is enabled be default. SSH can be disabled if desired using "**set enabled {yes | no}**". SSH is listening by default on TCP port 22. The port number can be changed if desired using the "**set ssh-port**" command. UCSM does not provide an option to limit which algorithms are enforced for SSH connections, so administrators using SSH should configure their SSH clients to use only the algorithms that are specified for use in the evaluated configuration, including RSA, AES, and SHA-1.

UCSM supports SSH key sizes of 768, 1024 and 2048. For the evaluated configuration only the key size of **2048** must be used when using SSH to connect to UCSM.

The following algorithms are allowed for use:

- Encryption Algorithms
  - *aes128-ctr,*
  - *aes192-ctr,*
  - *aes256-ctr,*
  - *aes128-gcm@openssh.com,*
  - *aes256-gcm@openssh.com*
- MAC Algorithms
  - *hmac-sha1,*
  - *hmac-sha2-256,*
  - *hmac-sha2-512*
- Key Exchange methods
  - *diffie-hellman-group14-sha1,*
  - *diffie-hellman-group16-sha512,*
  - *ecdh-sha2-nistp256,*
  - *ecdh-sha2-nistp384,*
  - *ecdh-sha2-nistp521*

- HTTPS is enabled by default and must remain enabled for remote administrative access to all management functions described in the Security Target. HTTPS is listening by default on TCP port 443. The port number can be changed if desired using the "**set https-port**" command. UCSM does not provide an option to limit which algorithms are enforced for HTTPS connections, so administrators using HTTPS should configure their HTTPS clients/browsers to use only the algorithms that are specified for use in the evaluated configuration, including RSA, AES, and SHA.
  - To configure HTTPS, refer to "Configuring HTTPS" in **[4]**.
    - UCS supports key modulus sizes of 2048, 2560, 3072, 3584, and 4096, and any modulus 2048 bits and larger are permitted in the evaluated configuration. The default key pair is 2048-bit.
    - Set the "Allowed SSL Protocols" to "Only TLSv1.2".
    - Set the cipher-suite-mode to "custom", and set the cipher-suite to prohibit 3DES ciphersuites (the cipher-suite enabled when the mode is HIGH differs from the one shown below in that the HIGH cipher-suite list would allow 3DES ciphers to be used).
      - If using the GUI, set the mode to "custom" and paste this string into the cipher-suite field:

```
ALL:!DH:!EDH:!ADH:!EXPORT40:!EXPORT56:
!LOW:!MEDIUM:!eNULL:!RC4:!DES:!3DES:+H
IGH:+EXP
```

- Select "Allowed SSL Protocol only TLSV1.2"
- If using the CLI, use the following steps:

```
scope system
scope services
enable https
set https cipher-suite-mode custom
set https cipher-suite
ALL:!DH:!EDH:!ADH:!EXPORT40:!EXPORT56:!LOW:!
MEDIUM:!eNULL:!RC4:!DES:!3DES:+HIGH:+EXP
set https ssl-protocol tls1-2
commit
```

- When the steps above have been applied, the following cipher-suites will be the only ones available for use.

TLSv1.2 Allowed Cipher Suites:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp521r1)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp521r1)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp521r1)
- TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048)
- TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048)
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp521r1)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp521r1)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp521r1)
- TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048)
- TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048)
- TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048)

- When the Java-based UCSM Client is used, it will also use TLSv1.2 and negotiate the connection using TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384.
- When using a browser-based HTTPS client, UCSM will negotiate the connection using the same ciphersuite that would be used with the Java-based UCSM Client, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, if the browser supports that ciphersuite, otherwise UCSM will negotiate one of the other ciphersuites listed above that allowed in the CC-certified configuration and all use RSA, AES, and SHA. If the browser does not support TLSv1.2 and at least one of the listed ciphersuites, the session negotiation will fail.

- HTTP is enabled by default, and should be reconfigured from the default to redirect to HTTPS. If redirect to HTTPS is not desired, HTTP must be disabled instead. HTTP is listening by default on TCP

port 80. The port number can be changed if desired using the "**set http-port"** command.

