Cisco Unified Computing System (UCS) Security Target

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Cisco Unified Computing System solution. 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.

Version 1.0
6 April, 2017

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

Table of Contents

List of Tables

List of Figures

1. Security Target Introduction

The Security Target contains the following sections:

- Security Target Introduction
- TOE Description
- Conformance Claims
- Security Problem Definition
- Security Objectives
- Security Requirements
- Assurance Measures
- TOE Summary Specification
- Rationale

The structure and content of this ST comply with the requirements specified in the Common Criteria (CC), Part 1, Annex A, and Part 3, Chapter 4.

1.1.   ST and TOE Identification

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

Table 1: ST and TOE Identification

ST Title	Cisco Unified Computing System Security Target
ST Revision	1.0
ST Publication Date	6 April, 2017
Guidance Document	Cisco Unified Computing System (UCS), version 3.1(2b) Common Criteria Operational User Guidance and Preparative Procedures, version 1.0
Vendor and ST Author	Cisco Systems, Inc.
TOE Reference	Cisco UCS 5100 Series Blade Server Chassis, B-Series Blade Servers, C-Series Rack-Mount Servers, 2200/2300 Series Fabric Extenders, and 6200/6300 Series Fabric Interconnects with UCSM 3.1(2b)
TOE Hardware Models	Cisco UCS 5108 Blade Server Chassis, Cisco UCS Blade Servers (B200 M3, B200 M4, B260 M4, B420 M3, B420 M4, and B460 M4), Cisco UCS Rack Servers (C220 M3, C220 M4, C240 M3, C240 M4, and C460 M4), Virtual Interface Cards (see listing in section 2.6), Cisco UCS Fabric Interconnects (6248UP, 6296UP, 6332, 6332-16UP, and 6324), and Cisco UCS Fabric Extenders (2232PP, 2204XP, 2208XP, and 2304)
TOE Software Version	Cisco Unified Computing System (UCS) Manager 3.1(2b)
ST Evaluation Status	In Evaluation

1.2. TOE Overview

The TOE is a unified computing solution, which provides access layer networking and servers.

1.3. TOE Product Type

The TOE, often referred to in this document as the UCS system, consists of hardware and software components that support Cisco's unified fabric, which run multiple types of data-center traffic over a single converged network adapter. The UCS features a role based access control policy to control the separation of administrative duties and provide a security log of all changes made.

A single Cisco Unified Computing System scales to up to forty chassis and three hundred twenty blade servers or rack-mount servers, all of which are administered through a single management entity called the Cisco UCS Manager. The Cisco UCS consists of the following primary hardware elements – Cisco UCS 5108 Blade Server Chassis, Cisco UCS Blade Servers (B200 M3, B200 M4, B260 M4, B420 M3, B420 M4, and B460 M4), Cisco UCS Rack Servers (C220 M3, C220 M4, C240 M3, C240 M4, and C460 M4), Virtual Interface Cards (see listing in section 2.6), Cisco UCS Fabric Interconnects (6248UP, 6296UP, 6332, 6332-16UP, and 6324), and Cisco UCS Fabric Extenders (2232PP, 2204XP, 2208XP, and 2304). The Fabric Interconnects and Fabric Extenders are based on the same switching technology as the Cisco Nexus™ 5000 Series. Fabric Interconnects also provide additional centralized management capabilities that form the basis of the Cisco UCS Manager.

Cisco UCS implements Cisco unified fabric within racks and groups of racks, supporting Ethernet and Fibre Channel protocols over 10 Gigabit Cisco® Data Center Ethernet and Fibre Channel over Ethernet (FCoE) links. The result of this network unification is a reduction by up to two-thirds of the switches, cables, adapters, and management points. All devices in a system remain under a single management domain, which remains highly available through the use of redundant components.

1.4. Supported non-TOE Hardware/ Software/ Firmware

The TOE supports (in some cases optionally) the following hardware, software, and firmware in its environment:

Table 2: Supported non-TOE Hardware/ Software/ Firmware

IT Environment Component	Required	Usage/ Purpose Description for TOE performance

UCS Management Workstation
 	
(The host operating system upon which the UCSM client application runs.)
	Yes	The GUI client applet of the Cisco UCS Manager (UCSM) is a Java-based application that allows remote administration of UCSM over TLS. The applet, which is part of the TOE, requires Sun JRE 1.6 or later, which is part of the IT environment.
		• The UCS Manager uses web start[1] to present the GUI and supports the following web browsers:
		    – Microsoft Internet Explorer 9.0 or higher
		    – Mozilla Firefox 7.0 or higher
		    – Google Chrome 14.0 or higher
		Note that that UCS Manager runs on the Fabric Interconnect component of the UCS system and the management workstation is used to connect to the UCS and run the UCSM client applet (the Java-based GUI).

SSHv2 Client	No	UCSM can be managed remotely via SSHv2.
SNMPv3 Client	No	UCSM can be managed remotely via SNMPv3.
Remote Authentication Server	No	A RADIUS, TACACS+, or 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.
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] 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.

2. 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:

- Cisco UCS Manager (UCSM) components
    - One or more Cisco UCS Fabric Interconnects [6248UP, 6296UP, 6332, or 6332-16UP (for use with C-Series or B-Series Servers), or 6324 (for use in the 5108 Blade Server Chassis)]
        - Cisco UCS Manager release 3.1(2b)
- Server and Fabric Extenders (with software loaded from the UCSM bundle)
    - Blade server configurations:
        - One or more Cisco UCS 5108 Chassis with:
            - Zero, one or more Cisco UCS Fabric Extenders (2204XP, 2208XP, or 2304)
            - One or more Cisco UCS Blade Servers (B200 M3, B200 M4, B260 M4, B420 M3, B420 M4, or B460 M4)
    - Rack-Mount Server configurations:
        - Zero, one or more Cisco Nexus 2232PP Fabric Extenders

Cisco Unified Computing System Security Target

- One or more Cisco UCS Rack Servers (C220 M3, C220 M4, C240 M3, C240 M4, or C460 M4)

Deployment note: One instance of the Cisco UCS Manager can manage: a cluster of two Fabric Interconnects; multiple Cisco UCS 5100 Series Chassis; 80 Fabric Extenders, and hundreds of Cisco UCS B-Series Blade Servers and/or C-Series Rack-Mount Servers. [Capacity details are provided for conceptual purposes only as capacity testing is not covered within the scope of the Common Criteria evaluation.]

2.1. Cisco UCS 5108 Chassis

The Cisco UCS 5108 Chassis physically houses blade servers and up to two fabric extenders. The enclosure is 6RU high supporting up to 56 servers per rack. The UCS 5108 supports up to eight half slot or four full slot blade servers with four power supplies and eight cooling fans. Both power supplies and fans are redundant and hot swappable. Featuring 90%+ efficient power supplies, front to rear cooling, and airflow optimized mid-plane, the Cisco UCS is optimized for energy efficiency and reliability.

Even though the Blade Server Enclosure and Cisco UCS System can house multiple blades, each blade acts as an individual physical server. Cisco UCS System provides a centralized and simplified management paradigm for all the blades.

The Cisco UCS 5108 can be managed by rack-mountable (1RU) Fabric Interconnects (6248UP, 6296UP, 6332, or 6332-16UP), or by the "UCS Mini" 6324 Fabric Interconnect (installed within the 5108 Chassis). Network connectivity for B-Series Blade Servers is provided via one or more Fabric Extenders installed within the 5108 chassis (2204XP, 2208XP, or 2304).

2.2. Cisco UCS Fabric Interconnects

The Cisco UCS 6248UP, and 6296UP Fabric Interconnects are high-throughput switches that consolidate I/O at the system level to provide line-rate, low-latency, lossless 10 Gigabit Ethernet, Cisco Data Center Ethernet, and Fiber Channel over Ethernet (FCoE). These Fabric Switches supply a unified network fabric that connects every server resource in the system once 10G Ethernet/FCoE downlinks and 10G Ethernet and 1/2/4Gb FC uplink modules are configured. The Cisco UCS 6200 Series interconnects support out-of-band management through a dedicated 10/100/1000-Mbps Ethernet management port as well as in-band management. Out of band management, switch redundancy, and console-based diagnostics are enabled through dedicated management, clustering, and RS-232 ports. A single UCS Series Fabric Switch unites up to 320 servers within a single system domain for maximum scalability.

The Cisco UCS 6200 Series Fabric Switch has two flavors – a 1RU switch (6248UP 48-Port Fabric Interconnect) and a 2RU switch (6296UP 96-port Fabric Interconnect).

