Cisco Unified Computing System (UCS) Standalone, version 4.0(4i)

Common Criteria Operational User Guidance and Preparative Procedures

Version 1.0

14 April 2020

EDCS-18141271

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 Integrated Management Controller (CIMC), version 4.0(4i). 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 Standalone with Cisco Integrated Management Controller (CIMC), version 4.0(4i) 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.

Links to all configuration guides:

- https://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-c-series-rack-servers/tsd-products-support-series-home.html
- https://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-s-series-storage-servers/tsd-products-support-series-home.html

Table 1: Document References

	C-Series Servers
[1]	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
[2]	Cisco Host Upgrade Utility User Guide – For the M5 Servers https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/sw/lomug/4_0/b_huu_4_0_2.html
[3]	Cisco UCS C-Series Servers Integrated Management Controller CLI **Configuration Guide**, Release 4.0 https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/sw/cli/config/guide/4_0/b_Cisco_UCS_C-Series_CLI_Configuration_Guide_40.html

	Cisco UCS C-Series Integrated Management Controller GUI **Configuration Guide**, Release 4.0 https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/sw/gui/config/guide/4_0/b_Cisco_UCS_C-series_GUI_Configuration_Guide_40.html
	Troubleshooting and Other References
[4]	Cisco UCS C-Series Servers Troubleshooting Guide https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/ts/guide/b_C-Series_Troubleshooting_Guide.html
[5]	**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
[6]	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
[7]	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
[8]	Cisco Host Upgrade Utility User Guide – For S3260 Storage Servers https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/sw/lomug/2-0-x/b_huu_S3260.html
[9]	Cisco UCS Integrated Management Controller CLI **Configuration Guide** for S3260 Storage Servers, Release 4.0 https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/sw/cli/config/guide/4_0/b_Cisco_UCS_C-Series_CLI_Configuration_Guide_for_S3260_Servers_40.html Cisco UCS C-Series Integrated Management Controller GUI **Configuration Guide** for S3260 Servers, Release 4.0 https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/sw/gui/config/guide/4_0/b_Cisco_UCS_C-series_GUI_Configuration_Guide_40.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

- Server (with software loaded from the CIMC bundle)
  - Rack-Mount Server configurations:

        - One or more Cisco UCS Rack Servers:
            - Any of: C220 M5, C240 M5, C480 M5 or C480 ML M5
    - Storage Server configurations:
        - One or more Cisco UCS Storage Servers (S3260 M5)

1.4.2. 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

1.4.3. 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 Integrated Management Controller (CIMC) is a Java-based application that allows remote administration of CIMC over TLS. The applet, which is part of the TOE, requires Sun JRE 1.7 or later, which is part of the IT environment. CIMCr 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: CIMC can be managed remotely via SSHv2.
- SNMPv3 Client: CIMC can be managed remotely via SNMPv3.
- Remote Authentication Server: A LDAP server is an optional component for use with the TOE.

[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.

- 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.

1.6. Excluded Functionality

UCS Manager with C-Series (Rack Mount) Servers and S-Series Storage Servers in Standalone is not supported; C-Series servers must be managed by Cisco Integrated Management Controller (CIMC).

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

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

CIMC has two modes of operation: booting; and normal operation.

- When booting, the CIMC normal boot sequence can be interrupted by the Authorised Administrator with direct local access to the serial console port. When the boot sequence is interrupted by pressing F8, CIMC presents a loader prompt, allowing the administrator to enter the image to be booted, then CIMC presents a boot prompt that allows the administrator to perform basic maintenance tasks like resetting the CIMC admin password. None of the network ports are operational while CIMC is booting.
    - 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 device which has no configuration. Setup mode is accessible initially only via the physical KVM (keyboard-video-mouse) access, 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 “Initial Server setup” in **[1]** and **“**Installing the System**”** in **[9]**.

- There is one form of normal operation: standalone. In a standalone configuration, only one IP address and the subnet mask are used for the single management port.

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 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

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: https://software.cisco.com .
- 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) https://mycase.cloudapps.cisco.com/case .

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

- For C-Series servers and S-Series servers, use the "**show detail**" command to ensure the correct firmware version is running. If the correct firmware version is not loaded, or not active refer to "Manage Firmware " in **[9]**, and "Cisco IMC Firmware Management" **[3]**. Example:
  - scope server {1|2}
    - scope bmc
      - scope firmware
        - show detail
- In the GUI for C-Series servers and S-Series servers, click on the "i" button in the top right hand corner of the display.

