Cisco Unified Computing System - Standalone

Security Target

Version: 1.0
Date: 14 April 2020

Contents

Table of Tables

Table of Figures

Document Introduction

Prepared By:
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), Cisco Unified Computing System Standalone. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements, and the IT security functions provided by the TOE which meet the set of requirements. Administrators of the TOE will be referred to as administrators, Authorized Administrators, TOE administrators, semi-privileged, privileged administrators, and security administrators in this document.

1 Security Target Introduction

This Security Target contains the following sections:

- Security Target Introduction
- Conformance Claims
- Security Problem Definition
- Security Objectives
- Security Requirements
- TOE Summary Specification
- References

The structure and content of this ST comply with the requirements specified in the Common Criteria (CC), Part 1, Annex A, and Part 2.

1.1 ST and TOE Reference

This section provides information needed to identify and control this ST and its TOE.

Table 1. ST and TOE Identification

Name	Description
ST Title	Cisco Unified Computing System Standalone Security Target
ST Version	1.0
Publication Date	14 April 2020
TOE Guidance	Cisco Unified Computing System Standalone version 4.0(4i) Common Criteria Operational User Guidance and Preparative Procedures, v1.0
Vendor and ST Author	Cisco Systems, Inc.
TOE Reference	Cisco Unified Computing System Standalone
TOE Hardware Models	Cisco UCS C-Series Rack Servers (C220 M5, C240 M5, C480 M5 and C480 ML M5) Cisco UCS S-Series Rack Servers (S3260 M5) Virtual Interface Cards (see listing in section 1.3.3)
TOE Software Version	Cisco Integrated Management Controller (CIMC) 4.0(4i)
Keywords	Virtualization, role-based access control, authentication

1.2 TOE Overview

The Target of Evaluation (TOE) is a Cisco UCS standalone rack servers that are rack-mounted Cisco UCS servers that are managed by the Cisco Integrated Management Controller (CIMC) rather than the Cisco UCS Manager. This currently includes Cisco UCS C-Series Rack Servers and Cisco UCS S-Series Storage Servers.

1.2.1 TOE Product Type

The TOE is a network device that consists of hardware and software components that support Cisco Unified Systems, running in standalone mode. The TOE features a role based access control policy to control the separation of administrative duties and provide a security log of all changes made.

In standalone mode each UCS C-Series and S Series server runs as an independent system. The Cisco Integrated Management Controller (CIMC) manages each platform as an individual entity in a Data Center or across remote locations. The Cisco UCS Standalone consists of the following primary hardware elements: –

- Cisco UCS C-Series Rack Servers (C220 M5, C240 M5, C480 M5 and C480 ML M5)
- Cisco UCS S-Series Rack Servers (S3260 M5)
- Virtual Interface Cards (see listing in section 1.3.3)

1.2.2 Required non-TOE Hardware/Software/Firmware

The TOE requires the following hardware/software/firmware in the IT environment when the TOE is configured in its evaluated configuration

Table 2. ST and TOE Identification

Component	Required	Usage/Purpose/Description
UCS Management Workstation (The host operating system upon which the CIMC client application runs.)	Yes	The GUI of the Cisco UCS CIMC is a Java-based application that allows remote administration of CIMC over TLS. The GUI, requires Sun JRE 1.7 or later, which is part of the IT environment. •The UCS CIMC uses web start 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
SSHv2 Client	No	CIMC can be managed remotely via SSHv2.
Remote Authentication Server	No	A LDAP server is an optional component of the operational environment.
SNMP v3 Server	No	An SNMPv3 Server is an optional component of the operational environment.

Component	Required	Usage/Purpose/Description
Syslog Server	No	A syslog server is an optional component for use with the TOE. It is a supplemental storage system for audit logs, but it does not provide audit log storage for the TOE. Failed authentication attempts are not logged to the local audit log, but are sent to a remote syslog server.
NTP Server	No	An NTP server is an optional component of the operational environment that would allow for synchronizing the TOE clocks with an external time source.
Firewall	Yes	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.

1.3 TOE Description

This section provides an overview of the Cisco Unified Computing System Target of Evaluation (TOE). This section also defines the TOE components included in the evaluated configuration of the TOE. The TOE consists of a minimum of one of each of the following components:

- Rack-Mount Server configurations (running CIMC):
  - One or more Cisco UCS Rack Servers:
    - Any of: C220 M5, C240 M5, C480 M5 or C480 ML M5
  - Cisco Integrated Management Controller (CIMC) 4.0(4)
- Storage Server configurations (running CIMC):
  - One or more Cisco UCS Storage Servers (S3260 M5)
  - Cisco Integrated Management Controller (CIMC) 4.0(4)

1.3.1 Cisco UCS Rack Mount C-Series Servers

UCS Rack Mount Servers, also known as C-Series Servers (, C220 M5, C240 M5, C480 M5 and C480 ML M5) extend UCS functionality to an industry-standard form factor and are designed for compatibility, and performance, and enable organizations to deploy systems incrementally, using as many or as few servers as needed.

The Rack Mount Servers support certain optional network adapters, none of which provides security functionality described in the ST. For a full compatibility matrix, refer to the Hardware and Software Interoperability Matrix for C-Series Servers referenced from the Cisco UCS Hardware and Software Compatibility available at https://ucshcltool.cloudapps.cisco.com/public/. Any software installed to the rack servers, including hypervisors and guest operating systems, is outside the TOE boundary.

1.3.2 Cisco UCS S-Series Storage Servers

UCS S-Series Storage Servers, also known as S-Series Servers (S3260 M5) is a modular, high-density, high-availability, dual-node storage- optimized server.

The S-series is a modular architecture that allows components be upgraded independently. The Rack Mount Servers support certain optional network adapters, none of which provides security functionality described in the ST. For a full compatibility matrix, refer to the Hardware and Software Interoperability Matrix for S-Series Servers referenced from the Cisco UCS Hardware and Software Compatibility available at https://ucshcltool.cloudapps.cisco.com/public/. Any software installed to the storage servers, including hypervisors and guest operating systems, is outside the TOE boundary.

1.3.3 Virtual Interface Cards (VIC) and other Network Adapters

Several network adapters, including Cisco UCS Virtual Interface Cards (VIC) are compatible with the TOE but do not enforce the security functionality described in this Security Target.

Network Adapters and Virtual Interface Cards compatible with C-Series 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

Network Adapters and Virtual Interface Cards compatible with S-Series Servers:

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

1.3.4 Cisco Integrated Management Controller (CIMC)

The UCS CIMC is the management module. UCS CIMC only runs in standalone mode and manages a server via the CIMC XML API, with both CLI and GUI options, enabling near real time configuration and reconfiguration of resources.

The software's role-based design supports existing best practices, allowing server, network, and storage administrators to contribute their specific subject matter expertise to a system design. It allows secure management of the TOE using TLS1.2, and SSHv2, and monitoring using SNMPv3 (read only).

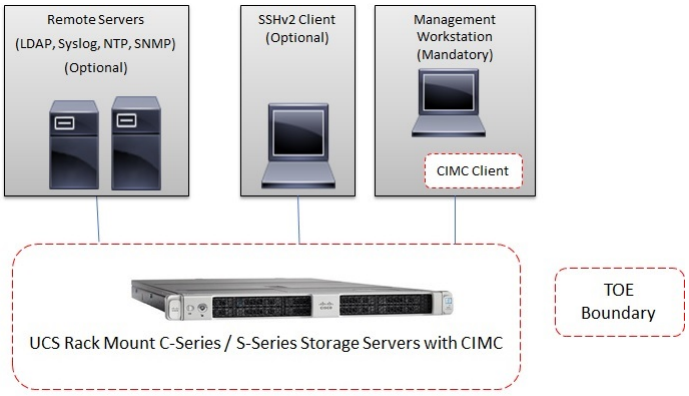
The UCS CIMC software is divided into two components: server and client side. The server side component is installed on the server. The server side component contains the XML based server daemon (XML API) that receives requests from the three different client access methods: GUI, CLI, and XML. The client side component (CIMC GUI) is a java application that provides the GUI for the administrator.

