Cisco Intersight Virtual Appliance with IMM Fabric and UCS Servers

Security Target

Version 0.12

February 10 2025

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

Table of Contents

List of Tables

List of Figures

Acronyms

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

Table 1 Acronyms

Acronyms / Abbreviations	Definition
API	Application Programming Interface
BMC	Baseboard Management Controller (renamed to CIMC)
CIMC	Cisco Integrated Management Controller
CLI	Command Line Interface
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.
LAN	Local Area Network
mLOM	Modular LAN on Motherboard
NIC	Network Interface Card, a physical or virtual (vNIC) adapter provide connectivity between a device/host and a network.
SNMP	Simple Network Management Protocol
SSH	Secure Shell
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
UCS	Unified Computing System
UUID	Universally Unique IDentifier
VIC	Virtual Interface Card, one of several Cisco interface cards for UCS servers.
VLAN	Virtual Local Area Network
VM	Virtual Machine, a virtualized guest operating system installed to a hypervisor.
VMM	Virtual Machine Manager, a hypervisor.
PVA	Private Virtual Appliance

DOCUMENT INTRODUCTION

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

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

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

1 SECURITY TARGET INTRODUCTION

The Security Target contains the following sections:

- Section 1: Security Target Introduction
- Section 2: Conformance Claims
- Section 3: Security Problem Definition
- Section 4: Security Objectives
- Section 5: IT Security Requirements
- Section 6: TOE Summary Specification
- Section 7: 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 Reference

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

Table 2 ST and TOE Identification

Name	Description
ST Title	Cisco Intersight Virtual Appliance with IMM Fabric and UCS Servers Security Target
ST Version	0.12
Publication Date	February 10 2025
TOE Guidance	Cisco Intersight Virtual Appliance with IMM Fabric and UCS Servers Common Criteria Operational User Guidance and Preparative Procedures, v0.7
Vendor and ST Author	Cisco Systems, Inc.
TOE Reference	Cisco Intersight Virtual Appliance 1.0.9 with IMM Fabric 4.3 UCS X-Series Servers and UCS C-Series Servers

TOE Hardware Models	➢ Cisco UCS X-Series: ▪ Chassis: UCSX-9508 ▪ M6 Compute Nodes (servers): UCSX-210C-M6 • VIC in M6 compute nodes: UCSX-V4-Q25GME, UCSX-V4-PCIME, or UCSX-V4-PCIME ▪ M7 Compute Nodes (servers): UCSX-210C-M7, UCSX-410C-M7 • VIC in M7 compute nodes: UCSX-ME-V5Q50G-D, UCSX-ML-V5Q50G-D, UCSX-ML-V5D200G-D, or UCSX-V4-PCIME ➢ Cisco UCS C-Series Servers and Virtual Interface Cards (VIC): ▪ M6 Servers[1]: UCSC-C220-M6, UCSC-C225-M6, UCSC-C240-M6, UCSC-C245-M6 • VIC for M6 C-Series servers: UCSC-PCIE-C25Q-04, UCSC-PCIE-C100-04, UCSC-P-V5Q50G, UCSC-P-V5D200G, UCSC-M-V25-04, UCSC-M-V5Q50G, UCSC-M-V100-04, UCSC-M-V5D200G ▪ M7 Servers[1]: UCSC-C220-M7, UCSC-C240-M7 • VIC for M7 C-Series servers: Same as for M6 C-Series servers. ➢ Cisco Fabric Interconnect (FI): ▪ UCS-FI-6454, UCS-FI-64108, and/or UCS-FI-6536 ➢ Cisco Intelligent Fabric Modules (IFM): ▪ For M6 compute nodes: UCSX-I-9108-25G, UCSX-I-9108-100G ▪ For M7 compute nodes: UCSX-I-9108-25G-D, UCSX-I-9108-100G-D
TOE Software Version	Cisco Intersight Virtual Appliance (PVA) version 1.0.9-677 (running on any UCS server listed in the TOE Hardware Models) Cisco Intersight Managed Mode (IMM) version 4.3(4.240074) Cisco UCS C-Series Server Firmware version 4.3(4.240152) Cisco UCS X-Series Server Firmware version 5.2(0.230127)
Keywords	Virtualization, fabric, server, RBAC, authentication

1.2 TOE Overview

The Target of Evaluation (TOE) is a unified computing solution, which provides access layer networking and servers. The TOE is the Cisco Intersight Virtual Appliance with IMM Fabric and UCS Servers, hereafter referred to as Cisco Intersight.