Table 3: Software Image Bundle for UCS C-220 M5 Series Servers Firmware

Release	4.0(4i)
Filename	ucs-c220m5-huu-4.0.4i.iso
Release Date	9-Dec-2019
Description	Cisco UCS Host Upgrade Utility
Size	472.19 MB

SHA512 Checksum	738fc6f9408bb619f79c5cc63dd022009886c1697d3c6a68f51b540614ef5aa20b74c0d0fef558c6d3fd0d38e4b2565b44eb10e77b5aac3d449f1ccfce5595fd

Table 4: Software Image Bundle for UCS C-240 M5 Series Servers Firmware

Release	4.0(4i)
Filename	ucs-c240m5-huu-4.0.4i.iso
Release Date	9-Dec -2019
Description	Cisco UCS Host Upgrade Utility
Size	491.41 MB
SHA512 Checksum	baed32d17386d507eadf56ed089c0a58b52dad8b6dad87427ad58fe30932a35219527aa068e0db2f1a2ea0f3f2223e03430c5c0e555c3b68d305650c4d36c128

Table 5: Software Image Bundle for UCS C-480 M5 Series Servers Firmware

Release	4.0(4i)
Filename	ucs-c480m5-huu-4.0.4i.iso
Release Date	9-Dec -2019
Description	Cisco UCS Host Upgrade Utility
Size	429.13 MB
SHA512 Checksum	edf788d1efd46cbc2a15e1be274ec2aeb01922fdc3ec41b7b480cfe951f7139ea7f4f9922bf0648cca760676c2531fa883dc75a8a04f060f34cec3e5fb870277

Table 6: Software Image Bundle for UCS C-480 ML M5 Series Servers Firmware

Release	4.0(4i)
Filename	ucs-c480m5-huu-4.0.4i.iso
Release Date	9-Dec -2019
Description	Cisco UCS Host Upgrade Utility
Size	429.13 MB
SHA512 Checksum	edf788d1efd46cbc2a15e1be274ec2aeb01922fdc3ec41b7b480cfe951f7139ea7f4f9922bf0648cca760676c2531fa883dc75a8a04f060f34cec3e5fb870277

Table 7: Software Image Bundle for UCS C3260 (S3260) Rack Server Software

Release	4.0(4i)
Filename	ucs-s3260-huu-4.0.4i.iso

Release Date	9-Dec -2019
Description	Cisco UCS Host Upgrade Utility - For M5 Servers
Size	437.92 MB
SHA512 Checksum	47736acf6127474ee758b49f8cfc64fd5cdcb8ea25896ef76b0f677baa2b2476dbe0684cebf2790f6398120260549c6568821a326b92b155baf1209c64b23f7b

Note: UCS C3260 name has changed to S3260.

3. Secure Installation

3.1. Physical Installation

Follow the hardware installation guides **[1]** and/or **[7]** 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, "Managing User Accounts," in **[3]** and **[9]**.

3.2.2. IP Address Configuration

Set static IP address, or configure DHCP. Complete the steps described in the "Configuring Common Properties" in **[3]** and ''Setting Static CMC and BMC Internal IP Addresses' **[1],[9]**.

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 "Nic Mode and NIC Redundancy Settings" within **[1] and [7]**.

For the evaluated configuration only the dedicated port is allowed to manage CIMC. The NIC Mode must be set to "Dedicated". Refer to "Configuring Network-Related Settings" within [3] and [9] to set the Nic mode to dedicated.

3.3.2. Server Ports

For configuration options and procedures related to server ports, refer to "Server NIC Configuration in **[3], [9]**.

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 CIMC 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 to provide remote authentication, time, or logging service. In

standalone mode only one VLAN can be enabled. For configuration options and procedures, refer to "Managing Network Adapters" in **[3], [9]**.

3.3.4. Serial over Lan (SoL)

Serial Over Lan (SOL) enables an administrator to connect remotely to a single server. Native serial redirection and SoL can not be used simultaneously.

By default (SoL) is Disabled. Refer to "Smart Serial" in [1]

For the evaluated configuration SoL must be DISABLED.

Refer to "Managing Remote Presence – Configuring serial Over Lan" [3] and [9] to ensure SoL is disabled.

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. CIMC 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.

  CIMC 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 CIMC.