1.4 TOE Evaluated Configuration

The following figure provides a visual depiction of an example TOE deployment. The TOE boundary includes all the hardware shown within Figure 1 and the CIMC firmware installed on the server. The hard drives, processors, network cards, memory are non-interfering.

In this topology, the remote servers, such as syslog, and NTP could be hosted on UCS servers, or third-party rack servers, or across the LAN Core.

Figure 1. TOE and Environment



1.5 Physical Scope of the TOE

The TOE is a hardware and software solution that makes up the Cisco Unified Computing System, and the TOE guidance documentation.

The TOE guidance documentation that is considered to be part of the TOE is the Cisco UCS Standalone Common Criteria Operational User Guidance and Preparative Procedures, a PDF document that, along with other PDF-based guidance referenced therein, can be obtained from the https://cisco.com web site.

The TOE hardware platforms are described in Table 3 Hardware Models and Specifications. For ordering of the TOE and delivery via commercial carriers, see https://apps.cisco.com/ccw/cpc/guest/home.

The firmware for the TOE is downloaded from https://software.Cisco.com Software. During TOE installation and upgrades of the firmware is initially uploaded to the server via the KVM console accessed via Cisco UCS CIMC (Cisco UCS CIMC identifies the component to be updated as BMC). The firmware is an iso image, and is found under "UCS C-Series Rack-Mount Standalone Server Software" and under "UCS S-Series Storage Servers" under as:

- Unified Computing System (UCS) Server Firmware

The software file format for the TOE is an iso file. The individual component firmware versions are identified with the version listed in the Software / Firmware section of the table below. For ordering and downloading the TOE software/firmware, see https://software.cisco.com/#.

The firmware located in the following directories in UCS C-Series Rack-Mount Standalone Server are outside the scope of the TOE:

- Unified Computing System (UCS) Capabilities Catalog
- Unified Computing System (UCS) Diagnostics
- Unified Computing System (UCS) Drivers
- Unified Computing System (UCS) Server Configuration Utility
- Unified Computing System (UCS) Utilities

The TOE is comprised of the following physical specifications as described in Table 3 below:

Table 3. Hardware Models and Description

Hardware Platform	Image	Processor	Size	Power	Interfaces
C-Series Rack Servers					
UCS C220 M5		One or two Intel® Xeon® processor scalable family CPUs	1RU: 1.7x16.89x29.8in (4.32x43x75.5cm)	Available with four types of power supplies: • 770W (AC) • 1050W (AC) • 1050W V2 (DC) 1600W (AC)	Front • Up to 10 drives • One KVM connector Rear • Two PCIe riser • One mLOM • Two USB 3.0 port • 1-Gb Ethernet dedicated management por • One RJ-45 connector serial port • Dual 1/10 Gb Ethernet portss VGA video port
UCS C240 M5		One or two Intel® Xeon® processor scalable family CPUs	2RU: 1.7x16.89x29.8in	Hot-pluggable, redundant 770W AC, 1050W AC, 1050W DC, and 1600W AC	Front • Up to 24 drives • One KVM connector Rear • Two PCIe riser • Two 2.5 inch drive • One mLOM • Two USB 3.0 port • 1-Gb Ethernet dedicated management por • One RJ-45 connector serial port • Two embedded (on the motherboard) Intel i350 GbE Ethernet controller ports
UCS C480 M5		Intel® Xeon® Scalable CPUs (2 or 4)	4RU: 16.9x19x32.7in (176x483x830cm)	Hot-pluggable, redundant 1600W AC	Front • Up to 24 hot swappable SAS/SATa drives

Hardware Platform	Image	Processor	Size	Power	Interfaces
					• One KVM console connector • Two CPU module bays Rear • Twelve PCIe slots • One serial port (DB-9) • One VGA video port (DB-15) • One 10/100/1000 Ethernet dedicated management port M1 • onw 10 Gb Ethernet port Three USB 2.0 ports
UCS C480 ML M5		Intel Xeon Scalable CPUs (2)	4RU: 6.9x19x32.7in (176x483x830cm)	1600W AC Power Supp	Front • Up to 24 hot swappable SAS/SATa drives • One KVM console connector • Two CPU module bays Rear • PCIe slots 11-14 • One serial port (DB-9) • One VGA video port (DB-15) • One 10/100/1000 Ethernet dedicated management port M1 • One 1Gb/ 10 Gb Ethernet port Three USB 2.0 ports
S-Series Storage Servers					

Hardware Platform	Image	Processor	Size	Power	Interfaces
S3260 M5		Dual Intel Xeon Scalable processors or E5-2600 v4 product family CPUs per server node. • M5 server node processors: Intel Xeon Scalable processor 4110, 4114, 5115, 6132, 6138, 6152	4RU height x 32-in. depth	4 hot-pluggable, N+N redundant 1050-watt (W) AC or DC 80 PLUS Platinum efficiency power supplies	Rear • Two server bays • Two System I/O controller (SIOC) • QSFP ports (two on each SIOC) • Chassis Management Controller (CMC) Debug Firmware Utility port (one each SIOC • 10/100/1000 dedicated management port, RJ-45 connector (one each SIOC) • Four SSDs drivebays • KVM console connector 1Gb Ethernet deicated management port (RJ-45)
Virtual Interface cards	See section 1.3.3				
Software / Firmware	Cisco Integrated Management Controller (CIMC) 4.0(4i)				
Guidance Documents	Cisco Unified Computing System Standalone version 4.0(4i) Common Criteria Operational User Guidance and Preparative Procedures, v1.0				

1.6 Logical Scope of the TOE

The TOE is comprised of several security features. Each of the security features identified above consists of several security functionalities, as identified below.

- Security Audit
- Identification and Authentication
- Security Management
- Protection of TSF
- Role Based Access Control

These features are described in more detail in the subsections below.

1.6.1 Security Audit

The Unified Computing System stores audit information in three different formats: audit log, events, and faults. This information is compiled to assist the administrator in monitoring the security state of the UCS as well as trouble shooting various problems that arise throughout the operation of the system. All three types of information are stored within a SQLite database stored on the server. The database is internal only and does not provide any externally visible interfaces for communication. In standalone mode, all audit data is stored locally. The TOE may be configured to send records to an external syslog server, in which case syslog is a supplemental service for monitoring, alerting and reporting, not the audit log storage mechanism of the TOE. Audit log storage and protection functionality comes from the TOE itself.

The UCS CIMC TOE component provides the ability to audit the actions taken by authorized administrators. Audited events include start-up and shutdown, configuration changes, administrative authentication, and administrative log-off. The TOE provides the capability for authorized administrators to review the audit records stored within the TOE.

1.6.2 Identification and Authentication

Cisco UCS supports two methods of authenticating administrator logins on the Cisco UCS CIMC: a local user database of passwords or a remote authentication server accessed either via LDAP. The TOE may be configured to use either the local user database or one of the remote authentication methods, but multiple authentication methods may not be selected. Remote authentication may be used to centralize user account management to an external authentication server.