The 1RU Fabric switch supports 48 fixed 10G FCoE ports, up to 960 Gbps throughput, 1 expansion module, 2 fan modules, and redundant power supplies. The 2RU Fabric switch supports 96 fixed 10G FCoE ports up to 1920 Gbps throughput, 3 expansion modules, 4 fan modules, and redundant power supplies.

The Cisco UCS 6300 Series Fabric Interconnects include two appliance-based (stand-alone) models (6332, and 6332-16UP), and one "UCS Mini" model (6324) installed within a 5108 Blade Chassis. The UCS Mini 6324 supports up to 20 servers, while the 6332 and 6332-16UP each support up to 160 servers. The 6332 supports 32 40-Gbps ports in one 1 rack unit (RU), while the 6332-16UP has 24 40-Gigabit Ethernet and Fibre Channel over Ethernet (FCoE) ports plus 16 ports that provide 1-10 Gbps and FCoE or can be configured as 4-,8-, and 16-Gbps Fibre Channel unified ports.

The external authentication server can act as a repository for authentication credentials. The Cisco UCS Fabric switch implements SSHv2, and TLS1.0/1.1/1.2 for secure network management, and SNMPv3 for monitoring (read only). The expansion modules supported on the Cisco UCS 6200 Series Fabric Switch can be used to increase the number of 10-Gbit Ethernet, FCoE and FC ports. The unified port module provides up to 16 ports that can be configured for 10 Gigabit Ethernet, FCoE and/or 1/2/4/8-Gbps native Fibre Channel using the SFP.

2.3. Cisco UCS Fabric Extenders

The Cisco UCS 2204XP and 2208XP Fabric Extenders extends the I/O fabric into the blade server enclosure (the 5108 Blade Server Chassis) providing a direct 10Gbs connection between blade servers and fabric switch simplifying diagnostics, cabling, and management. The fabric extender multiplexes and forwards all traffic using a cut-through architecture over one to four 10Gbps unified fabric.

The 2304 Fabric Extender is also installed into the 5108 Blade Server Chassis. It includes four 40 Gigabit Ethernet, FCoE-capable, Quad Small Form-Factor Pluggable (QSFP+) ports that connect the blade chassis to the fabric interconnect. Each Cisco UCS 2304 has four 40 Gigabit Ethernet ports connected through the midplane to each half-width slot in the chassis. Typically configured in pairs for redundancy, two fabric extenders provide up to 320 Gbps of I/O to the chassis.

The Cisco UCS 2232PP Fabric Extender is a stand-alone appliance (not installed into the blade server chassis) and provides 32 10 Gb Ethernet and Fibre Channel over Ethernet (FCoE) Small Form-Factor Pluggable Plus (SFP+) server ports and eight 10 Gb Ethernet and FCoE ports in a 1RU form factor. The 2232PP extends the I/O fabric between Fabric Interconnect hardware and Rack Servers (C-Series servers).

2.4. Cisco UCS Blade Servers

Cisco UCS Blade Servers (B200 M3, B200 M4, B260 M4, B420 M3, B420 M4, and B460 M4) are designed for compatibility, performance, energy efficiency, large memory footprints, manageability, and unified I/O connectivity. Based on Intel® Xeon® 5500 series processors, B-Series Blade Servers adapt to application demands, scale energy use, and offer a platform for virtualization. Each Cisco UCS B-Series Blade Server utilizes converged network adapters for consolidated access to the unified fabric with various levels of transparency to the operating system. This design reduces the number of adapters, cables, and access-layer switches for LAN and SAN connectivity at the rack level.

The Blade Servers support network adapters from a number of manufacturers that do not provide any of the security functionality described in the ST. For a full compatibility matrix, refer to the Hardware and Software Interoperability Matrix for B-Series Servers referenced from the Cisco UCS B-Series Servers Documentation Roadmap available at Cisco.com. Any software installed to the Blade servers, including hypervisors and guest operating systems, is outside the TOE boundary.

2.5. Cisco UCS Rack Mount C-Series Servers

UCS Rack Mount Servers, also known as C-Series Servers (C220 M3, C220 M4, C240 M3, C240 M4, and C460 M4) 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 C-Series Servers Documentation Roadmap available at Cisco.com. Any software installed to the Blade servers, including hypervisors and guest operating systems, is outside the TOE boundary.

2.6. 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 B-Series Servers:

- Cisco UCS VIC 1240
- Cisco UCS VIC 1280
- Cisco UCS VIC 1340

- Cisco UCS VIC 1380
- Cisco UCS 82598KR-10 Gigabit Ethernet Network Adapter
- Cisco UCS M71KR-Q QLogic Converged Network Adapter
- Cisco UCS M71KR-E Emulex Converged Network Adapter
- Cisco UCS M81KR Virtual Interface Card
- Cisco UCS M72KR-Q QLogic Converged Network Adapter
- Cisco UCS M72KR-E Emulex Converged Network Adapter
- Cisco UCS M61KR-I Intel Converged Network Adapter
- Cisco UCS NIC M51KR-B Broadcom BCM57711 Network Adapter

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

- Cisco UCS VIC 1225
- Cisco UCS VIC 1225T
- Cisco UCS VIC 1285
- Cisco UCS P81E Virtual Interface Card
- Emulex OneConnect Universal Converged Network Adapter
- QLogic QLE8152 Dual Port 10 Gb Ethernet to PCIe Converged Network Adapter
- Cisco UCS X520 Intel Converged Network Adapter
- Broadcom NetXtreme II 5709 Quad Port Ethernet PCIe Adapter Card with TOE and iSCSI HBA
- Broadcom NetXtreme II 57711 Dual Port 10 Gb Ethernet PCIe Adapter Card with TOE and iSCSI HBA
- Emulex LightPulse LPe11002 4 Gbps Fibre Channel PCI Express Dual Channel HBA
- QLogic SANblade QLE2462, Dual Port 4 Gbps Fibre Channel to PCI Express HBA

2.7. Cisco UCS Manager (UCSM)

The Cisco UCS Manager software integrates the components of a Cisco Unified Computing System into a single, seamless entity. It can manage up to three hundred and twenty blade servers as a single logical domain via the UCSM 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. Any user's role may be limited to a subset of the system's resources using organizations and locales, so that a Cisco Unified Computing System can be partitioned and shared between organizations using a multi-tenant model. It allows secure management of the TOE using TLS1.0/1.1/1.2, and SSHv2, and monitoring using SNMPv3 (read only).

The UCS Manager software is divided into two components: server and client side. The server side component is installed on the 6248UP or 6296UP Fabric Interconnect hardware. 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 (UCSM GUI) is a java application that provides the GUI for the administrator.

The UCS Manager software may be deployed in a standalone configuration (on a single Fabric Interconnect), or in a clustered configuration with one pair of Fabric Interconnects. When clustered, management configuration data and event log storage are centralized in the primary Fabric Interconnect and accessed by the subordinate member of the cluster. In a cluster configuration the two Fabric Interconnect appliances use a pair of directly-connected Ethernet ports allowing these cross-connects to operate within the protected network boundary. Clustered FI are to be deployed in close proximity to each other such that the network cables between them are protected by a single physically secure environment that protects both FI.

2.8. 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 software / firmware for the TOE is bundled in a single image and is distributed to components within the TOE by Cisco UCS Manager. The individual component firmware versions are identified with the version listed in the Software / Firmware section of the table below.

The TOE is comprised hardware identified in the following table.

Table 3: Physical Scope of the TOE

	Fabric Interconnects	Fabric Extenders	C-Series Rack Servers	Cisco UCS 5108 Chassis	Fabric Interconnects for B-Series	Fabric Extenders for B-Series	B-Series Blade Servers
Image							
TOE Component Model Numbers	UCS 6248UP	Nexus 2232PP	UCS C220 M3	UCS 5108	UCS 6324	UCS 2204XP	UCS B200 M3
	UCS 6296UP		UCS C220 M4			UCS 2208XP	UCS B200 M4
	UCS 6332		UCS C240 M3			UCS 2304	UCS B260 M4
	UCS 6332-16UP		UCS C240 M4				UCS B420 M3
			UCS C460 M4				UCS B420 M4
							UCS B460 M4
			C-Series NICs: As listed in section *2.6*.				**B-Series NICs:** As listed in section *2.6*.
Software / Firmware	Unified Computing System (UCS) Complete Software Bundle version 3.1(2b) which includes Cisco UCS Manager 3.1(2b), and the UCSM Client GUI Java-based applet.						
Guidance Documentation	"Cisco Unified Computing System (UCS), version 3.1(2b) Common Criteria Operational User Guidance and Preparative Procedures" (*Including all supplemental guidance documents referenced therein.*)						

2.9.   Logical Scope of the TOE

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

1. Audit

2. Identification & Authentication

3. Management

4. Network Separation

5. Role Based Access Control

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

2.9.1. 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 Fabric Interconnect as part of UCSM. The database is internal only and does not provide any externally visible interfaces for communication. When UCS is deployed in a clustered configuration all instances of the UCS Manager record audit information with the primary UCS Manager instance. In standalone mode, all audit data is stored locally. Regardless of standalone or clustered configuration, 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 Manager 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.