1.2.1 TOE Product Type

The TOE consists of hardware and software components that support Cisco's unified fabric, which carries multiple types of datacenter traffic over a dedicated fabric hardware (in the form of stand-alone appliances, chassis-integrated modules, and converged network adapters). Cisco Intersight provides a role-based access control (RBAC) policy to control the separation of administrative duties and provide a security log of all changes made.

The TOE includes a single management entity called the Cisco Intersight Virtual Appliance, at least one Fabric component, and one or more UCS servers. Though the minimal TOE deployment could include only one of each of the TOE component types, one Cisco Intersight Virtual Appliance can manage thousands of UCS servers and all the interconnected

[1] When ordering, both UCS M6 and M7 servers offer an S and N version. The only differences are in the internal drive compatibility. More details can be found in the UCS M6 Datasheet page and the UCS M7 Datasheet page.

fabric components. [Note, capacity details are provided for conceptual purposes only as capacity testing is not covered within the scope of the Common Criteria evaluation.]

Cisco Intersight implements Cisco Unified Fabric supporting Ethernet and Fibre Channel protocols over Cisco® Data Center Ethernet and Fibre Channel over Ethernet (FCoE) links with speeds up to 200Gbps. 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.

1.2.2 Supported non-TOE Hardware/ Software/ Firmware

The TOE supports (in some cases optionally) the following hardware, software, and firmware in its environment when the TOE is configured in its evaluated configuration:

Table 3 IT Environment Components

Component	Required	Usage/Purpose Description for TOE performance
Management Workstation with web browser and SSH client	Yes	To support remote administration of the TOE, a remote management workstation must have an SSH client that supports SSHv2 and one of the following supported web browser versions: • Google Chrome 62.0.3202.94 and later • Firefox 57.0.1 and later • Safari 10.1.1 and later • Microsoft Edge (Chromium) Beta and later
Remote Authentication (AAA) Server	No	An LDAPS 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.
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 administrative interfaces of the TOE must be separated from public/untrusted networks by an application-aware firewall such that remote access to the TOE's management interfaces are prohibited from untrusted networks and only allowed from trusted networks.

1.3 TOE Description

This section provides an overview of the Cisco Intersight 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 component types, Server and Fabric component:

- One Cisco Intersight Virtual Appliance
- One or more managed servers with VIC:
  - Cisco UCS X-Series:
    - Chassis: UCSX-9508
    - M6 Compute Nodes (servers): UCSX-210C-M6
      - VIC in M6 compute nodes: UCSX-V4-Q25GME, or UCSX-V4-PCIME
    - M7 Compute Nodes (servers): UCSX-210C-M7, UCSX-410C-M7

      - VIC in M7 compute nodes: UCSX-ME-V5Q50G-D, UCSX-ML-V5Q50G-D, UCSX-ML-V5D200G-D or UCSX-V4-PCIME
  - ➢ Cisco UCS C-Series Servers and Virtual Interface Cards (VIC):
    - ▪ M6 Servers[1]: UCSC-C220-M6, UCSC-C225-M6, UCSC-C240-M6, UCSC-C245-M6
      - VIC for M6 C-Series servers: UCSC-PCIE-C25Q-04, UCSC-PCIE-C100-04, UCSC-P-V5Q50G, UCSC-P-V5D200G, UCSC-M-V25-04, UCSC-M-V5Q50G, UCSC-M-V100-04, UCSC-M-V5D200G
    - ▪ M7 Servers[1]: UCSC-C220-M7, UCSC-C240-M7
      - VIC for M7 C-Series servers: Same as for M6 C-Series servers.
- ❖ One or more managed Fabric components:
  - ➢ Cisco Fabric Interconnect (FI):
    - ▪ UCS-FI-6454, UCS-FI-64108, and/or UCS-FI-6536
  - ➢ Cisco Intelligent Fabric Modules (IFM):
    - ▪ For M6 compute nodes: UCSX-I-9108-25G, UCSX-I-9108-100G
    - ▪ For M7 compute nodes: UCSX-I-9108-25G-D, UCSX-I-9108-100G-D