The system has a default user account, admin, which cannot be modified or deleted. This account is the system administrator account and has full privileges.

Each user account must have a unique user name that does not start with a number. For authentication purposes, a password is required for each user account.

User accounts can be configured to expire at a predefined time. When the expiration time is reached the account is locked and must be unlocked by an authorized administrator. By default, user accounts do not expire.

1.6.3 Security Management

UCS can be managed using the graphical user interface (over TLS1.2), the command line (over SSHv2 or by local console access via the RS-232 port), or by manipulating an XML API. Each of these interfaces can be used in the evaluated configuration to administer the UCS. The interfaces all operate on the same XML data structures and provide identical functionality. For all management channels, users have a default read-only authorization to access non-sensitive management objects (passwords are never exposed to an external management interface). Additional user privileges each grant access to modify specific management objects.

An administrator can use Cisco UCS CIMC to perform management tasks for all physical and virtual devices within a Cisco UCS instance.

1.6.3.1 Cisco UCS Hardware Management

An administrator can use CIMC to manage all hardware within a Cisco UCS instance, including the following:

- Chassis (not security-relevant to the TSF)
- Fans (not security-relevant to the TSF)
- Ports
- Cards
- Slots
- I/O modules

1.6.3.2 Cisco UCS Resource Management

An administrator can use Cisco CIMC to create and manage all resources within a Cisco UCS instance, including the following:

- World Wide Name (WWN) addresses, used in Storage Area Networks
- Bandwidth (not security-relevant to the TSF)

1.6.3.3 Server Administration in a Cisco UCS Instance

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

- Monitor faults, alarms, and the status of equipment.

1.6.3.4 Network Administration in a Cisco UCS Instance

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

- Enable a VLAN
- Configure IP blocking and filtering
- Configure the quality of service classes and definitions
- Configuring NTP

1.6.3.5 Storage Administration in a Cisco UCS Instance

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

- Configure ports, port channels, and SAN
- Configure the quality of service classes and definitions

1.6.3.6 Tasks that Cannot be Performed in Cisco CIMC

Cisco UCS CIMC cannot be used to perform system management tasks that are not specifically related to device management within a Cisco UCS instance.

Cross-System Management is not permitted. An administrator cannot use Cisco UCS CIMC to manage more than one system.

Provisioning and management of operating systems and applications is not permitted. Cisco UCS CIMC provisions a server and, as a result, exists below the operating system on a server. Therefore, you cannot use it to provision or manage operating systems or applications on other servers.

1.6.3.7 UCS Secure Access

The UCS CIMC provides access for an administrator using SSHv2, TLS1.2, or SNMPv3.

SSHv2 is used to access the command line interface for the UCS CIMC. SSHv2 authentication uses the UCS CIMC username and password. The command line interface is also accessible over the local serial port.

TLS1.2 is used to access the UCS CIMC interface. The UCS CIMC interface serves as a launch point for the Java application which also utilizes TLS1.2 to protect the confidentially of the information.

SNMPv3 is used to export system traps and support remote monitoring (read only). SNMPv3 includes support for SHA authentication and AES-128 for protection of the confidential system information.

1.6.3.8 UCS XML API

The XML API is a way to integrate or interact with the Unified Computing System (UCS), because XML is the native format of communication within the UCS. For example, both the CLI and GUI use the same XML API to communicate with the CIMC. The UCS XML interface accepts XML documents (APIs) sent over HTTPS. Client developers can use the programming language of their choice generate XML documents containing the API methods.

1.6.4 Protection of the TSF

The TOE internally maintains the date and time. This date and time is used as the timestamp that is applied to audit records generated by the TOE. The TOE provides the Authorized Administrators the capability to change the timezone in order to update the TOE's clock to maintain a reliable timestamp. The timestamp is updated accordingly when the timezone is changed.

1.6.5 Role Based Access Control

Role-Based Access Control (RBAC) is a method of restricting or authorizing system access for users based on user roles. A role defines the privileges of a user in the system that a user is allowed access. Because users are not directly assigned privileges, management of individual user privileges is simply a matter of assigning the appropriate roles.

A user is granted write access to desired system resources only if the assigned role grants the access privileges allows access. For example, a user with the Server Administrator role could update server configurations.

Privileges

Privileges give their holder access to specific system resources and permission to perform specific tasks. The following table lists each privilege and the user role given that privilege by default.

Table 4 Privileges and Default Role Assignments

Privilege	Management Capabilities	Default Role Assignment
admin	System administration	Administrator
read-only	Read-only access.	Read-Only
User	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 Toggle the locator LED Ping an IP address	User

User Roles

User roles contain one or more privileges that define the operations allowed for the user who is assigned the role. A user cannot be assigned more than 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.

The system contains the following default user roles:

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.

Read-Only: Read-only access to system configuration with no privileges to modify the system state.

User: 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 and Ping an IP address.

A role can not be deleted.

1.7 Excluded Functionality

The following functionality is excluded from the evaluation.

- C-Series (Rack Mount) Servers and S-Series Storage Servers managed by UCS Manager are not supported in standalone mode.; C-Series servers and S-Series Storage Servers must be managed by UCS 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. In UCS, the common information model (CIM)-XML is used for server hardware monitoring. (CIM-XML is a different interface than the XML API used by the UCS CIMC GUI and UCS CIMC CLI.)
- All other functionality is supported in the evaluated configuration.

2 Conformance Claims

2.1 Common Criteria Conformance Claim

The ST and the TOE it describes are conformant with the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, Version 3.1, Revision 5, April 2017
    - Part 2 Conformant
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1, Revision 5, April 2017
    - Part 3 Conformant

The ST and TOE are package conformant to evaluation assurance package: EAL2.

2.2 Protection Profile Conformance Claim

This ST claims no compliance to any Protection Profiles.

3 Security Problem Definition

This chapter identifies the following:

- Significant assumptions about the TOE's operational environment.
- IT related threats to the organization countered by the TOE.
- Environmental threats requiring controls to provide sufficient protection.
- Organizational security policies for the TOE as appropriate.

This document identifies assumptions as A.assumption with "assumption" specifying a unique name. Threats are identified as T.threat with "threat" specifying a unique name. Organizational Security Policies (OSPs) are identified as P.osp with "osp" specifying a unique name.

3.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 5. TOE Assumptions

Assumption	Assumption Definition
A.ADMIN	All authorized administrators are assumed not evil, will follow TOE administrative guidance, and will not disrupt the operation of the UCS system intentionally.
A.BOUNDARY	The UCS system must be separated from public/untrusted networks by a firewall such that remote access to the TOE interfaces and management workstations is prohibited from untrusted networks and only allowed from trusted networks.
A.PHYSICAL	The facility housing the UCS system must 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.
A.POWER	The facility housing the UCS system must have a power management strategy using UPS or backup generators to ensure that power continues to flow under any adverse conditions.
A.REDUNDANT_NET	The network connectivity feeding the UCS system in the datacenter must provide redundant links to protect against network administrator operator error or network equipment failure.
A.REMOTE_SERVERS	When remote servers are used, such as SNMP server, syslog server, or NTP server communications between the TOE and the remote servers shall be protected.

3.2 Threats

The following table lists the threats addressed by the TOE and the IT Environment. The assumed level of expertise of the attacker for all the threats identified below is Basic.