- If desired, to disable HTTP, refer to "Disabling Communication Services", in **[4]**.
- To reconfigure HTTP to redirect to HTTPS:
- scope system
  - scope services
    - enable http
    - enable https
    - enable http-redirect
    - commit

- SNMPv3 user accounts must be configured use AES with 128 bit keys and SHA-1 (enable "SHA", must not enable "MD5"). For a full description of the process using CLI, see "Creating an SNMPv3 User" in **[4]**.
  - Require use of AES with 128 bit key length and use of SHA-1:
    - Via CLI:
      - scope monitoring
        - enable snmp
        - create snmp-user [user-name]
        - set aes-128 **yes**
        - set auth **sha**
        - set password {prompted for password}
        - set priv-password {prompted for password}
        - commit-buffer
    - Via GUI, on the Navigation pane, on the Admin tab, under Communication Management, then under Communication Services, and in the SNMP Users area:
      - Create SNMP User
        - Set the Auth Type field to **SHA**
        - Check the "**Use AES-128"** check box
        - Set the password, and the privacy password.
- IPMI is disabled by default and must remain disabled in the evaluated configuration. IPMI commands and responses are not encrypted unless a ciphersuite is specified by the IPMI client as part of the IPMI

request (the most secure ciphersuite supported by IPMI v2.0 is "cipher suite ID 3," which uses HMAC-SHA1-96 for integrity and AES-CBC-128 for confidentiality).

- SMASH CLP is enabled by default and cannot be disabled. The interface is read-only.
- CIM XML is disabled by default, and must remain disabled in the evaluated configuration.

3.4.2. Authentication Server Protocols

- RADIUS (outbound) for authentication of TOE administrators to remote authentication servers are disabled by default but can be enabled by administrators in the evaluated configuration.
  - To configure RADIUS refer to "RADIUS Providers" **[4]**. Specification of a key is required to ensure RADIUS traffic is encrypted between UCS and the remote RADIUS server. Use best practice for selection and protection of a key to ensure that the key is not easily guessable and is not shared with unauthorized users.
- TACACS+ (outbound) for authentication of TOE administrators to remote authentication servers are disabled by default but can be enabled by administrators in the evaluated configuration.
  - To configure TACACS+, refer to "TACACS+ Providers" in **[4]**. Specification of a key is required to ensure TACACS+ traffic is encrypted between UCS and the remote TACACS+ server. Use best practice for selection and protection of a key to ensure that the key is not easily guessable and is not shared with unauthorized users.
- LDAP (outbound) for authentication of TOE administrators to remote authentication servers is disabled by default and should only be used with TLS encryption enabled. UCS supports encryption of LDAP connections using TLS (LDAPS). To configure LDAP refer to "Creating an LDAP Provider" in **[4]**. When creating the LDAP provider via GUI, check the "Enable SSL" checkbox. When creating an LDAP provider via CLI, include the "set ssl **yes**" command.

3.4.3. Logging and Alerting Protocols

- Syslog (outbound) for transmission of UCS syslog events to a remote syslog server is disabled by default but can be enabled in the evaluated configuration (to enable transmission of all events to a remote syslog server including failure messages that are not stored locally) with the understanding that syslog traffic is transmitted unencrypted, so any protection from unauthorized disclosure or modification while in transit must be provided by the operational environment.
  - To configure syslog, refer to

  - CLI -"Enabling Syslog Messages to Store In a Local File"
  - GUI – "Configuring the Syslog using Cisco UCS Manager GUI"

  in **[10]**. To enable the transmitting of syslog messages to remote syslog servers (up to 3 servers can be configured), include the "set syslog remote-destination …" commands (if using CLI), or if using GUI click the "Enabled" radio button under "Remote Destinations" within Admin > Faults, Events and Audit Log > Syslog.