1.3.1 Intersight Virtual Appliance

The Cisco Intersight Virtual Appliance is the OS and software provided as a Virtual Machine (VM). This is a software-only TOE component installed on VMware ESXi 7.0 or later with VMware vSphere Web Client 7.0 or later. Intersight functions as the central management component of the TOE to allow configuration of all TOE components via the Intersight WebUI. The underlying platform of the VM, which includes the underlying server hardware and the hypervisor, are outside the TOE boundary.

1.3.2 UCS X-Series Components

The Cisco UCS X-Series components of the TOE include a chassis (UCSX-9508) that provides power and cooling for one or more UCS X-Series Compute Nodes, and one or more X-Series network adapters. The UCSX-9508 is 12-inch (7 RU) tall chassis that fits in a standard 19-inch-wide rack. The chassis can house up to eight (8) X-Series compute nodes, each of which will have one Virtual Interface Card (VIC) installed, which will provide network connectivity between the Compute Node and the backplane of the chassis. The chassis also contains up to two (2) Cisco UCS 9108 Intelligent Fabric Modules (IFMs), which connect the chassis to upstream Cisco UCS 6400 Series Fabric Interconnects.

1.3.3 UCS C-Series Servers

Cisco UCS C-Series Servers, also known as Rack Mount Servers, 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.

1.3.4 Virtual Interface Cards (VIC) and other Network Adapters

Several network adapters, including Cisco UCS Virtual Interface Cards (VIC) are compatible with the UCS X-Series and C-Series servers. These VICs are managed by the Intersight and enforce the traffic flow control to and from the UCS servers.

1.3.5 Fabric Interconnects (FI)

The Cisco Fabric Interconnects run in Intersight Managed Mode (IMM) and enforce traffic flow control between UCS and entities outside the TOE boundary. The traffic flow control rules (the 'Fabric') of the TOE are configured via the Intersight component of the TOE.