Table 6. Threats

Threat	Threat Definition
T.NOAUTH	A system user (VM user, OS administrator) attempts to bypass the security of the UCS CIMC so as to access and use security functions and/or non-security functions resulting in a compromise of the TSF.
T.SNIFF	A hacker places network-sniffing software between a remote administrator and the UCS CIMC and records authentication information.
T.ACCOUNTABILITY	A TOE administrator is not accountable for their actions on the TOE because the audit records are not generated or reviewed.

3.3 Organizational Security Policies

No Organizational Security Polices (OSPs) have been defined for this TOE.

4 Security Objectives

This Chapter identifies the security objectives of the TOE and the IT Environment. The security objectives identify the responsibilities of the TOE and the TOE's IT environment in meeting the security needs.

This document identifies objectives of the TOE as O.objective with objective specifying a unique name. Objectives that apply to the IT environment are designated as OE.objective with objective specifying a unique name.

4.1 Security Objectives for the TOE

The following table, Security Objectives for the TOE, identifies the security objectives of the TOE. These security objectives reflect the stated intent to counter identified threats and/or comply with any security policies identified. An explanation of the relationship between the objectives and the threats/policies is provided in the rationale section of this document.

Table 7. Security Objectives for the TOE

TOE Security Objective	TOE Security Objective Definition
O.IDAUTH	The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions or, for certain specified services, to a connected network.
O.ENCRYP	The TOE must protect the confidentiality of its dialogue with an authorized administrator through encryption, if the TOE allows administration to occur remotely from a connected network.
O.AUDREC	The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes.
O.ACCOUN	The TOE must provide user accountability for information flows through the TOE and for all use of security functions related to audit.
O.SECFUN	The TOE must provide functionality that enables an authorized administrator to use the TOE security functions and must ensure that only authorized administrators are able to access such functionality.
O.ADMIN	The TOE must provide a secure channel for administration.

4.2 Security Objectives for the Environment

All of the assumptions stated in Section Security Problem Definition – Assumptions, are considered to be security objectives for the environment. The following are the non-IT security objectives, which, in addition to those assumptions, are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 8. Security Objectives for the Environment

Environment Security Objective	IT Environment Security Objective Definition
OE.ADMIN	Personnel measures are in place to ensure well trained and trusted administrators are authorized to manage the TOE.
OE.BOUNDARY	The UCS system must be separated from 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.
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.
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.
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.

5 Security Requirements

This section identifies the Security Functional Requirements for the TOE. The Security Functional Requirements included in this section are derived from Part 2 of the *Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, dated: April 2017* and all international interpretations.

5.1 Conventions

The CC defines operations on Security Functional Requirements: assignments, selections, assignments within selections and refinements. This document uses the following font conventions to identify the operations defined by the CC.

Table 9. Security Requirement Conventions

Convention	Indication
Assignment	Allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [[***selected-assignment***]])
Selection	Allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
Iteration	Allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a number placed at the end of the component. (e.g., (1), (2), (3).)
Refinement	Allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
Extended Requirements	Are identified with "(EXT)" in of the functional class/name and are those not found in Part 2 of the CC.
Other	sections of the ST use bolding to highlight text of special interest, such as captions.

5.2 TOE Security Functional Requirements

This section identifies the Security Functional Requirements for the TOE. The TOE Security Functional Requirements that appear in the following table are described in more detail in the following subsections

Table 10. Security Functional Requirements

Class Name	Component Identification	Component Name
FAU: Security Audit	FAU_GEN.1	Audit data generation
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
	FAU_STG.1	Protected audit trail storage
	FAU_STG.4	Prevention of audit data loss
FDP: User Data Protection	FDP_ACC.2	Complete access control

Class Name	Component Identification	Component Name
	FDP_ACF.1	Security attribute based access control
FIA: Identification and authentication	FIA_ATD.1	User attribute definition
	FIA_SOS.1	Verification of secrets
	FIA_UAU.2	Timing of authentication
	FIA_UAU.5	Multiple authentication mechanisms
	FIA_UID.2	User identification before any action
FMT: Security management	FMT_MOF.1	Management of security functions behavior
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialization
	FMT_MTD.1	Management of TSF data
	FMT_SAE.1	Time-based authorization
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
FPT: Protection of the TSF	FPT_STM.1	Reliable time stamps
FTP: Trusted path/channels	FTP_TRP.1	Trusted Path

5.3 Class: Security Audit (FAU)

5.3.1 FAU_GEN.1 – Audit Data Generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [***not specified***] level of audit; and

c) [**the events listed in** Error! Reference source not found.].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the cPP/ST, [**information specified in column three of** Error! Reference source not found.].

Table 11. Auditable Events

SFR	Auditable Event	Additional Audit Record Contents
FMT_SMR.1	Modifications to user role assignments.	The identity of the authorized administrator performing the modification, user identity being modified, and details being associated with the authorized administrator role.
FIA_UAU.5	Use of the user authentication mechanism on CIMC CLI and GUI	The user identities provided to the CIMC.

SFR	Auditable Event	Additional Audit Record Contents
FDP_ACF.1	Role-based access control requests submitted via the CIMC CLI, and GUI.	The user identity requesting the change and the object being accessed.
FPT_STM.1	Attempts to change the time.	The identity of the authorized administrator performing the operation.
FTP_TRP.1	Attempts to use the trusted path functions.	Identification of the user associated with all trusted path invocations including failures, if available.

5.3.2 FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide [**an authorized administrator**] with the capability to read [**all locally stored audit trail data**] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.3.3 FAU_SAR.3 Selectable audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [**sorting and filtering**] of audit data based on:

a) [**record identifier**;

b) **affected object**;

c) **user**]

5.3.4 FAU_STG.1 Protected audit trail storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to [***prevent***] unauthorized modifications to the stored audit records in the audit trail.

5.3.5 FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1 The TSF shall [***overwrite the oldest stored audit records***] and [***no other actions***] if the audit trail is full.

5.4 Class: User Data Protection (FDP)

5.4.1 FDP_ACC.2 Complete access control

FDP_ACC.2.1 The TSF shall enforce the [**role based access control SFP**] on [Subjects: **Authenticated Administrators**; Objects: **Resources, Configuration Settings**] and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

5.4.2 FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the [**role based access control SFP**] to objects based on the following: [

Subject security attributes:

- **Authenticated Administrators:**
    - **User Identity – Identity of the administrator**

- **Privileges – The cumulative set of privileges obtained from the roles assigned to the Authenticated Administrator.**

Object security attributes:

- **Configuration Settings**
  - **Privilege – The privilege that an Authenticated Administrator must hold in order to write to the configuration setting**].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

- **Authenticated Administrators are granted access to Resources. Authenticated**
- **Authenticated Administrators whose set of Privileges includes the Privilege attribute of the Configuration Setting being accessed are granted read and write access to the object, or,**
- **Authenticated Administrators whose set of Privileges does not include the Privilege attribute of the Configuration Setting being accessed are granted read-only to the Configuration Setting for resources in which the Administrator has access**].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**none**].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [**none**].

5.5 Class: Identification and Authentication (FIA)

5.5.1 FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [

For all user types (CIMC, and SNMPv3):

a) login id;

b) password;

and for CIMC users only:

c) account expiration date;

And for SNMPv3 users only:

d) privacy password].

5.5.2 FIA_SOS.1 Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [

- **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 (!, @, #, $, %, ^, &, *, -, _, +, =).**
-].

Application Note: This requirement applies to the local password database and on the password selection functions provided by the TOE (for administrative accounts only, not SNMPv3 passwords), but remote authentication servers may have preconfigured passwords which do not meet the quality metrics.