2.9.2. Identification & Authentication

Cisco UCS supports two methods of authenticating administrator logins on the Cisco UCS Manager: a local user database of passwords (and optionally SSH keys) or a remote authentication server accessed either via LDAP, RADIUS, or TACACS+. 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. When UCS is deployed in a clustered configuration all instances of the UCS Manager share the local user database.

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 local 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.

2.9.3. Management

UCS can be managed using the graphical user interface (over TLS1.0/1.1/1.2), 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 (keys and 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 Manager to perform management tasks for all physical and virtual devices within a Cisco UCS instance.

2.9.3.1. Cisco UCS Hardware Management

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

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

2.9.3.2. Cisco UCS Resource Management

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

- Servers
- World Wide Name (WWN) addresses, used in Storage Area Networks
- MAC addresses
- Universally Unique Identifiers (UUIDs), assigned to each server
- Bandwidth (not security-relevant to the TSF)

2.9.3.3. Server Administration in a Cisco UCS Instance

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

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

2.9.3.4. Network Administration in a Cisco UCS Instance

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

- Configure uplink ports, port channels, and LAN PIN groups
- Create VLANs
- Configure the quality of service classes and definitions
- Create the pools and policies related to network configuration, such as MAC address pools and Ethernet adapter profiles

2.9.3.5. Storage Administration in a Cisco UCS Instance

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

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

2.9.3.6. Tasks that Cannot be Performed in Cisco UCS Manager

Cisco UCS Manager 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 Manager to manage systems or devices that are outside the Cisco UCS instance where Cisco UCS Manager is located. For example, one cannot manage heterogeneous environments, such as non-Cisco UCS x86 systems, SPARC systems, or PowerPC systems.

Provisioning and management of operating systems and applications is not permitted. Cisco UCS Manager provisions servers 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 servers.

2.9.3.7. UCS Secure Access

The UCS Manager provides access for an administrator using SSHv2, TLS1.0/1.1/1.2, or SNMPv3.

SSHv2 is used to access the command line interface for the UCS Manager. SSHv2 authentication uses the UCS Manager username and password. SSHv2 can also be configured on a per-user basis for public key authentication. The command line interface is also accessible over the local serial port.

TLS1.0/1.1/1.2 is used to access the UCS Manager interface. The UCS Manager interface serves as a launch point for the Java application which also utilizes TLS1.0/1.1/1.2 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.

2.9.3.8. 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 UCS Manager. 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.

2.9.4. Network Separation

2.9.4.1. VLAN Separation

VLANs enable efficient traffic separation, provide better bandwidth utilization, and alleviate scaling issues by logically segmenting the physical local-area network (LAN) infrastructure into different subnets so that VLAN packets are presented to interfaces within the same VLAN.

The most important requirement of VLANs is the ability to identify the origination point for packets with a VLAN tag to ensure packets can only travel to interfaces for which they are authorized.

The Cisco UCS 6200 Series Fabric Interconnect hardware requires VLANs to function. When the administrator configures network adapters on a per server basis, VLANs are specified for each adapter.

2.9.4.2. VSAN Separation

Virtual SAN (VSAN) technology partitions a single physical Storage Area Network (SAN) into multiple VSANs. VSAN capabilities allow the Cisco UCS 6200 Series Fabric Interconnect Hardware to logically divide a large physical fabric into separate isolated environments to improve SAN scalability, availability, manageability, and network security.

Each VSAN is a logically and functionally separate SAN with its own set of Fibre Channel fabric services. This partitioning of fabric services greatly reduces network instability by containing fabric reconfigurations and error conditions within an individual VSAN. The strict traffic segregation provided by VSANs helps ensure that

the control and data traffic of a given VSAN is confined within its own domain, increasing SAN security.

Traffic is contained within VSAN boundaries and devices reside only in one VSAN thus ensuring absolute separation between user groups. This ensures the confidentiality of data traversing the VSAN from users and devices belonging to other VSANs. It should be noted that devices, such as file servers and tape storage devices are not part of the TOE but part of the TOE environment and may be configured to participate in a VSAN. Each network interface of an HBA connected to the TOE may only participate in a single VSAN.

2.9.5. Role Based Access Control

Role-Based Access Control (RBAC) is a method of restricting or authorizing system access for users based on user roles and locales. A role defines the privileges of a user in the system and the locale defines the organizations (domains) 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 and locales.

A user is granted write access to desired system resources only if the assigned role grants the access privileges and the assigned locale allows access. For example, a user with the Server Administrator role in the Engineering organization could update server configurations in the Engineering organization, but would not be able to update server configurations in the Finance organization unless the locales assigned to the user include the Finance organization.

2.9.5.1. Privileges

Privileges give their holder access to specific system resources and permission to perform specific tasks. Privileges can be added to the default roles (except the 'Administrator' and 'Read-Only' roles), and new custom roles can be created with custom-defined sets of privileges.

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
aaa	System security and AAA	AAA Administrator
admin	System administration	Administrator
ext-lan-config	External LAN configuration	Network Administrator
ext-lan-policy	External LAN policy	Network Administrator
ext-lan-qos	External LAN QoS	Network Administrator
ext-lan-security	External LAN security	Network Administrator
ext-san-config	External SAN configuration	Storage Administrator
ext-san-policy	External SAN policy	Storage Administrator
ext-san-qos	External SAN QoS	Storage Administrator
ext-san-security	External SAN security	Storage Administrator
fault	Alarms and alarm policies	Operations
operations	Logs and Smart Call Home	Operations
org-management	Organization management	Operations
pod-config	Pod configuration	Network Administrator

pod-policy	Pod policy	Network Administrator
pod-qos	Pod QoS	Network Administrator
pod-security	Pod security	Network Administrator
power-mgmt	Read-and-write access to power management operations	Facility Manager
read-only	Read-only access. Read-only cannot be selected as a privilege; it is assigned to every user role.	Read-Only
server-equipment	Server hardware management	Server Equipment Administrator
server-maintenance	Server maintenance	Server Equipment Administrator
server-policy	Server policy	Server Equipment Administrator
server-security	Server security	Server Security Administrator
service-profile-compute	Service profile compute	Server Compute Administrator
service-profile-config	Service profile configuration	Server Profile Administrator
service-profile-config-policy	Service profile configuration policy	Server Profile Administrator
service-profile-ext-access	Service profile end point access	Server Profile Administrator
service-profile-network	Service profile network	Network Administrator
service-profile-network-policy	Service profile network policy	Network Administrator
service-profile-qos	Service profile QoS	Network Administrator
service-profile-qos-policy	Service profile QoS policy	Network Administrator
service-profile-security	Service profile security	Server Security Administrator
service-profile-security-policy	Service profile security policy	Server Security Administrator
service-profile-server	Service profile server management	Server Profile Administrator
service-profile-server-oper	Service profile consumer	Server Profile Administrator
service-profile-server-policy	Service profile pool policy	Server Profile Administrator
service-profile-storage	Service profile storage	Storage Administrator
service-profile-storage-policy	Service profile storage policy	Storage Administrator

2.9.5.2. User Roles

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

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

The system contains the following default user roles:

- AAA Administrator: Read-and-write access to users, roles, and AAA configuration. Read access to the rest of the system.

- Administrator: Complete read-and-write access to the entire system. The default admin account is assigned this role by default and this association cannot be changed.

- Facility Manager: Read-and-write access to power management operations.

- Network Administrator: Read-and-write access to fabric interconnect infrastructure and network security operations. Read access to the rest of the system.

- Operations: Read-and-write access to systems logs, including the syslog servers, and faults. Read access to the rest of the system.

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

- Server Compute Administrator: Read and write access to most aspects of service profiles. However, the user cannot create, modify or delete vNICs or vHBAs.

- Server Equipment Administrator: Read-and-write access to physical server related operations. Read access to the rest of the system.

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

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

- Storage Administrator: Read-and-write access to storage operations. Read access to the rest of the system.

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

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

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

2.9.5.3. User Locales

A user can be assigned one or more locales. Each locale defines one or more organizations (domains) the user is allowed access, and access is limited to the organizations specified in the locale. Access control based on locales is enforced on all roles, including the full access Administrator role. A locale without any organizations may be created, this grants unrestricted access to system resources in all organizations.