  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. CIMC 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 HTTP" in **[3],[9]**.
    - 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:!EXPORT
        56:!LOW:!MEDIUM:!eNULL:!RC4:!DES:!3
        DES:+HIGH:+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 CIMC 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, CIMC will negotiate the connection using the same ciphersuite that would be used with the Java-based CIMC Client, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, if the browser supports that ciphersuite, otherwise CIMC 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 ""Configuring HTTP" in **[3],[9]**.
  - 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 **[3]**.
  - 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

-

- 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 "LDAP Servers" in **[3], [9]**. 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 "Sending the Cisco IMC Log to a Remote Server" in **[3], [9]**. To enable the transmitting of syslog messages to remote syslog servers (up to 2 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.

- 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 only one role.

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 ‘Configuring Local Users **[3], [9]**.

4.1.1. Default Roles and Privileges

The system contains the following default user roles:

- Admin: Complete read-and-write access to the entire system. A user with this role can perform all actions available through the GUI and CLI. The default admin account is assigned this role by default and this association cannot be changed.
- User: user with this role can perform the following tasks:
  - View all information
  - Manage the power control options such as power on, power cycle, and power off
  - Launch the KVM console and virtual media
  - Clear all logs
  - Ping.
- Read-Only: Read-only access to system configuration with no privileges to modify the system state.

4.1.2. Custom Roles and Modification of Default Roles

New custom roles can not be created and default roles can not be modified or deleted.

4.2. Passwords

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

- Minimum of 8 and a maximum of 20 characters long;
- Does not contain the user’s name;
- Contains characters from three of these four categories:
  - English uppercase characters (A through Z);
  - English lowercase characters (a through z);
  - Base 10 digits (0 through 9);
- Non-alphabetic characters (!, @, #, $, %, ^, &, *, -, _, +, =).

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 admin privilege. For more information, refer to "Managing User Accounts" in **[3],[9]**.

4.4. Account Expiration, Deletion 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 "Enabling Password Expiry" in **[3], [9]**.

To delete a user account, the administrator must follow the following steps.

- Go to User Management>Session Management, check whether the user has an active session. The administrator terminates the active session by selecting the session and clicking on the "Terminate session" tab. The user session will be terminated immediately.
- Go to Admin>User Management>Local User Management. Selects the account to be deleted and click the tab "Delete User".

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 CIMC 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 > Network > NTP Setting, and enter the hostname or IP address of the NTP server.

For more information, refer to "Configuring Network Time Protocol Settings" in **[3], [9]**.

In the evaluated configuration, the time zone should be set as desired when CIMC 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 CIMC into the syslog message is not accurate, and does not match what would be displayed on the CIMC CLI using the "show clock" or "show timezone" commands.

4.6. Identification and Authentication

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

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

4.7. Common Criteria and FIPS Mode

In the evaluated configuration, it is recommended, that CIMC be configured to have FIPS and Common Criteria enabled.

To enable via the GUI, under Admin, click Security Management>Security Configuration.

In the work pane tick Enable FIPS checkbox and Enable CC checkbox.

For more information, refer to "Managing Certificates and server Security" in **[3],** Viewing Network Adapter Properties **[9]**.

Note: When you switch the FIPS mode, it restarts the SSH, KVM, SNMP, webserver, XMLAPI, and redfish services in configurations that only support FIPS-approved algorithms.

4.8. Cisco Intersight Management

In the evaluated configuration, Intersight management must be disabled. In the evaluated TOE, bi-directional communication between the Intersight Cloud application and the server is not allowed.

To disable via the GUI, under Admin click Device Connector. In Settings>General ensure the Device Connector tab is "OFF".

For more information, refer to "Enabling or Disabling Cisco Intersight Management" in **[3]**.

4.9. Removable Media

Each server provides a number of optional removable media. Removable media is outside the scope of the evaluation.

Note: Use of virtual media (via the virtual KVM interface) is still permitted.

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 CIMC instance. 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: CIMC 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 CIMC 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 CIMC 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 refer “Viewing Faults and Logs” to **[3],[9]**.

5.2. Deleting Audit Records

The storage capacity for each log type is 131,068 records, and is not configurable. When each log reaches capacity, the oldest records are overwritten by new records. It is possible for users with admin and user role to clear logs.

For more information refer “Viewing Faults and Logs” to **[3],[9]**.

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 8 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 Integrated Management Controller (CIMC), version 4.0(4x) as described in section 1.3 of the document.
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	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

	from the Fabric Interconnect to a management workstation.	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

7.2. 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 any time, 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