5.5.3 FIA_UAU.2 User authentication before any action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.5.4 FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.5.1 The TSF shall provide [

- **Local authentication:**
  - **Password;**
- **Remote authentication:**
  - **LDAP;**

] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [**verification of local authentication password or by querying a remote authentication server**].

5.5.5 FIA_UID.2 User identification before any action

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.6 Class: Security Management (FMT)

5.6.1 FMT_MOF.1 – Management of Security Functions Behavior

FMT_MOF.1.1 The TSF shall restrict the ability to [***determine the behavior of, disable, enable, modify the behaviour of***] the functions [**described in FMT_SMF.1**] to [**administrative roles defined in FMT_SMR.**1].

5.6.2 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [**role based access control SFP**] to restrict the ability to [***modify,* [*none*]**]] the security attributes [**listed in section FDP_ACF1.1**] to [**Administrator**].

5.6.3 FMT_MSA.3 Static attributes initialisation

FMT_MSA.3.1 The TSF shall enforce the [**role based access control SFP**] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow [**Administrator**] to specify alternative initial values to override the default values when an object or information is created.

5.6.4 FMT_MTD.1 Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to [***set***] the [**timezone used to form the timestamps in FPT_STM.1.1**] to [**Administrator**].

5.6.5 FMT_SAE.1 Time-limited authorisation

FMT_SAE.1.1 The TSF shall restrict the capability to specify an expiration time for [**CIMC accounts**] to [**Administrato**r].

FMT_SAE.2.1 For each of these security attributes, the TSF shall be able to [**lock expired CIMC accounts**] after the expiration time for the indicated security attribute has passed.

Application note: By default, CIMC accounts are not set to expire, but expiration can be enabled and an “expiration date” value set for any CIMC account. Expired accounts can be unlocked be changing the expiration date to a future date.

5.6.6 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

[

a) **Determine and modify the behavior of the audit trail management;**

b) **Query, modify, delete, and assign the user attributes defined in FIA_ATD.1.1;**

c) **Set the timezone for FPT_STM.1.1**.].

5.6.7 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles [

- **admin (Administrator)**
- **read-only (Read-Only)**
- **User**].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Application note: This SFR identifies the subset of CIMC account privileges relevant to Security Management (FMT) requirements in this ST

5.7 Class: Protection of the TSF (FPT)

5.7.1 FPT_STM.1 – Reliable Time Stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

5.8 Class: Trusted Path/Channels (FTP)

5.8.1 FTP_TRP.1 – Trusted Path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [***remote***] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [***modification, disclosure***].

FTP_TRP.1.2 The TSF shall permit [***remote users***] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [***initial user authentication, [and management of the TOE via administrative interfaces***]].

Application note: Remote administrative interfaces relevant to this SFR include the CIMC CLI (via SSH), CIMC GUI or custom queries to the XML API (via TLS), and SNMPv3. The interfaces that would support remote administration are all disabled by default and remain disabled in the CC-certified configuration: CIM-XML, HTTP, IPMI, SNMP (other than SNMPv3), and Telnet.

5.9 TOE SFR Dependencies Rationale

This section of the Security Target demonstrates that the identified TOE Security Functional Requirements include the appropriate hierarchical SFRs and dependent SFRs. The following table lists the TOE Security Functional Components and the Security Functional Components, each are hierarchical to and dependent upon and any necessary rationale.

N/A in the Rationale column means the Security Functional Requirement has no dependencies and therefore, no dependency rationale is required. Satisfied in the Rationale column means the Security Functional Requirements dependency was included in the ST.

Table 12. SFR Dependency Rationale

SFR	Dependency	Rationale
FAU_GEN.1	FPT_STM.1	Met by FPT_STM.1
FAU_SAR.1	FAU_GEN.1	Met by FAU_GEN.1
FAU_SAR.3	FAU_SAR.1	Met by FAU_SAR.1
FAU_STG.1	FAU_GEN.1	Met by FAU_GEN.1
FAU_STG.4	FAU_STG.1	Met by FAU_STG.1
FDP_ACC.2	FDP_ACF.1	Met by FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	Met by FDP_ACC.2 Met by FMT_MSA.3
FIA_ATD.1	No dependencies	N/A
FIA_SOS.1	No dependencies	N/A
FIA_UAU.2	FIA_UID.1	Met by FIA_UID.1
FIA_UAU.5	No dependencies	N/A
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	Met by FMT_SMR.1 Met by FMT_SMF.1N/A
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Met by FDP_ACC.1 Met by FMT_SMR.1 Met by FMT_SMF.1
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Met by FMT_SMR.1 Met by FMT_MSA.1
FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	Met by FMT_SMF.1 Met by FMT_SMR.1
FMT_SAE.1	FMT_SMR.1 FMT_STM.1	Met by FMT_SMR.1 Met by FMT_STM.1
FMT_SMF.1	No dependencies	N/A
FMT_SMR.1	FIA_UID.1	Met by FIA_UID.2
FPT_STM.1	No dependencies	N/A
FTP_TRP.1	No dependencies	N/A

5.10 Security Assurance Requirements

The TOE assurance requirements for this ST are EAL2 derived from Common Criteria Version 3.1, Revision 5. The assurance requirements are summarized in the table below.

Table 13. Assurance Requirements

Assurance Class	Component	Components Description
Development (ADV)	ADV_ARC.1	Architectural Design with domain separation and non-bypassability
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance Documents (AGD)	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative User guidance
Life Cycle Support (ALC)	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
Tests (ATE)	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability Assessment (AVA)	AVA_VAN.2	Vulnerability analysis

5.11 Security Assurance Requirements Rationale

This Security Target claims conformance to EAL2. This target was chosen to ensure that the TOE has a moderate level of assurance in enforcing its security functions when instantiated in its intended environment which imposes no restrictions on assumed activity on applicable networks.

5.12 Assurance Measures

The TOE satisfies the identified assurance requirements. This section identifies the Assurance Measures applied by Cisco to satisfy the assurance requirements. The table below lists the details.

Table 14. Assurance Measures

Assurance Component	Rationale
ADV_ARC.1	The architecture description provides the justification how the security functional requirements are enforced, how the security features (functions) cannot be bypassed, and how the TOE protects itself from tampering by untrusted active entities. The architecture description also identifies the system initialization components and the processing that occurs when the TOE is brought into a secure state (e.g. transition from a down state to the initial secure state (operational)).

Assurance Component	Rationale
ADV_FSP.2	The functional specification describes the external interfaces of the TOE; such as the means for a user to invoke a service and the corresponding response of those services. The description includes the interface(s) that enforces a security functional requirement, the interface(s) that supports the enforcement of a security functional requirement, and the interface(s) that does not enforce any security functional requirements. The interfaces are described in terms of their purpose (general goal of the interface), method of use (how the interface is to be used), parameters (explicit inputs to and outputs from an interface that control the behavior of that interface), parameter descriptions (tells what the parameter is in some meaningful way), and error messages (identifies the condition that generated it, what the message is, and the meaning of any error codes).The development evidence also contains a tracing of the interfaces to the SFRs described in this ST.
ADV_TDS.1	The TOE design describes the TOE security functional (TSF) boundary and how the TSF implements the security functional requirements. The design description includes the decomposition of the TOE into subsystems and/or modules, providing the purpose of the subsystem/module, the behavior of the subsystem/module and the actions the subsystem/module performs. The description also identifies the subsystem/module as SFR (security function requirement) enforcing, SFR supporting, or SFR non-interfering; thus identifying the interfaces as described in the functional specification. In addition, the TOE design describes the interactions among or between the subsystems/modules; thus providing a description of what the TOE is doing and how.
AGD_OPE.1	The Administrative Guide provides the descriptions of the processes and procedures of how the administrative users of the TOE can securely administer the TOE using the interfaces that provide the features and functions detailed in the guidance..
AGD_PRE.1	The Installation Guide describes the installation, generation, and startup procedures so that the users of the TOE can put the components of the TOE in the evaluated configuration.
ALC_CMC.2 ALC_CMS.2	The Configuration Management (CM) document(s) describes how the consumer (end-user) of the TOE can identify the evaluated TOE (Target of Evaluation). The CM document(s), identifies the configuration items, how those configuration items are uniquely identified, and the adequacy of the procedures that are used to control and track changes that are made to the TOE. This includes details on what changes are tracked, how potential changes are incorporated, and the degree to which automation is used to reduce the scope for error.