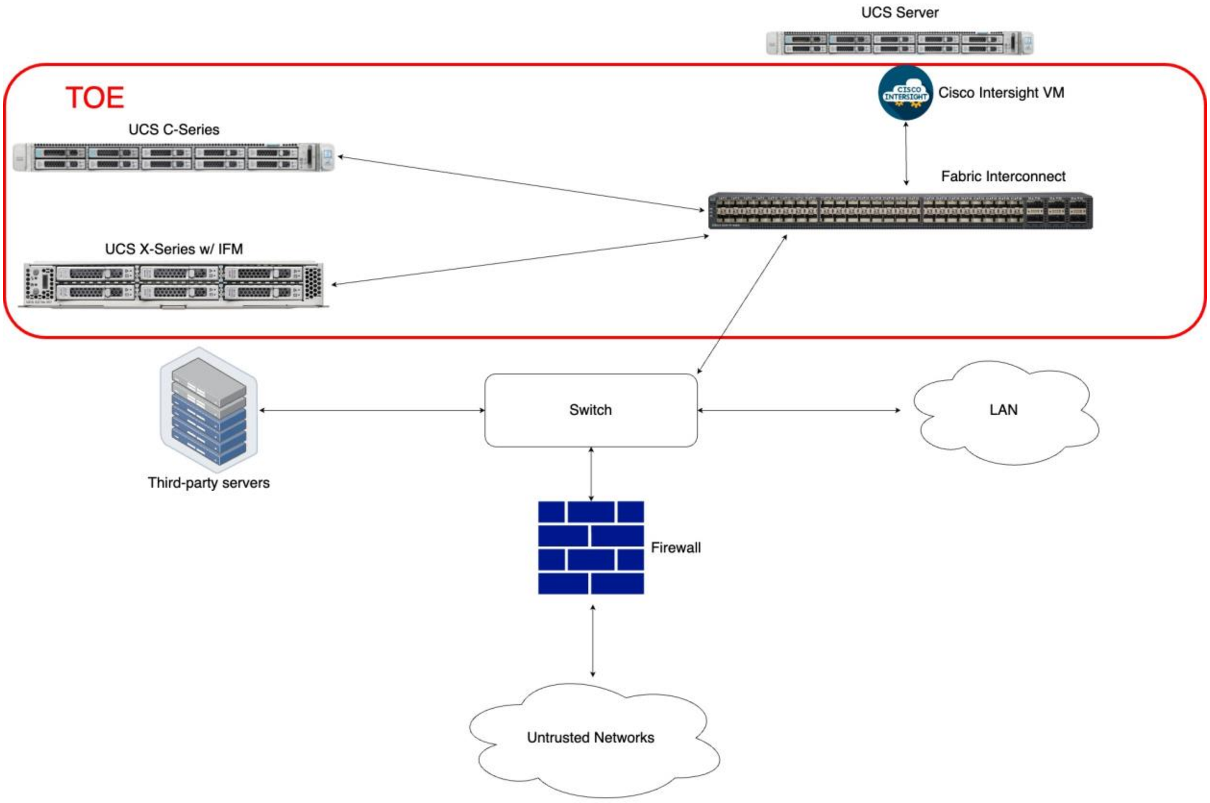
1.3.6 Intelligent Fabric Modules (IFM):

The Intelligent Fabric Modules (IFM) enforce traffic flow control between Fabric Interconnects (FI) and the VIC installed within each UCS server/node.

1.4 TOE Evaluated Configuration

The following figure provides a visual depiction of an example TOE deployment. The TOE boundary includes the TOE components including a firewall to protect the TOE management interfaces from untrusted networks. In this topology, the remote servers, such as LDAPS, syslog, and NTP could be hosted on UCS servers, or third-party rack servers, or across the LAN Core. The TOE boundary does not include any hypervisors and guest operating systems installed to the servers.

Figure 1 Sample Deployment of TOE components with non-TOE components



1.5 Physical Scope of the TOE

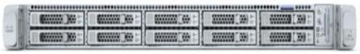
The TOE is a hardware and software solution that makes up the Cisco Intersight Virtual Appliance with IMM Fabric and UCS Servers, and the TOE guidance documentation. The TOE guidance documentation that is considered part of the TOE is the guidance document referenced in Table 2, a PDF document that, along with other PDF-based guidance referenced therein, can be obtained from the https://cisco.com web site.

The TOE hardware platforms are described in Table 4 Hardware Models and Specifications. For ordering of the TOE and delivery via commercial carriers, see https://apps.cisco.com/ccw/cpc/guest/home.

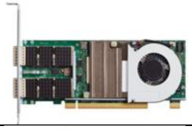
All software and firmware of the TOE is bundled into installation image of the Cisco Intersight Virtual Appliance, which is provided by Cisco as an OVA file downloadable from https://software.Cisco.com. Installation and upgrade of software on each TOE component (FI and UCS servers) is handled through the Cisco Intersight Virtual Appliance.