- Note, UCS provides other mechanisms other than syslog for batch transmission of event logs to a remote server including FTP, TFTP, SCP, and SFTP (SCP and SFTP are encrypted via SSH, while FTP and TFTP are unencrypted). Refer to "Configuring the SEL Policy" in **[10]** for more information.

- SNMP Traps (outbound) for transmission of UCS SNMP events to a remote SNMP server is disabled by default but can be enabled in the evaluated configuration. SNMP traps are supported using SNMPv1, SNMPv2c, and SNMPv3. To encrypt the messages, use SNMPv3 and set the privilege to "Priv" to enable authentication and encryption.
  - To configure or delete an SNMP Trap host refer to "Creating an SNMP Trap" in **[10]**.
- SMTP mail (outbound) can be configured as part of custom "call home" profiles to send alerts for administratively-specified events via email (unencrypted) to administratively-defined email addresses.

4. Secure Configuration

4.1. User Roles

User roles contain one or more privileges that define the operations allowed for the user who is assigned the role. A user can be assigned one or more roles. A user assigned multiple roles has the combined privileges of all assigned roles. For example, if Role1 has storage related privileges, and Role2 has server related privileges, then users who are assigned to both Role1 and Role2 have storage and server related privileges.

All roles include read access to all configurations on the system, and all roles except Read-Only can modify some portion of the system state. A user assigned a role can modify the system state in that user's assigned area.

For more information see 'Role-Based Access Configuration' **[4]**.

4.1.1. Default Roles and Privileges

The system contains the following default user roles:

- AAA Administrator: Read-and-write access to users, roles, and AAA configuration. Read access to the rest of the system.
- Administrator: Complete read-and-write access to the entire system. The default admin account is assigned this role by default and this association cannot be changed.
- Facility Manager: Read-and-write access to power management operations through the power management privilege. Read access to the remaining system.
- Network Administrator: Read-and-write access to fabric interconnect infrastructure and network security operations. Read access to the rest of the system.
- Operations: Read-and-write access to systems logs, including the syslog servers, and faults. Read access to the rest of the system.
- Read-Only: Read-only access to system configuration with no privileges to modify the system state.
- Server Compute Administrator: Read and write access to most aspects of service profiles. However, the user cannot create, modify or delete vNICs or vHBAs.
- Server Compute: Read and write access to most aspects of service profiles. However, the user cannot create, modify or delete vNICs or vHBAs.
- Server Equipment Administrator: Read-and-write access to physical server related operations. Read access to the rest of the system.

- Server Profile Administrator: Read-and-write access to logical server related operations. Read access to the rest of the system.
- Server Security Administrator: Read-and-write access to server security related operations. Read access to the rest of the system.
- Storage Administrator: Read-and-write access to storage operations. Read access to the rest of the system.

Privileges give their holder access to specific system resources and permission to perform specific tasks. Privileges can be added to the default roles.

The following table lists each privilege and the user role given that privilege by default.

Table 6 Privileges and Default Role Assignments

Privilege	Management Capabilities	Default Role Assignment
aaa	System security and AAA	AAA Administrator
admin	System administration	Administrator
ext-lan-config	External LAN configuration	Network Administrator
ext-lan-policy	External LAN policy	Network Administrator
ext-lan-qos	External LAN QoS	Network Administrator
ext-lan-security	External LAN security	Network Administrator
ext-san-config	External SAN configuration	Storage Administrator
ext-san-policy	External SAN policy	Storage Administrator
ext-san-qos	External SAN QoS	Storage Administrator
ext-san-security	External SAN security	Storage Administrator
fault	Alarms and alarm policies	Operations
operations	Logs and Smart Call Home	Operations
org-management	Organization management	Operations
pod-config	Pod configuration	Network Administrator
pod-policy	Pod policy	Network Administrator
pod-qos	Pod QoS	Network Administrator
pod-security	Pod security	Network Administrator
power-mgmt	Read-and-write access to power management operations	Facility Manager
read-only	Read-only access. Read-only cannot be selected as a privilege; it is assigned to every user role.	Read-Only
server-equipment	Server hardware management	Server Equipment Administrator
server-maintenance	Server maintenance	Server Equipment Administrator
server-policy	Server policy	Server Equipment Administrator