Assurance Component	Rationale
ALC_DEL.1	The Delivery document describes the delivery procedures for the TOE to include the procedure on how to download certain components of the TOE from the Cisco website and how certain components of the TOE are physically delivered to the user. The delivery procedure detail how the end-user may determine if they have the TOE and if the integrity of the TOE has been maintained. Further, the delivery documentation describes how to acquire the proper license keys to use the TOE components.
ATE_COV.1	The Test document(s) consist of a test plan describes the test configuration, the approach to testing, and how the subsystems/modules and TSFI (TOE security function interfaces) has been tested against its functional specification and design as described in the TOE design and the security architecture description. The test document(s) also include the test cases/procedures that show the test steps and expected results, specify the actions and parameters that were applied to the interfaces, as well as how the expected results should be verified and what they are. Actual results are also included in the set of Test documents.
ATE_FUN.1	
ATE_IND.2	Cisco will provide the TOE for testing.
AVA_VAN.2	Cisco will provide the TOE for testing.

6 TOE Summary Specification

This chapter identifies and describes how the Security Functional Requirements identified above are met by the TOE.

Table 15. TSS Rationale

<table>
<tr><th>TOE SFRs</th><th>How the SFR is Met</th></tr>
<tr><td>FAU_GEN.1</td><td>Shutdown and start-up of the audit functions are logged by events for reloading the UCS, and the events when the UCS comes back up. Audit is enabled whenever the TOE is on. The TOE also records an audit record whenever the TOE (and audit functionality) is Shutdown.

UCS generates events in the following format, with fields for date and time, severity, source and descriptionof the event as in this example:

2019 May 4 06:42:07 UTC Notice C220-WZP21690J4W (4.0(4B)):FCGI:1329 Login success (user: FredSmith, ip 10.56.234.170, service: webgui)

The auditable events include:

<table>
<tr><th>Auditable Events</th><th>Rationale</th></tr>
<tr><td>Successful modifications to user role assignments</td><td>Successful modifications to users/roles are logged in the local audit log. Failed attempts to make such modifications are not logged.</td></tr>
<tr><td>Successful and failed use of the user authentication mechanism on CIMC CLI and GUI</td><td>All login attempts to the CIMC CLI and GUI are logged. Successful attempts are logged to the local audit log, and optionally to a remote syslog server. Failed authentication attempts are not logged to the local audit log, but are sent to a remote syslog server.</td></tr>
<tr><td>Successful role-based access control requests submitted via the CIMC CLI, and GUI.</td><td>Successful changes to configuration data is logged to the local admin log.</td></tr>
<tr><td>Successful and failed attempts to change to the time.</td><td>Successful and failed attempts to change the system time and any time-related parameters including time zone or NTP server configuration are logged in the local audit log, and optionally to a remote syslog server. Manual setting of the clock can only be performed via the CLI.</td></tr>
</table>
</td></tr>
</table>

TOE SFRs	How the SFR is Met
	Successful and failed attempts to use the trusted path functions. / Successful and failed use of SSHv2 is logged only to a remote syslog server.
FAU_SAR.1	The UCS CIMC allows all administrative accounts to review the local audit store. These audit records are available to the authorized (authenticated) administrator through the administrative GUI and CLI provided by the UCS CIMC. The administrator can view TOE audit records through the provided GUI and CLI.
FAU_SAR.3	The UCS stores the events in order by date. Events are added to the top of the buffer display as they are generated, and UCS displays these new events at the top. The UCS allows for sorting and filtering of the events based on one of the following: Audit record ID; the affected object; or the user associated with the audit event..
FAU_STG.1	Audit records can be viewed by the authorized administrator via the UCS CIMC. Audit records are stored on the UCS in an internal file. The TOE does not provide any interfaces that would allow unmediated access to the audit records. This file can only be deleted by the authorized administrator through the UCS CIMC. The file cannot be altered.
FAU_STG.4	When local audit stores become full the oldest audit records will be deleted when new records are written, preserving a continuous audit trail. The TOE supports transmission of audit records to a remote audit server to provide more long-term storage of audit trails.
FDP_ACC.2 and FDP_ACF.1	The TOE implements an extensive Role Based Access Control system for administrative access to the TOE. The TOE implements three predefined administrative roles for administrative users. Each predefined role is associated with privileges that grant access permissions to the different configuration objects of the TOE. During user creation each administrator is assigned a User ID, and role assignments.
FIA_ATD.1	The UCS supports definition of administrators by individual user IDs, and these IDs are associated with a specific role. For each administrator, the TOE maintains the following attributes: • Login ID, • Password, • Account Expiration, • Role, and Roles are mapped to a collection of privileges that grant access to specific system resources and permission to perform specific tasks.

FIA_SOS.1	To prevent users from choosing insecure passwords, each password 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);**

TOE SFRs	How the SFR is Met
	○ **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 (for administrative accounts only, not SNMPv3 passwords), but remote authentication servers may have pre-configured passwords which do not meet the quality metrics.
FIA_UID.2 and FIA_UAU.2	By default, CIMC uses the local database for identification and authentication. No access is allowed without encountering an authentication prompt. Only after authentication is an administrator able to perform any actions. Remote authentication servers may be used in support of administrator access to the CLI and GUI.
FIA_UAU.5	The UCS CIMC may be configured for local or remote authentication. In the case of local authentication, account passwords are verified against hashes stored the /etc/shadow system file. In the case of remote authentication, user credentials are passed to a remote LDAP server for verification. In the remote authentication case, only password authentication is used for SSH. The HTTPS GUI authenticates against the local authentication database or remote authentication server, per system configuration. The SSH CLI authenticates users using SSH password authentication, verified against the local authentication database or remote authentication server.
FMT_MOF.1	All administrative accounts are assigned one role, and every role must at least possess the "read-only" privilege, so all accounts are able to read the audit logs. Abilities to disable, enable, and modify configuration settings is determined by the roles (and the privileges therein) assigned to each account, as defined by FMT_SMR.1.
FMT_MSA.1	The UCS access policies are configured to protect the UCS itself and to restrict the ability to enter privileged configuration mode to users with the correct role and privilege. Newly created users are not associated with any role and do not have any privilege but read-only unless roles are explicitly assigned an authorized administrator. The TOE provides the following access to TOE administrative functionality: A. Access to other administrative functionality of the TOE is provided to administrative users in a manner consistent with the access policy defined in FDP_ACF.1.
FMT_MSA.3	Restrictive default values are provided for role based access control. No administrative access is granted unless the role associated with the administrative user attempting to access the TOE is allowed access.
FMT_MTD.1	The UCS is configured to restrict the ability to enter privileged configuration operations to those users with the correct role assigned. The TOE only allows users with the *admin* privilege access to another user's security attributes (ID, Password, Account Expiration Date, Role). The TOE only allows users with the *admin* privilege the ability to set the TOE timezone.
FMT_SAE.1	The TOE provides administrative users with the admin privilege to set a time period after which administrative accounts are deactivated.
FMT_SMF.1	The UCS is configured to restrict the ability to enter privileged configuration operations to those users holding the correct privilege from their assigned role(s). The