Users with AAA Administrator privileges (AAA Administrator role) or the Administrator role can assign organizations to the locale of other users. The assignment of organizations is restricted to only those in the locale of the user assigning the organizations. For example, if a locale contains only the Engineering organization then a user assigned that locale can only assign the Engineering organization to other users.

Administrators can hierarchically manage organizations. A user that is assigned at a top-level organization has automatic access to all organizations under it. For example, an Engineering organization can contain a Software Engineering organization and a Hardware Engineering organization. A locale containing only the Software Engineering organization has access to system resources only within that organization; however, a locale that contains the Engineering organization has access to the resources for both the Software Engineering and Hardware Engineering organizations.

2.9.6. 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 2 and all the software and firmware installed on the Fabric Interconnects and Fabric Extenders, and all the firmware on the servers. The TOE boundary does not include any hypervisors and guest operating systems installed to the servers.

Figure 2: Sample Deployment of a Subset of TOE Components

Cisco Unified Computing System

Cisco UCS 6200 Series Fabric Interconnects

Cisco UCS 6248UP   - or -   Cisco UCS 6296UP

Cisco UCS Manager (Embedded)

160 Gbps per Chassis   80 Gbps per Chassis   Data and Management   Data and Management

Cisco UCS 2208XP Fabric Extender

Cisco UCS 2204XP Fabric Extender

Cisco Nexus 2232PP 10GE Fabric Extender

Cisco UCS 5108 Blade Server Chassis

Data   Management

Cisco UCS B-Series Blade Servers

Cisco UCS C-Series Rack Servers

The following diagram shows an example deployment of the TOE components including a firewall to protect the TOE management interfaces from untrusted networks. In this topology, the remote servers, such as RADIUS, syslog, and NTP could be hosted on UCS servers, or third-party rack servers, or across the LAN Core.

Figure 3: Sample TOE Deployment Interconnected with Non-TOE Components

Cisco Unified Computing System Security Target
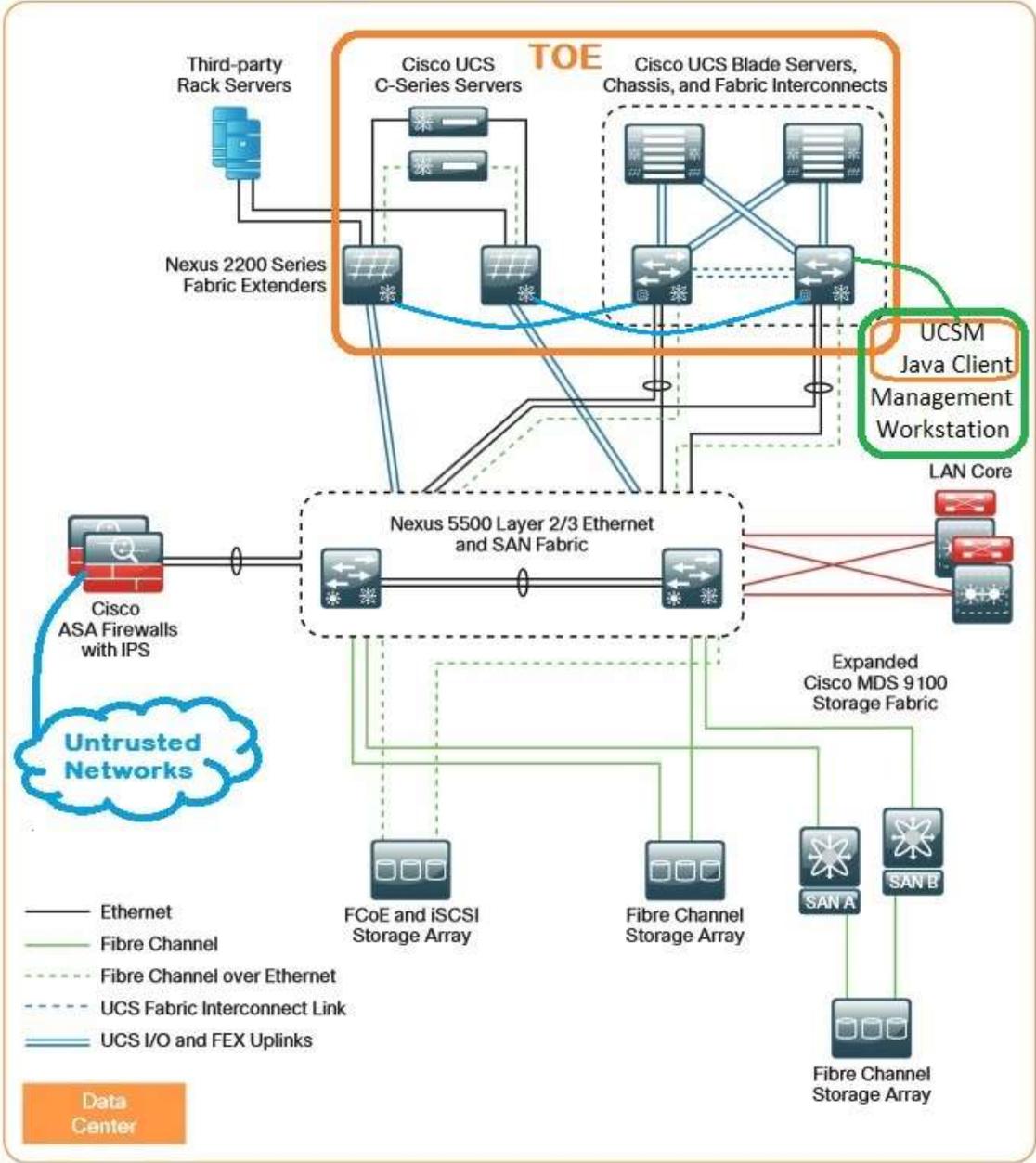
2.9.6.1. Excluded Functionality

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

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

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

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

CIM-XML is disabled by default, and must remain disabled in the evaluated configuration. 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 UCSM GUI and UCSM CLI.)

All other functionality is supported in the evaluated configuration.

2.10. Conformance Claims

2.10.1. 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 4, September 2012
    - o Part 2 Conformant
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1, Revision 4, September 2012
    - o Part 3 Conformant

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

2.10.2. Protection Profile Conformance

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.

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

3.1. Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's IT 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.VSAN	Each network interface of an HBA connected to the TOE may only participate in a single VSAN.
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 remote authentication servers, 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. The assumed level of expertise of the attacker for all the threats identified below is basic.

Table 6: Threats

Threat Name	Threat Definition
T.NORMAL_USE	A system user (VM user, OS administrator, or Hypervisor administrator) attacks the UCS infrastructure from an allowed channel (web application, Windows share access, application, or other installed utility) and compromises the TSF.
T.NOAUTH	A system user (VM user, OS administrator, or Hypervisor administrator) attempts to bypass the security of the UCS 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 system 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.
T.CONFIGURE_NO	A TOE administrator with authorized access to one or more UCS locales (domains) unknowingly (due to unfamiliarity with the current TOE configuration, or unfamiliarity with TOE administrative guidance) attempts to access or modify attributes of another UCS locale to which the administrator has not been granted access, resulting in misconfiguration of the TOE.
T.ATTACK_ANOTHER	A system user (VM user, OS administrator, or Hypervisor administrator) attempts to bypass TOE controls to gain unauthorized access to another UCS-hosted environment resulting in a violation of a TOE SFP.

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 Obj.	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.VLANSEC	The TOE must ensure that Ethernet frames received by the TOE are only forwarded in a manner consistent with the VLAN for which the traffic is associated.

TOE Security Obj.	TOE Security Objective Definition
O.VSANSEC	The TOE must ensure that FC-2 frames received by the TOE are only forwarded in a manner consistent with the VSAN for which the traffic is associated.
O.ADMIN	The TOE must provide a secure channel for administration.

4.2.   Security Objectives for the Environment

The assumptions identified previously are incorporated as security objectives for the environment. They levy additional requirements on the environment, which are largely satisfied through procedural or administrative measures. The following table, Security Objectives for the Environment, identifies the security objectives for the environment.

Table 8: Security Objectives for the Environment

Env. Security Objectives	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.VSAN	Each network interface of a storage device in the operational environment of the TOE may only participate in a single VSAN.
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. The physical security does not apply to Java applets once the applets have been downloaded from the Fabric Interconnect to a management workstation.
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 verbatim from Part 2 of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, dated: September 2012

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:

- Refinement: Indicated with **bold** text, or ~~strikethrough~~ as necessary;
- Selection: Indicated with <u>underlined</u> text;
- Assignment: text in brackets ([ ]);
- Assignment within a Selection: Indicated with [<u>underlined</u>] text in brackets;
- Iteration: Indicated by appending the iteration number and the iteration title in parenthesis, e.g., (1), (2), (3).