server-security	Server security	Server Security Administrator
service-profile-compute	Service profile compute	Server Compute Administrator
service-profile-config	Service profile configuration	Server Profile Administrator
service-profile-config-policy	Service profile configuration policy	Server Profile Administrator
service-profile-ext-access	Service profile end point access	Server Profile Administrator
service-profile-network	Service profile network	Network Administrator
service-profile-network-policy	Service profile network policy	Network Administrator
service-profile-qos	Service profile QoS	Network Administrator
service-profile-qos-policy	Service profile QoS policy	Network Administrator
service-profile-security	Service profile security	Server Security Administrator
service-profile-security-policy	Service profile security policy	Server Security Administrator
service-profile-server	Service profile server management	Server Profile Administrator
service-profile-server-oper	Service profile consumer	Server Profile Administrator
service-profile-server-policy	Service profile pool policy	Server Profile Administrator
service-profile-storage	Service profile storage	Storage Administrator
service-profile-storage-policy	Service profile storage policy	Storage Administrator

For a more granular overview of which operations relate to each privilege refer to chapter “Cisco UCS XML Object-Access Privileges” in Cisco UCS Manager XML API Programmer’s Guide **[15].**

4.1.2. Security-Relevant Functions Allowed for Default Roles

A server administrator can use Cisco UCS Manager to perform server management tasks within a Cisco UCS instance, including the following:

- Create server pools and policies related to those pools, such as qualification policies
- Create policies for the servers, such as discovery policies, scrub policies, and IPMI policies
- Create service profiles and, if desired, service profile templates
- Apply service profiles to servers
- Monitor faults, alarms, and the status of equipment

A network administrator can use Cisco UCS Manager to perform tasks required to create LAN configuration for a Cisco UCS instance, including the following:

- Configure uplink ports, port channels, and LAN PIN groups
- Create VLANs

- Configure the quality of service classes and definitions
- Create the pools and policies related to network configuration, such as MAC address pools and Ethernet adapter profiles

A storage administrator can use Cisco UCS Manager to perform tasks required to create SAN configuration for a Cisco UCS instance, including the following:

- Configure ports, port channels, and SAN PIN groups
- Create VSANs
- Configure the quality of service classes and definitions
- Create the pools and policies related to the network configuration, such as WWN pools and Fibre Channel adapter profiles

4.1.3. Custom Roles and Modification of Default Roles

New custom roles can be created, deleted, or modified to add or remove any combination of privileges. Default roles can be deleted or modified except the 'admin' and 'read-only' roles. When a role is modified, the new privileges are applied to all users assigned to that role. Privilege assignment is not restricted to the privileges defined for the default roles. That is, you can use a custom set of privileges to create a unique role. For example, the default Server Administrator and Storage Administrator roles have different set of privileges, but a new Server and Storage Administrator role can be created that combines the privileges of both roles.

If a role is deleted after it has been assigned to users, it is also deleted from those user accounts.

User profiles on AAA servers (RADIUS or TACACS+) contain the roles corresponding to the privileges granted to that user. The cisco-av-pair vendor-specific attribute is used to store the role information. The AAA servers return this attribute with the request and parse it to get the roles. LDAP servers return the roles in the user profile attributes.

Refer to **[4]** for more information about UCS roles and privileges.

4.2. Passwords

To prevent users from choosing insecure passwords, each password for local user accounts must meet the following requirements:

- At least eight characters long
- Does not contain more than three consecutive characters, such as abcd
- Does not contain more than two repeating characters, such as aaabbb
- Does not contain dictionary words
- Does not contain common proper names
- Does not start with a number

This requirement applies to the local password database and on the password selection functions provided by the TOE, but remote authentication servers may have pre-configured passwords which do not meet the quality metrics.