<table>
<tr><th>TOE SFRs</th><th>How the SFR is Met</th></tr>
<tr><td></td><td>TOE provides the ability manage the operation of the TOE, audit trail, administrative access, administrative users and timestamps. Administrators can configure:
Auditing:
Enable or disable local storage of syslog messages, and set the syslog level to store locally, and set the size of the local audit storage.
Enable sending audit logs to up to three syslog servers, specifying the syslog severity level and syslog facility of audit messages to be sent to each server.
Individually enable/disable three ‘sources’ (categories) of syslog messages to be generated including Faults (system faults, including hardware connections/disconnections), Events (other system-level events), and Audits (all other messages).
Administrative users and access: Add/remove/modify custom roles, add/remote/modify user (admin) accounts, enable/disable/configure AAA protocols including LDAPS.
Timestamps: Manually set the local system timezone or add/remove one or more NTP servers.</td></tr>
<tr><td>FMT_SMR.1</td><td>Table 4 lists the privileges associated with management capabilities and default roles supported by the TOE. All accounts assigned to roles with any privilege mapped to an SFR (see table below) is considered an authorized administrator (relevant to FMT_SMR.1).<table><tr><th>Privilege</th><th>Relevance to Evaluated Security Functions</th></tr><tr><td>admin</td><td>FMT_MSA.1.1
FMT_MSA.3.2
FMT_MTD.1.1
FMT_SAE.1.1</td></tr><tr><td>read-only</td><td>None</td></tr><tr><td>User</td><td>None</td></tr></table></td></tr>
<tr><td>FPT_STM.1</td><td>The UCS provides a source of date and time information for the system, used in audit timestamps and in validating service requests. The clock function is reliant on the system clock provided by the underlying hardware. The timezone for the clock can be set in CIMC by the administrator.</td></tr>
<tr><td>FTP_TRP.1</td><td>The UCS TOE protects remote command line access to management functions using the SSH protocol for authentication, integrity protection and confidentiality

The UCS TOE protects remote web-based access to management functions using the TLS (TLS1.2) from the CIMC client software (HTML), or customized queries, all of which access the underlying XML API via the web server running on the Fabric Interconnect.</td></tr>
</table>

6.1 TOE Bypass and interference/logical tampering Protection Measures

The UCS TOE consists of a hardware and software solution. The UCS hardware platform protects all operations in the TOE from interference and tampering by untrusted subjects. All security policy enforcement functions must be invoked and succeed prior to functions proceeding.

The TOE has been designed so that all locally maintained TSF data can only be manipulated via the secured management interface, a CLI and GUI (CIMC) interface. The CLI interface achieves a trusted path via SSH password authentication and is recommended for authorized administrator access from outside the network boundary protecting the TOE servers. The GUI interface is a partially trusted path, but TLS client authentication is not performed, and it is recommended that the GUI interface be used from within the trusted network. There are no undocumented interfaces for managing the product.

All sub-components included in the TOE hardware rely on the main UCS chassis for power, memory management, and access control. In order to access any portion of the TOE, the Identification & Authentication mechanisms of the UCS must be invoked and succeed.

No processes outside of the UCS are allowed direct access to any TOE memory. The TOE only accepts traffic through legitimate TOE interfaces. None of these interfaces provide any access to internal TOE resources.

The UCS provides a secure domain for its operation. Each component has its own resources that other components within the same UCS platform are not able to affect.

The TOE includes the Cisco UCS CIMC software. This software includes a server and client component. The server component is resident within the TOE hardware and is protected by the mechanisms described above.

The client portion of the Cisco UCS CIMC is dependent on the IT environment. This software component runs on the operating systems identified in Table 2, above. The software is protected by the Operating System on which the software is installed.

This design, combined with the fact that only an administrative user with the appropriate role may access the TOE security functions, provides a distinct protected domain for the TOE that is logically protected from interference and is not bypassable.

7 RATIONALE

This section describes the rationale for the Security Objectives and Security Functional Requirements as defined within this Security Target. Additionally, this section describes the rationale for not satisfying all of the dependencies. The table below illustrates the mapping from Security Objectives to Threats and Policies

7.1 Rationale for TOE Security Objectives

Table 16. Summary of Mappings between Threats, Policies and the Security Objectives

	T.NOAUTH	T.SNIFF	T.ACCOUNTABILITY
O.IDAUTH	X		
O.ENCRYP		X	
O.AUDREC			X
O.ACCOUN			X
O.SECFUN	X		X
O.ADMIN		X	

Table 17. Rationale for Mapping of Threats, Policies and the Security Objectives for the TOE

Objective	Rationale for Coverage
O.IDAUTH	This security objective is necessary to counter the threat T.NOAUTH as it ensures that all users must be identified and authenticated.
O.ENCRYP	This security objective is necessary to counter the threat T.SNIFF by requiring that all administrative traffic be encrypted to prevent usable information from being extracted from a sniffed session.
O.AUDREC	This security objective is necessary to counter the threat

Objective	Rationale for Coverage
	T.ACCOUNTABILITY by requiring the TOE to record any administrative session allowing the identification of mistakes, by recording all auditable information in a human reviewable format, and by identifying attempted administrative actions even when the action is from an administrator with inappropriate authorization.
O.ACCOUN	This security objective is necessary to counter the threat T.ACCOUNTABILITY by ensuring that all administrators are accountable for their actions even when the action is from an administrator with inappropriate authorization.
O.SECFUN	This security objective is necessary to counter the threats T.ACCOUNTABILITY, and T. NOAUTH by ensuring only authorized administrators have access to the TOE security functions.
O.ADMIN	This security objective counters the threat T.SNIFF by providing a secure channel for administration.

7.2 Rationale for the Security Objectives for the Environment

The security requirements are derived according to the general model presented in Part 1 of the Common Criteria. Specifically, the tables below illustrate the mapping between the security requirements and the security objectives and the relationship between the threats, policies and IT security objectives. The functional and assurance requirements presented in this Security Target are mutually supportive and their combination meets the stated security objectives.

Table 18. Mappings of Assumptions and the Security Objectives for the OE

Assumption	OE.ADMIN	OE.BOUNDARY	OE.PHYSICAL	OE.POWER	OE.REDUNDANT_NET	OE.REMOTE_SERVERS
A.ADMIN	X					

A.BOUNDARY		X				
A.PHYSICAL			X			
A.POWER				X		
A.REDUNDANT_NET					X	
A.REMOTE_SERVERS						X

Table 19. Rationale for Mapping of Threats, Policies and Objectives for the OE

Assumptions	Rationale for Coverage of Environmental Objectives
OE.ADMIN	This security objective satisfies A.ADMIN by ensuring that competent and trusted administrators manage the TOE.
OE.BOUNDARY	This security objective satisfies A.BOUNDARY by ensuring that the UCS system is separated from public networks by an application aware firewall.
OE.PHYSICAL	This security objective satisfies A.PHYSICAL by ensuring that the UCS system is physically protected from unauthorized access.
OE.POWER	This security objective satisfies A.POWER by ensuring that the UCS system has sufficient power to operate.
OE.REDUNDANT_NET	This security objective satisfies A.REDUNDANT_NET by ensuring network availability.
OE.REMOTE_SERVERS	This security objective satisfies A. REMOTE_SERVERS by protecting communications between the TOE and optional remote servers.