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 9: Security Functional Requirements

SFR	Component Name
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_ACC.2	Complete access control
FDP_ACF.1	Security attribute based access control
FDP_IFC.1 (1)	Subset information flow control (1)
FDP_IFC.1 (2)	Subset information flow control (2)
FDP_IFF.1 (1)	Simple security attributes (1)
FDP_IFF.1 (2)	Simple security attributes (2)
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_MOF.1	Management of security functions behavior
FMT_MSA.1 (1)	Management of security attributes (1)
FMT_MSA.1 (2)	Management of security attributes (2)
FMT_MSA.1 (3)	Management of security attributes (3)
FMT_MSA.3 (1)	Static attribute initialization (1)
FMT_MSA.3 (2)	Static attribute initialization (2)
FMT_MSA.3 (3)	Static attribute initialization (3)
FMT_MTD.1 (1)	Management of TSF data (1)
FMT_MTD.1 (2)	Management of TSF data (2)
FMT_SAE.1	Time-based authorization
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FPT_FLS.1	Failure with preservation of secure state
FPT_ITT.2	TSF data transfer separation
FPT_PHP.1	Passive detection of physical attack
FPT_RCV.2	Automated recovery
FPT_STM.1	Reliable time stamps
FTP_TRP.1	Trusted Path

■

5.2.1. Security audit (FAU)

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 <u>not specified</u> level of audit; and
c) [the events listed in Table 11].

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, 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 ST, [information specified in column three of Table 11].

Table 10: Auditable Events

Functional Component	Auditable Event	Additional Audit Record Content
FMT_SMR.1	Modifications to user role assignments. Modifications to mappings between roles and privileges.	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 UCSM CLI and GUI	The user identities provided to the UCSM.
FDP_ACF.1	Role-based access control requests submitted via the UCSM CLI, and GUI.	The user identity requesting the change and the object being accessed.
FPT_PHP.1	Insertion/removal of server disks. Insertion/removal of network cards or expansion cards.	Identification of the server (or Fabric Interconnect, or Fabric Extender) and device (disk drive or network card or expansion card)
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.

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.

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]

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 <u>prevent</u> unauthorized modifications to the stored audit records in the audit trail.

FAU_STG.4   **Protected audit trail storage**

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

5.2.2. User Data Protection (FDP)

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.

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:
    - o User Identity – Identity of the administrator
    - o Locale – Identification of resources for which the user has authority
    - o Privileges – The cumulative set of privileges obtained from the roles assigned to the Authenticated Administrator.

Object security attributes:

- Resource
    - o Locale - Identification of resource group
- Configuration Settings
    - o 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 in which the assigned locale for the Authenticated Administrator and the assigned locale for the Resource are the same. Authenticated Administrators assigned locales that are different from the locales assigned to the Resources are not granted access, and,
- 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 (per the locale)].

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].

FDP_IFC.1(1)   Subset Information Flow Control (1)

FDP_IFC.1.1(1)   The TSF shall enforce the [VLAN information flow control SFP] on [

Subject: physical network interfaces

Information: IP packets

Operations: permit or deny layer two communication].

FDP_IFC.1(2)   Subset Information Flow Control (2)

FDP_IFC.1.1(2)   The TSF shall enforce the [VSAN information flow control SFP] on [

Subjects: Switch network interfaces
Information: FC-2 Frames
Operations: Permit or Deny FC Frames].

FDP_IFF.1(1)   Simple Security Attributes (1)

FDP_IFF.1.1(1)   The TSF shall enforce the [VLAN information flow control SFP] based on the following types of subject and information security attributes: [

Subject Security Attributes:
     • Assigned VLAN ID
Information Security Attributes:
     • VLAN ID field in 802.1q Frame Header].

FDP_IFF.1.2(1)   The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [the receiving VLAN interface must be assigned a VLAN ID, and that assigned VLAN ID must match the VLAN ID in the 802.1q header of the received frame, or the received frame must be untagged].

FDP_IFF.1.3(1)	The TSF shall enforce the [information flow so that only frames containing a matching VLAN ID in the header will be forwarded to other VLAN interfaces with a matching assigned VLAN ID].
FDP_IFF.1.4(1)	The TSF shall explicitly authorize an information flow based on the following rules: [untagged frames are assigned the native VLAN ID of the switch (VLAN 1 by default) and thus may be received at VLAN interfaces with any VLAN ID].
FDP_IFF.1.5(1)	The TSF shall explicitly deny an information flow based on the following rules: [none].

FDP_IFF.1(2)   **Simple Security Attributes (2)**

FDP_IFF.1.1(2)	The TSF shall enforce the [VSAN information flow control SFP] based on the following types of subject and information security attributes: [
	Subject Security Attributes:
	• Assigned VSAN ID
	Information Security Attributes:
	• VSAN ID field in the EISL Frame Header].
FDP_IFF.1.2(2)	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [the VSAN ID in the EISL frame header must match the VSAN ID associated with the FCoE VLAN that receives the frame].
FDP_IFF.1.3(2)	The TSF shall enforce the [information flow so that only frames with a matching VSAN ID in the header will be forwarded].
FDP_IFF.1.4(2)	The TSF shall explicitly authorize an information flow based on the following rules: [untagged frames are assigned VSAN ID of 1 and thus may be received at VSAN interfaces with VSAN ID 1].
FDP_IFF.1.5(2)	The TSF shall explicitly deny an information flow based on the following rules [none].

5.2.3. Identification and Authentication (FIA)

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 (UCSM, and SNMPv3):
	    a) login id;
	    b) password;
	and for UCSM users only:
	    d) SSH key pair (optional instead of password);
	    e) account expiration date;
	    f) locale;

And for SNMPv3 users only:
g) privacy password].

FIA_SOS.1   **Verification of secrets**

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

- At least eight characters long;
- Does not contain more than three consecutive characters, such as abcd;
- Does not contain more than two repeating characters, such as aaabbb;
- Does not contain dictionary words;
- Does not contain common proper names].

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 pre-configured passwords which do not meet the quality metrics.

FIA_UAU.2   **Timing of authentication**

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.

FIA_UAU.5   **Multiple authentication mechanisms**

FIA_UAU.5.1   The TSF shall provide [

- Local authentication:
  - Password;
  - SSH public key authentication (for SSH, not for UCSM);
- Remote authentication:
  - RADIUS;
  - LDAP;
  - TACACS+;

] 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 proof of possession of SSH private key or by querying a remote authentication server].

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.

5.2.4. Security Management (FMT)

FMT_MOF.1   **Management of security functions behaviour**

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].

FMT_MSA.1(1)   **Management of security attributes (1)**

FMT_MSA.1.1(1)   The TSF shall enforce the [VLAN information flow control SFP] to restrict the ability to query, modify, delete, [none] the security attributes [sending and receiving VLAN interface and VLAN ID in packet header specified in VLAN policies] to [Administrator, Network Administrator, and any custom role holding ext-lan-config, ext-lan-policy or admin privilege].

FMT_MSA.1(2)   **Management of security attributes (2)**

FMT_MSA.1.1(2)   The TSF shall enforce the [VSAN information flow control SFP] to restrict the ability to modify, [none] the security attributes [sending and receiving VSAN interface and VSAN ID specified in VLAN policies] to [Administrator, Network Administrator, and any custom role holding ext-san-config, ext-san-policy or admin privilege].

FMT_MSA.1(3)   **Management of security attributes (3)**

FMT_MSA.1.1(3)   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, AAA Administrator, and any custom role holding aaa or admin privilege].

FMT_MSA.3(1)   **Static attribute initialization (1)**

FMT_MSA.3.1(1)   The TSF shall enforce the [VLAN information flow control SFP] to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(1)   The TSF shall allow [Administrator, Network Administrator, and any custom role holding ext-lan-config, or ext-lan-policy or admin privilege] to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3(2)   **Static attribute initialization (2)**

FMT_MSA.3.1(2)   The TSF shall enforce the [VSAN information flow control SFP] to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(2)   The TSF shall allow [Administrator, Network Administrator, and any custom role holding ext-san-config, ext-san-policy or admin privilege] to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3(3)   **Static attribute initialization (3)**

FMT_MSA.3.1(3)   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(3)   The TSF shall allow [Administrator, AAA Administrator, and any custom role holding aaa or admin privilege] to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1(1)   Management of TSF data (1)

FMT_MTD.1.1(1)   The TSF shall restrict the ability to query, modify, delete, [and assign] the [user attributes defined in FIA_ATD.1.1] to [Administrator, AAA Administrator, and any custom role holding aaa or admin privilege].