The requirements above are enforced by UCS for CLI and GUI accounts. IPMI also supports password-based authentication, but IPMI is disabled by default and must remain disabled in the CC-evaluated configuration.

4.3. Password Expiration

By default, passwords are not set to expire, but password expiration can be set for each user by a user who has the aaa or admin privilege. For more information, refer to "Password Profile for Locally Authenticated Users" in **[4]**.

4.4. Account Expiration and Activation

By default, user accounts do not expire. User accounts can be configured to expire at a predefined time by a user who has the aaa or admin privilege. When the expiration time is reached the user account is disabled. For more information, refer to "Password Profile for Locally Authenticated Users" in **[4]**.

NOTE: When a user account is created, it is not functional (cannot be used for login) until its password has been set. This is true even if the Account Status is set to "active," as the Account Status setting is intended to be used to enable/disable accounts that are fully configured, including having password set. To view whether the password has been set for any account, open the user properties page, and look to the right of the password field, which with either say, "Set: yes", or "Set: no".

4.5. Clock Management

In the evaluated configuration, it is recommended, though not essential that UCSM be configured to use NTP. When configured to use NTP, the system will not allow users to manually set the clock. An administrator must have the admin or server-maintenance privilege to be able to set the clock or configure the system's use of an NTP server. To add an NTP server via the GUI, clock "Add NTP Server" under Admin > Time Zone Management > Timezone, and enter the hostname or IP address of the NTP server.

In the evaluated configuration, the time zone should be set as desired when UCSM is initially deployed, and should not be modified thereafter. Modification of the time zone may yield unexpected results in messages transmitted via syslog such that the time zone written by UCSM into the syslog message is not accurate, and does not match what would be displayed on the UCSM CLI using the "show clock" or "show timezone" commands.

4.6. Identification and Authentication

The UCS Manager can be configured to use any of the following authentication methods:

- Local authentication (password or SSH public key authentication);
  - Authorized administrators with the aaa or admin privileges may configure local authentication.
- Remote authentication (RADIUS, LDAP, or TACACS+)
  - Authorized administrators with the aaa or admin privileges may configure remote authentication.
  - Refer to “Authentication Server Protocols” elsewhere in this document for more details.

5. Security Relevant Events

UCS maintains two types of logs: SEL (system event log), and the Audit Log. The SEL provides temporary event storage on each device. The Audit Log is stored centrally on the primary UCS Manager instance and replicated to secondary instances (if present). For the most complete view audited events, across all devices, and to view the auditable events defined in the Security Target, administrators should review the Audit Log. Note: UCSM does not generate audit events specific to startup or shutdown of the audit log or system event log because those logs cannot be stopped or started independent of booting or shutting down UCSM itself, which are audited events. Configuration of syslog servers is audited within the local audit log. Failed authentication attempts are not logged to the local audit log, but are sent to a remote syslog server.

5.1. Reviewing, Sorting, and Filtering Audited Events

Using the UCS Manager GUI, administrators with any privilege level can review, sort and filter audited events based on record identifier (ID); affected object; or user.

- To perform sorting:
  - Go to Admin > Faults, Events and Audit Log > Audit Log
    - Click on any one of the tabs to sort by that field:
      - ID
      - Affected Object
      - User
- To perform filtering:
  - Go to Admin > Faults, Events and Audit Log > Audit Log
    - Click on the “Filter” link and enter desired filter parameters on the Filter page.

For more information about logging refer to **[10]**.

5.2. Deleting Audit Records

The storage capacity for each log type is 10,000 records, and is not configurable. When each log reaches capacity, the oldest records are overwritten by new records. It is not possible for administrators with any privilege to edit, purge or delete records.

To configure the length of time before cleared fault messages are deleted, use the

- CLI - “**set retention-interval**” command
- GUI – “**Clear Interval** field” in the Global Fault Policy tab

described in **[10]**.

6. Security Measures for the Operational Environment

Proper operation of the TOE requires functionality from the environment. It is the responsibility of the authorized users of the TOE to ensure that the TOE environment provides the necessary functions The following identifies the requirements and the associated security measures of the authorized users.