7.3 Rationale for requirements/TOE Objectives

The security requirements are derived according to the general model presented in Part 1 of the Common Criteria. Specifically, the tables below illustrate the mapping between the security requirements and the security objectives and the relationship between the threats, and IT security objectives.

Table 20. Security Objective to Security Requirements Mappings

SFR	O.IDAUTH	O.ENCRYP	O.AUDREC	O.ACCOUN	O.SECFUN	O.ADMIN
FAU_GEN.1			X	X		

SFR	O.IDAUTH	O.ENCRYP	O.AUDREC	O.ACCOUN	O.SECFUN	O.ADMIN
FAU_SAR.1			X	X		
FAU_SAR.3			X	X		
FAU_STG.1	X				X	
FAU_STG.4	X				X	
FDP_ACC.2					X	
FDP_ACF.1					X	
FIA_ATD.1	X					
FIA_SOS.1	X					
FIA_UAU.2	X					
FIA_UAU.5	X					
FIA_UID.2	X					
FMT_MOF.1					X	
FMT_MSA.1					X	
FMT_MSA.3					X	
FMT_MTD.1					X	
FMT_SAE.1					X	
FMT_SMF.1					X	
FMT_SMR.1					X	
FPT_STM.1			X			
FTP_TRP.1		X				X

Table 21. Summary of Mappings between IT Security Objectives and SFRs

SFR	Rationale
FAU_GEN.1	This component outlines what data must be included in audit records and what events must be audited. This component traces back to and aids in meeting the following objectives: O.AUDREC, O.ACCOUN.

SFR	Rationale
FAU_SAR.1	This component ensures that the audit trail is understandable. This component traces back to and aids in meeting the following objectives: O.AUDREC, O.ACCOUN.
FAU_SAR.3	This component ensures that a variety of searches and sorts can be performed on the audit trail. This component traces back to and aids in meeting the following objectives: O.AUDREC, O.ACCOUN.
FAU_STG.1	This component is chosen to ensure that the audit trail is protected from tampering, the security functionality is limited to the authorized administrator and that start-up and recovery does not compromise the audit records. This component traces back to and aids in meeting the following objective: O.IDAUTH, O.SECFUN.
FAU_STG.4	This component is chosen to ensure that the audit trail is protected from loss by ensuring that the audit trail is maintained in a predictable way when the audit store becomes full. This component traces back to and aids in meeting the following objective: O.IDAUTH, O.SECFUN.
FDP_ACC.2	This component ensures that the TOE provides administrative access to only TOE administrators with the appropriate authorization. This component traces back to and aids in meeting the following objective: O.SECFUN.
FDP_ACF.1	This component ensures that the TOE provides administrative access to only TOE administrators with the appropriate authorization. This component traces back to and aids in meeting the following objective: O.SECFUN.
FIA_ATD.1	This component exists to provide users with attributes to distinguish one user from another, for accountability purposes and to associate the role chosen in FMT_SMR.1 with a user. This component traces back to and aids in meeting the following objective: O.IDAUTH.
FIA_SOS.1	This component ensures user passwords meet defined quality metrics. This component traces back to and aids in meeting the following objective: O.IDAUTH.
FIA_UAU.2	This component ensures that before anything occurs on behalf of a user, the user's identity is authenticated to the TOE.

SFR	Rationale
	This component traces back to and aids in meeting the following objective: O.IDAUTH.
FIA_UAU.5	This component identifies the multiple authentication mechanisms permitted for users. This component traces back to and aids in meeting the following objective: O.IDAUTH.
FIA_UID.2	This component ensures that before anything occurs on behalf of a user, the user's identity is identified to the TOE. This component traces back to and aids in meeting the following objective: O.IDAUTH.
FMT_MOF.1	This component ensures that the TSF restrict abilities to determine the behavior of, disable, enable, modify the behavior of functions as defined in FMT_SMF.1to the administrative roles defined in FMT_SMR.1. This component traces back to and aids in meeting the following objectives: O.SECFUN.
FMT_MSA.1	This component ensures the TSF enforces the Role Based Administrative Access Control to restrict the ability to modify those security attributes that are listed in section FDP_ACF.1. This component traces back to and aids in meeting the following objectives: O.SECFUN.
FMT_MSA.3	This component ensures that there is a default deny policy for the Role Based Administrative Access Control security rules. This component traces back to and aids in meeting the following objectives: O.SECFUN
FMT_MTD.1	This component ensures that the TSF restrict abilities to set the time and date used to form timestamps to only the authorized administrator. This component traces back to and aids in meeting the following objective: O.SECFUN.
FMT_SAE.1	This component ensures user accounts can be given a time limit by administrators. This component traces back to and aids in meeting the following objective: O.SECFUN.
FMT_SMF.1	This component ensures that the TSF restrict the set of management functions to the authorized administrator. This component traces back to and aids in meeting the following objective: O.SECFUN.

SFR	Rationale
FMT_SMR.1	This component ensures that the TOE maintains authorized administrator roles to manage the TOE administrative security functionality. This component traces back to and aids in meeting the following objective: O.SECFUN.
FPT_STM.1	This component ensures that the date and time on the TOE is dependable. This is important for the audit trail. This component traces back to and aids in meeting the following objective: O.AUDREC.
FTP_TRP.1	This component ensures that administrators have a trusted path to access the TOE. This component traces back to and aids in meeting the following objectives: O.ADMIN, and O.ENCRYP.

8 References

The documentation listed below was used to prepare this ST

Table 22. References

Identifier	Description
[CC_PART1]	Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated September 2012, version 3.1, Revision 5, CCMB-2017-04-001
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated September 2012, version 3.1, Revision 5, CCMB-2017-04-002
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated September 2012, version 3.1, Revision 5, CCMB-2017-04-003
[CEM]	Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated September 2012, version 3.1, Revision 5, CCMB-2017-04-004

8.1 Acronyms and Terms

The following acronyms and terms are common and may be used in this Security Target.

Table 23. Acronyms and Terms

Acronym/Term	Definition
API	Application Programming Interface
BMC	Baseboard Management Controller (renamed to CIMC)
CIMC	Cisco Integrated Management Controller
CIM-XML	Common Information Model XML
CLI	Command Line Interface
EISL	Enhanced Inter-Switch Link (ISL), a multiple-VSAN trunk connection between switches.
FCoE	Fibre Channel over Ethernet
FC-SP	Fibre Channel – Security Protocol
GUI	Graphical User Interface
HBA	Host Bus Adapter, a physical or virtual (vHBA) adapter providing connectivity between a server and a storage device.
ISL	Inter-Switch Link, a VSAN connection between switches.

Acronym/Term	Definition
LAN	Local Area Network
mLOM	Modular LAN on Motherboard
NIC	Network Interface Card, a physical or virtual (vNIC) adapter provide connectivity between a device/host and a network.
SAN	Storage Area Network
SNMP	Simple Network Management Protocol
SSH	Secure Shell
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
UCS	Unified Computing System
UCSM	UCS Manager
UUID	Universally Unique IDentifier
VIC	Virtual Interface Card, one of several Cisco interface cards for UCS servers, e.g. models 1225, 1225T, 1240, 1280, 1340 etc.
VLAN	Virtual Local Area Network
VM	Virtual Machine, a virtualized guest operating system installed to a hypervisor.
VMM	Virtual Machine Manager, a hypervisor.
VSAN	Virtual Storage Area Network

9 Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.

10 Contacting Cisco

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