FMT_MTD.1(2)   Management of TSF data (2)

FMT_MTD.1.1(2)   The TSF shall restrict the ability to [set] the [time and date used to form the timestamps in FPT_STM.1.1] to [Administrator, Operations, Network Administrator, and any custom role holding operations, ext-lan-config, ext-lan-security, or admin privilege].

FMT_SAE.1 Time-limited authorisation

FMT_SAE.1.1   The TSF shall restrict the capability to specify an expiration time for [UCSM accounts] to [Administrator, AAA Administrator, and any custom role holding aaa or admin privilege].

FMT_SAE.1.2   For each of these security attributes, the TSF shall be able to [lock expired UCSM accounts] after the expiration time for the indicated security attribute has passed.

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

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 system time for FPT_STM.1.1.].

FMT_SMR.1   Security roles

FMT_SMR.1.1   The TSF shall maintain the roles [

- aaa (AAA Administrator)
- admin (Administrator)
- facility-manager (Facility Manager)
- network (Network Administrator)
- operations (Operations)
- read-only (Read-Only)

- server-compute (Server Compute Administrator)
- server-equipment (Server Equipment Administrator)
- server-profile (Server Profile Administrator)
- server-security (Server Security Administrator)
- storage (Storage Administrator)
- custom roles

].

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

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

5.2.5. Protection of the TSF (FPT)

FPT_FLS.1   **Failure with preservation of secure state**

FPT_FLS.1.1   The TSF shall preserve a secure state when the following types of failures occur [failure of hardware subcomponents and software subcomponents].

Application note: The failures relevant to this SFR are those that would potentially result in network connectivity failures, and are mitigated by the TOE automatically making use of redundant network paths.

FPT_ITT.2   **TSF data transfer separation**

FPT_ITT.2.1   The TSF shall protect TSF data from <u>disclosure, modification</u> when it is transmitted between separate parts of the TOE.

FPT_ITT.2.2   The TSF shall separate user data from TSF data when such data is transmitted between separate parts of the TOE.

Application note: The TSF data relevant to this SFR is the traffic transmitted on the isolated VLANs across network cables among the physically separate components of the TOE (Fabric Interconnects, Fabric Extenders, and Servers).

FPT_PHP.1   **Passive detection of physical attack**

FPT_PHP.1.1   The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.1.2   The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

FPT_RCV.2   **Automated recovery**

FPT_RCV.2.1   When automated recovery from [failure of a standalone (un-clustered) Fabric Interconnect, or failure of one or more clustered Fabric Interconnects] is not possible, the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.

FPT_RCV.2.2   For [failure of the primary (active) clustered Fabric Interconnect when a secondary (passive) cluster member is online], the TSF shall ensure the return of the TOE to a secure state using automated procedures.

FPT_STM.1   **Reliable time stamps**

FPT_STM.1.1   The TSF shall be able to provide reliable time stamps **for its own use**.

5.2.6. Trusted Path/Channels (FTP)

FTP_TRP.1   **Trusted path**

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

FTP_TRP.1.2   The TSF shall permit <u>remote users</u> to initiate communication via the trusted path.

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

Application note: Remote administrative interfaces relevant to this SFR include the UCSM CLI (via SSH), UCSM 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.

5.3.   TOE SFR Hierarchies and Dependencies

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 11: Security Functional Requirement Dependencies

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	FMT_MSA.3 FDP_ACC.1	Met by FMT_MSA.3(3) Met by FDP_ACC.2
FDP_IFC.1(1)	FDP_IFF.1	Met by FDP_IFF.1(1)

FDP_IFC.1(2)	FDP_IFF.1	Met by FDP_IFF.1(2)
FDP_IFF.1(1)	FDP_IFC.1 FMT_MSA.3	Met by FDP_IFC.1(1) Met by FMT_MSA.3 (1)
FDP_IFF.1(2)	FDP_IFC.1 FMT_MSA.3	Met by FDP_IFC.1(2) Met by FMT_MSA.3 (2)
FIA_ATD.1	No dependencies	N/A
FIA_SOS.1	No dependencies	N/A
FIA_UAU.2	FIA_UID.1	Met by FIA_UID.2
FIA_UAU.5	No dependencies	N/A
FIA_UID.2	No dependencies	N/A
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	Met by FMT_SMR.1 and FMT_SMF.1
FMT_MSA.1(1)	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Met by FDP_IFC.1 (1) Met by FMT_SMR.1 Met by FMT_SMF.1
FMT_MSA.1(2)	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Met by FDP_IFC.1 (2) Met by FMT_SMR.1 Met by FMT_SMF.1
FMT_MSA.1(3)	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Met by FDP_ACC.2 Met by FMT_SMR.1 Met by FMT_SMF.1
FMT_MSA.3 (1)	FMT_MSA.1 FMT_SMR.1	Met by FMT_MSA.1 (1) Met by FMT_SMR.1
FMT_MSA.3 (2)	FMT_MSA.1 FMT_SMR.1	Met by FMT_MSA.1 (2) Met by FMT_SMR.1
FMT_MSA.3 (3)	FMT_MSA.1 FMT_SMR.1	Met by FMT_MSA.1 (3) Met by FMT_SMR.1
FMT_MTD.1(1)	FMT_SMF.1 FMT_SMR.1	Met by FMT_SMF.1 Met by FMT_SMR.1
FMT_MTD.1(2)	FMT_SMF.1 FMT_SMR.1	Met by FMT_SMF.1 Met by FMT_SMR.1
FMT_SAE.1	FMT_SMR.1 FPT_STM.1	Met by FMT_SMR.1 Met by FPT_STM.1
FMT_SMF.1	No dependencies	N/A
FMT_SMR.1	FIA_UID.1	Met by FIA_UID.2
FPT_FLS.1	No dependencies	N/A
FPT_ITT.2	No dependencies	N/A
FPT_PHP.1	No dependencies	N/A
FPT_RCV.2	AGD_OPE.1	Met by AGD_OPE.1
FPT_STM.1	No dependencies	N/A
FTP_TRP.1	No dependencies	N/A

5.4. TOE Security Assurance Requirements

The TOE assurance requirements for this ST are EAL2 derived from Common Criteria Version 3.1, Revision 4. The assurance requirements are summarized in the table below.

Table 12: SAR Requirements

Assurance Class	Components	Components Description
Development	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_OPE.1	Operational user guidance

	AGD_PRE.1	Preparative User guidance
Life Cycle Support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

5.4.1. 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.

5.5.   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 13: Assurance Measures

Component	How the requirement will be met
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)).
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.
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 ATE_FUN.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_IND.2	Cisco will provide the TOE for testing.
AVA_VAN.2	Cisco will provide the TOE for testing.

6. TOE Summary Specification

6.1. TOE Security Functional Requirement Measures

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

Table 14: TOE SFRs Measures

TOE SFRs	How the SFR is Met
FAU_GEN.1	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, type of event (identifier code), subject identities, and outcome of the event as in this example:

19252,sys/user-ext/sh-login-admin-ttyS0_1_3947,session,internal,2009-06-18T01:48:31,creation,Fabric A: local user admin logged in from console

Auditable events include:

Auditable Event	Rationale
Successful modifications to user role assignments and modifications to mappings between roles and privileges.	Successful modifications to users/roles/privileges are logged in the local audit log. Failed attempts to make such modifications are not logged.
Successful and failed use of the user authentication mechanism on UCSM CLI and GUI	All login attempts to the UCSM 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.
Successful role-based access control requests submitted via the UCSM CLI, and GUI.	Successful changes to configuration data is logged to the local admin log.
Successful and failed attempts to change to the time.	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.
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 Manager 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 Manager. The administrator can view TOE audit records through the provided GUI and CLI. When the TOE is deployed in a clustered configuration, audit review for the entire cluster is permitted.
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. When the TOE is deployed in a clustered configuration, audit review for the entire cluster is permitted. Sorting and filtering options via CLI are limited, so use of GUI is recommended for reviewing logs.
FAU_STG.1	Audit records can be viewed by the authorized administrator via the UCS Manager. 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 Manager. The file cannot be altered. When the TOE is deployed in a clustered configuration, audit logs are stored centrally on the primary UCS Manager instance and replicated to secondary instances for backup purposes.
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. When the TOE is deployed in a clustered configuration, audit logs are stored centrally on the primary UCS Manager instance and replicated to secondary instances for backup purposes.