Table 7 Environment Objectives

Security Objective for the Operational Environment (from the Security Target)	**Definition of the Security Objective** (from the Security Target)	**Responsibility of the Administrators**
OE.ADMIN	Personnel measures are in place to ensure well trained and trusted administrators are authorized to manage the TOE.	Authorized Administrators must be trained and must read, understand and follow the guidance in this document to securely install and operate the TOE. It is the responsibility of the authorized administrator of the TOE to ensure that the Operational Environment provides the necessary functions and adheres to the environment security objectives [this document, Sect. 6] and follow all guidance in this document as well as the official Cisco documentation for the Cisco Unified Computing System with Cisco UCS Manager, version 4.0(4b) as described in section 1.3 of the document.
OE.VSAN	Each network interface of a storage device in the operational environment of the TOE may only participate in a single VSAN.	It is the responsibility of the authorized administrator of the TOE to ensure that the Operational Environment provides the necessary functions and adheres to the environment security objectives [this document, Sect. 6]. The authorized administrator must ensure that the TOE is only participating in a single VSAN.
OE.BOUNDARY	The UCS system must be separated from public networks by an application aware firewall.	It is the responsibility of the authorized administrator of the TOE to ensure that the Operational Environment provides the necessary functions and adheres to the environment security objectives [this document, Sect. 6]. The authorized administrator must ensure that the UCS system is separated from the public networks by an application aware firewall.

OE.PHYSICAL	The operational environment of the TOE shall have a physical security policy preventing unauthorized physical access to the UCS. The policy must document physical security controls including access control, physical separation of hardware, and monitoring policies to ensure no unauthorized physical access to the UCS system is allowed. The physical security does not apply to Java applets once the applets have been downloaded from the Fabric Interconnect to a management workstation.	It is the responsibility of the authorized administrator of the TOE to ensure that the Operational Environment provides the necessary functions and adheres to the environment security objectives [this document, Sect. 6]. The Administrator must ensure that a security policy describing the physical security controls to prevent the unauthorized physical access to the UCS is produced and has been implemented to ensure only authorised physical access to the UCS system is allowed.
OE.POWER	The operational environment of the TOE shall incorporate a power management strategy using UPS or backup generators to ensure that power continues to flow under any adverse conditions.	It is the responsibility of the authorized administrator of the TOE to ensure that the Operational Environment provides the necessary functions and adheres to the environment security objectives [this document, Sect. 6]. The authorized administrator must ensure that a power management strategy using UPS or backup generators to ensure that power continues to flow under any adverse conditions has been incorporated into the environment of the TOE.
OE.REDUNDANT_NET	The operational environment of the TOE shall provide redundant network links to protect against network administrator operator error or network equipment failure.	It is the responsibility of the authorized administrator of the TOE to ensure that the Operational Environment provides the necessary functions and adheres to the environment security objectives [this document, Sect. 6]. The authorized administrator must ensure that the TOE provides redundant network links.
OE.REMOTE_SERVERS	The operational environment of the TOE shall optionally provide remote authentication servers, SNMP servers, syslog servers, and/or NTP servers, and will protect communications between the TOE and the servers.	It is the responsibility of the authorized administrator of the TOE to ensure that the Operational Environment provides secure session between the TOE and remote servers.

7. Related Documentation

Use this document in conjunction with the Unified Computing documentation at the following location:

- http://www.cisco.com/c/en/us/products/servers-unified-computing/index.html

The following sections provide sources for obtaining documentation from Cisco Systems.

7.1. Obtaining Documentation

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation at:

With CCO login:
http://www.cisco.com/en/US/partner/docs/general/whatsnew/whatsnew.html

Without CCO login:
http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- http://www.cisco.com
- http://www-china.cisco.com
- http://www-europe.cisco.com

7.2. Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

7.3. Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click Feedback in the toolbar and select Documentation. After you complete the form, click Submit to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc., Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

8. Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com