FDP_IFC.1(1) and FDP_IFF.1(1)	Network interfaces are grouped into VLANs, so Layer 2 broadcast packets will be issued to only interfaces within that VLAN. Packets will have a VLAN ID associated to them indicating which VLAN they are allowed to access. The TOE will enforce VLAN separation by only allowing packets onto the VLAN that matches the VLAN ID. VLAN traffic will not be forwarded to interfaces not in that VLAN.
FDP_IFC.1 (2) and FDP_IFF.1(2)	VSANs provide isolation among devices that are physically connected to the same fabric. The underlying VSAN implementation allows creation of multiple logical SANs over a common physical infrastructure. Each VSAN can contain up to 239 switches and has an independent address space that allows identical Fibre Channel IDs (FCIDs) to be used simultaneously in different VSANs.
	Traffic is contained within VSAN boundaries and devices reside only in one VSAN thus ensuring absolute separation between the data traversing separate VSANs. This ensures the traffic flow control of data traversing the VSAN from users and devices belonging to other VSANs. Each separate virtual fabric is isolated from one another using a hardware-based frame tagging mechanism on VSAN member ports.
	When traffic is sent or received on a VSAN interface the TOE examines the VSAN ID. If the TOE is configured, through assignment of administrator-defined Service Policies, to allow the frames to pass, the traffic will be allowed to flow. Otherwise, the traffic is not allowed to pass.
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 nine 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. The TOE also provides the ability to define custom roles with custom sets of privileges. During user creation each administrator is assigned a User ID, a Locale, and role assignments. The Locale attribute defines system resources that the administrator can access. If a resource is assigned a different Locale than the Administrator, no access is granted. For resources that an administrator may access, the role assigned to the administrator defines the administrative capabilities that administrator is permitted for that resource. If an administrator is assigned a role without access to a specific Configuration Setting, the administrator cannot access the object.
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, • SSH key pair, • Account Expiration, • Role, and • Locale. 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: • At least eight characters long • Does not contain more than three consecutive characters, such as abcd • Does not contain more than two repeating characters, such as aaabbb • Does not contain dictionary words • Does not contain common proper names 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, UCS Manager 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 Manager 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. A user account may also be configured with an SSH public key to facilitate SSH public key authentication. User SSH keys may be entered in OpenSSH, SECSH and X.509 certificate formats.
	In the case of remote authentication, user credentials are passed to a remote RADIUS, TACACS+ or 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 public key authentication if keys have been provisioned for the user, otherwise it uses SSH password authentication, verified against the local authentication database or remote authentication server.
FMT_MOF.1	All administrative accounts are assigned at least 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(1) FMT_MSA.1(2) FMT_MSA.1(3)	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 with the 'aaa' privilege. Similarly, users are associated with no locales (note this is distinct from being associated with an empty locale with global organizational access).
	The TOE provides the following access to TOE administrative functionality :
	A. Accounts with the privileges associated with "Network Administrator" Role have query, modify, and delete access to the VLAN Policies
	B. Accounts with the privileges associated with "Storage Administrator" Role have modify access to the VSAN Policies
	C. 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(1) FMT_MSA.3(2) FMT_MSA.3(3)	Restrictive default values are provided for VLANs, VSANs, and role based access control.
	No information flows are allowed for traffic (VLAN/VSAN) unless the traffic the attribute combination of receiving/sending interface and VLAN/VSAN ID is explicitly allowed in an administratively configured information flow policy.
	No administrative access is granted unless the role associated with the administrative user attempting to access the TOE is allowed access.
FMT_MTD.1(1) FMT_MTD.1(2)	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 *aaa* or *admin* privilege access to another user's security attributes (ID, Password, SSH Key, Account Expiration Date, Role, and Locale), with the limitation that the assignment of organizations is restricted to only those in the locale of the user assigning the organizations. The TOE only allows users with the *admin, operations, ext-lan-config,* or *ext-lan-security* privilege the ability to set the TOE time.

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).

FMT_SMF.1 (continued):

The TOE provides the ability manage the operation of the TOE, audit trail, administrative access, administrative users and timestamps. Administrators can configure:

- Auditing:
  - o 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.
  - o 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.
  - o 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, RADIUS, and TACACS+.
- Timestamps: Manually set the local system time, or add/remove one or more NTP servers.

FMT_SMR.1:

Table 4 (ST section 2.9.5.1) lists the privileges associated with management capabilities and default roles supported by the TOE. Other privileges exist in UCS that can be assigned to roles as needed to define custom roles, but the other privileges defined in UCS are not relevant to supporting the security functionality described in the FMT_* requirements in this ST. 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).

Privilege	Relevance to Evaluated Security Functions
aaa	FMT_MSA.1.1(3)FMT_MSA.3.2(3) FMT_MTD.1.1(1) FMT_SAE.1.1
admin	FMT_MSA.1.1(1) FMT_MSA.1.1(2) FMT_MSA.1.1(3) FMT_MSA.3.2(1) FMT_MSA.3.2(2) FMT_MSA.3.2(3) FMT_MTD.1.1(1) FMT_MTD.1.1(2) FMT_SAE.1.1
ext-lan-config	FMT_MSA.1.1(1) FMT_MSA.3.2(1) FMT_MTD.1.1(2)
ext-lan-policy	FMT_MSA.1.1(1) FMT_MSA.3.2(1)
ext-lan-qos	None
ext-lan-security	FMT_MTD.1.1(2)
ext-san-config	FMT_MSA.1.1(2) FMT_MSA.3.2(2)
ext-san-policy	FMT_MSA.1.1(2) FMT_MSA.3.2(2)
ext-san-qos	None

ext-san-security	None
fault	None
operations	FMT_MTD.1.1(2)
org-management	None
pod-config	None
pod-policy	None
pod-qos	None
pod-security	None
power-mgmt	None
read-only	None
server-equipment	None
server-maintenance	None
server-policy	None
server-security	None
service-profile-compute	None
service-profile-config	None
service-profile-config-policy	None
service-profile-ext-access	None
service-profile-network	None
service-profile-network-policy	None
service-profile-qos	None
service-profile-qos-policy	None
service-profile-security	None
service-profile-security-policy	None
service-profile-server	None
service-profile-server-oper	None
service-profile-server-policy	None
service-profile-storage	None
service-profile-storage-policy	None

FPT_FLS.1	UCS can be configured with redundant network paths, and/or with the Fabric Interconnects in a clustered configuration such that failure of one UCS component does not result in loss of system functionality, and does not compromise the security of the system. Use of redundant network paths can be achieved with a single (non-clustered) Fabric Interconnect with multiple uplink ports configured as a port-channel, which provides bandwidth aggregation as well as link redundancy, so if one uplink fails the other will continue to operate.
FPT_ITT.2	Transfer of configuration data between Fabric Interconnects and Fabric Extenders, and between Fabric Extenders and Servers is protected by use of VLAN-protected Layer-2 communications using VLANs reserved for UCS management traffic and isolated from user traffic to/from guest VMs and storage devices.
FPT_PHP.1	UCS can be configured to alert and generate audit messages for a variety of hardware changes and network connectivity changes. Viewing audit messages requires the 'read-only' privilege, and all roles (default and custom) include the 'read-only' privilege.
FPT_RCV.2	When a stand-alone Fabric Interconnect with UCSM fails, or a cluster of Fabric Interconnects fail, the Fabric Interconnect can be administered via local console connection instead of through UCSM GUI, allowing maintenance and troubleshooting of the system. When two Fabric Interconnects are configured as a clustered pair, the primary (active) FI sends configuration changes to subordinate (passive) FI to ensure the two remain synchronized. The subordinate FI polls the primary FI using 'keep-alive' messages to confirm the primary FI continues to be active. If the primary FI fails to respond, the subordinate FI will promote itself from subordinate to primary, its database will become the active database, and its ports will begin to forward traffic in accordance with the

	current configuration. If the original primary FI becomes active again it will begin to poll the new primary FI using 'keep-alive' messages, but it will not automatically promote itself to primary. Authorized administrators can manually trigger a change in primary/subordinate status at any time.
FPT_STM.1	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. This functionality can be set in UCSM.
FTP_TRP.1	The UCS Fabric Interconnect protects remote command line access to management functions using the SSH protocol for authentication, integrity protection and confidentiality. The SSH implementation RSA keys of 2048 bit modulus. To achieve trusted path requires that an authorized administrator holding the aaa or admin privilege configures user keys. Distribution of those user keys is outside the scope of the TOE.
	The UCS Fabric Interconnect protects remote web-based access to management functions using the TLS (TLS1.0, TLS1.1, and TLS1.2) from the UCSM client software (Java applet, or HTML), or customized queries, all of which access the underlying XML API via the web server running on the Fabric Interconnect.

6.2.   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 (UCSM) interface. The CLI interface achieves a trusted path via SSH public key 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.

There are no unmediated traffic flows into or out of the TOE. The information flow policies identified in the SFRs are applied to all traffic received and sent by the UCS. Both communication types including data plane communication and, control plane communications are mediated by the TOE. Data plane communication refers to data-center traffic that sent and received to/from external IT entities. Control plane

communications refer to administrative traffic used to control the operation of the TOE. There is no opportunity for unaccounted traffic flows to flow into or out of the TOE.

The TOE provides a secure domain for each VLAN to operate within. Each VLAN has its own forwarding plane resources that other VLANs within the same TOE are not able to affect.

The TOE provides a secure domain for each VSAN to operate within. Each VSAN has its own resources that other VSANs within the same TOE are not able to affect.

The TOE includes the Cisco UCS Manager 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 Manager 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 the Security Objectives

Table 15: Summary of Mappings between Threats, Policies and the Security Objectives

	O.IDAUTH	O.ENCRYP	O.AUDREC	O.ACCOUN	O.SECFUN	O.VLANSEC	O.VSANSEC	O.ADMIN
T.NORMAL_USE						X	X	
T.NOAUTH	X					X	X	
T.SNIFF		X						X
T.ACCOUNTABILITY			X	X	X			
T.CONFIGURE_NO					X			
T.ATTACK_ANOTHER						X	X	

Table 16: Rationale for Mapping of Threats, Policies and the Security Objectives for the TOE

Objective	Rationale
O.IDAUTH	This security objective is necessary to counter the threat T.NOAUTH because it ensures that all users must be authenticated.

Objective	Rationale
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 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.CONFIGURE_NO by ensuring the TOE provides the means for administrative users to appropriately configure the TOE. Additionally, this objective provides the administrative capability to reconfigure previous administrative actions.
O.VLANSEC	This security objective is necessary to counter the threats: T.NORMAL_USE, T.NOAUTH, and T.ATTACK_ANOTHER by requiring that the TOE only forward traffic in a manner consistent with the VLANs for which the traffic is associated preventing access to resources for which the traffic should not be associated.
O.VSANSEC	This security objective is necessary to counter the threats: T.NORMAL_USE, T.NOAUTH, and T.ATTACK_ANOTHER by requiring that the TOE only forward traffic in a manner consistent with the VSANs for which the traffic is associated preventing access to resources for which the traffic should not be associated.
O.ADMIN	This security objective counters the threat T.SNIFF by providing a secure channel for administration.

Table 17: Mappings of Assumptions and the Security Objectives for the OE

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

Table 18: Rationale for Mapping of Threats, Policies and Objectives for the OE

Objective	Rationale
OE.ADMIN	This security objective satisfies A.ADMIN by ensuring that competent and trusted administrators manage the TOE.
OE.VSAN	This security objective satisfies A.VSAN by ensuring that devices connected to the TOE will only participate in one VSAN per network interface.
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.

Table 19: Summary of Mappings between SFRs and Security Objectives

SFR	O.IDAUTH	O.ENCRYP	O.AUDREC	O.ACCOUN	O.SECFUN	O.VLANSEC	O.VSANSEC	O.ADMIN
FAU_GEN.1			X	X				
FAU_SAR.1			X	X				
FAU_SAR.3			X	X				
FAU_STG.1	X				X			
FAU_STG.4	X		X	X	X			
FDP_ACC.2					X			
FDP_ACF.1					X			
FDP_IFC.1 (1)						X		
FDP_IFC.1 (2)							X	
FDP_IFF.1 (1)						X		
FDP_IFF.1 (2)							X	
FIA_ATD.1	X							
FIA_SOS.1	X							
FIA_UAU.2	X							
FIA_UAU.5	X							
FIA_UID.2	X							
FMT_MSA.1 (1)					X			
FMT_MSA.1 (2)					X			
FMT_MSA.1 (3)					X			
FMT_MSA.3 (1)					X			
FMT_MSA.3 (2)					X			
FMT_MSA.3 (3)					X			
FMT_MTD.1 (1)					X			

FMT_MTD.1 (2)					X			
FMT_SAE.1					X			
FMT_SMF.1					X			
FMT_SMR.1					X			
FPT_FLS.1					X			
FPT_ITT.2					X			X
FPT_PHP.1					X			
FPT_RCV.2					X			
FPT_STM.1			X					
FTP_TRP.1		X						X

7.2. Rationale for SFRs/TOE Objectives

This section provides rationale for the Security Functional Requirements demonstrating that the Security Functional Requirements are suitable to address the security objectives. The table below illustrates the mapping from SFRs to Security Objectives.

Table 20: Summary of Mappings between IT Security Objectives and SFRs

SFR	Rationale for Mapping to Objective
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.
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.
FDP_IFC.1 (1)	This component satisfies this policy by ensuring that all Ethernet traffic received from an external entity is only passed if it is associated with a configured VLAN.

	This component traces back to and aids in meeting the following objective: O.VLANSEC.
FDP_IFC.1 (2)	This component satisfies this policy by ensuring that all FC-2 frames received from an external entity are only passed if they are associated with a configured VSAN.
	This component traces back to and aids in meeting the following objective: O.VSANSEC.
FDP_IFF.1 (1)	This component satisfies this policy by ensuring that all Ethernet traffic received from an external entity is only passed if it is associated with a configured VLAN.
	This component traces back to and aids in meeting the following objective: O.VLANSEC.
FDP_IFF.1 (2)	This component satisfies this policy by ensuring that all FC-2 frames received from an external entity are only passed if they are associated with a configured VSAN.
	This component traces back to and aids in meeting the following objective: O.VSANSEC.
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.
	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_MSA.1 (1)	This component ensures the TSF enforces the VLAN SFP to restrict the ability to query, delete, and modify those security attributes that are listed in section FDP_IFF.1 (1).
	This component traces back to and aids in meeting the following objectives: O.SECFUN.
FMT_MSA.1 (2)	This component ensures the TSF enforces the VSAN SFP to restrict the ability to modify those security attributes that are listed in section FDP_IFF.1 (2).
	This component traces back to and aids in meeting the following objectives: O.SECFUN.
FMT_MSA.1 (3)	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 (1)	This component ensures that there is a default deny policy for the VLAN information flow control security rules.
	This component traces back to and aids in meeting the following objectives: O.SECFUN
FMT_MSA.3 (2)	This component ensures that there is a default deny policy for the VSAN information flow control security rules.
	This component traces back to and aids in meeting the following objectives: O.SECFUN

FMT_MSA.3 (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 (1)	This component ensures that the TSF restrict abilities to query, modify, delete and assign certain user attributes as defined in FIA_ATD.1.1 to only the authorized administrator.
	This component traces back to and aids in meeting the following objective: O.SECFUN.
FMT_MTD.1 (2)	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.
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_FLS.1	This component helps ensure the TOE is protected from unintended configuration changes through the ability maintain the integrity of the system in partial or fully failed states.
	This component traces back to and aids in meeting the following objective: O.SECFUN.
FPT_ITT.2	This component ensures that the TOE protects TSF data when it is transmitted between separate parts of the TOE.
	This component traces back to and aids in meeting the following objectives: O.SECFUN , and O.ADMIN.
FPT_PHP.1	This component helps ensure the TOE is protected from unintended configuration changes through the ability monitor changes to hardware configurations and connectivity.
	This component traces back to and aids in meeting the following objective: O.SECFUN.
FPT_RCV.2	This component helps ensure the TOE is protected from unintended configuration changes through the ability to recover to a known-good state after full or partial failure.
	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.Glossary: Acronyms and Abbreviations

The following acronyms and abbreviations are used in this Security Target:

Table 21: Acronyms or Abbreviations

Acronym or Abbreviation	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.
LAN	Local Area Network
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, 1285, 1240, 1280, 1340, and 1380.
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

XML	Extensible Markup Language
XML API	The UCS Manager XML API is a programmatic interface for managing UCS via CLI, or GUI.

9. Glossary: References and Related Documents

The following documentation was used to prepare this ST:

[CC_PART1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated September 2006, version 3.1, Revision 4, CCMB-2006-09-001

[CC_PART2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated September 2007, version 3.1, Revision 4, CCMB--2007-09-002

[CC_PART3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated September 2007, version 3.1, Revision 4, CCMB-2007-09-003

[CEM] Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated September 2007, version 3.1, Revision 2, CCMB-2007-09-004

10. Obtaining Documentation, Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html