The TOE is comprised of the following physical specifications as described in Table 4 below:

Table 4 Hardware Models and Specifications

Hardware	Picture	Physical Size	Network Connectivity
X-Series Servers			
UCSX-9508		Height: 12.05 inches (30.6 cm); 7 RU Width: 17.55 inches (44.6 cm) Depth: 34.81 inches (88.4 cm)	Refer to compatible Fabric Modules: UCSX-I-9108-25G, UCSX-I-9108-25G-D, UCSX-I-9108-100G, UCSX-I-9108-100G-D
UCSX-210C-M6		Height: 1.80 in. (45.7 mm) Width: 11.28 in. (286.5 mm) Depth: 23.7 in. (602 mm)	Refer to compatible VICs: UCSX-V4-Q25GME, or UCSX-V4-PCIME
UCSX-210C-M7		Height: 1.80 in. (45.7 mm) Width: 11.28 in. (286.5 mm) Depth: 23.7 in. (602 mm)	Refer to compatible VICs: UCSX-ME-V5Q50G-D, UCSX-ML-V5Q50G-D, UCSX-ML-V5D200G-D, or UCSX-V4-PCIME
UCSX-410C-M7		Height: 3.67 in. (93.22 mm) Width: 11.28 in. (286.52 mm) Depth: 23.8 in. (604.52 mm)	Refer to compatible VICs: UCSX-ME-V5Q50G-D, UCSX-ML-V5Q50G-D, UCSX-ML-V5D200G-D, or UCSX-V4-PCIME
C-Series Rack Servers			
UCSC-C220-M6		Height: 1.70 in. (4.3 cm) Width: 16.9 in. (42.9 cm) Depth: 30 in. (76.2 cm)	Refer to compatible VICs: UCSC-PCIE-C25Q-04, UCSC-PCIE-C100-04, UCSC-P-V5Q50G, UCSC-P-V5D200G, UCSC-M-V100-04, UCSC-M-V25-04, UCSC-M-V5D200G, UCSC-M-V5Q50G,
UCSC-C225-M6		Height: 1.70 in. (4.3 cm) Width: 16.9 in. (42.9 cm) Depth: 30 in. (76.2 cm)	Same as above.
UCSC-C240-M6		Height: 3.42 in. (8.7 cm) Width: 16.9 in. (42.9 cm) Depth: 30 in. (76.2 cm)	Same as above.
UCSC-C245-M6,		Height: 3.42 in. (8.7 cm) Width: 16.9 in. (42.9 cm)	Same as above.

		Depth: 30 in. (76.2 cm)	
UCSC-C220-M7		Height: 1.70 in. (4.3 cm) Width: 16.9 in. (42.9 cm) Depth: 30 in. (76.2 cm)	Same as above.
UCSC-C240-M7		Height: 3.42 in. (8.7 cm) Width: 16.9 in. (42.9 cm) Depth: 30 in. (76.2 cm)	Same as above.
Fabric Interconnects (FI)			
UCS-FI-6454		Height: 1.72 in. (4.4 cm) Width: 17.3 in. (43.9 cm) Depth: 22.5 in. (57.1 cm)	48 x 10/25-Gbps SFP28 ports and 6 x 40/100-Gbps QSFP28 ports
UCS-FI-64108		Height: 3.38 in. (8.33 cm) Width: 17.42 in. (44.25 cm) Depth: 22.95 in. (58.29 cm)	96 x 10/25-Gbps SFP28 ports and 12 x 40/100-Gbps QSFP28 ports
UCS-FI-6536		Height: 3.42 in. (8.7 cm) Width: 16.9 in. (42.9 cm) Depth: 30 in. (76.2 cm)	36 x 10/25/40/100-Gbps and FCoE ports with optional unified ports
Intelligent Fabric Modules (IFM)			
UCSX-I-9108-25G UCSX-I-9108-25G-D		Height: 1.67 inches (4.2 cm) Width: 14.93 inches (37.9 cm) Depth: 11.76 inches (29.9 cm)	8 x 25GbE/FCoE external optical ports, and 32 GbE/FCoE internal ports.
UCSX-I-9108-100G UCSX-I-9108-100G-D		Height: 1.67 inches (4.2 cm) Width: 14.93 inches (37.9 cm) Depth: 11.76 inches (29.9 cm)	8 x 100G or 32 x 25G or a combination of 100G and 25G depending on the VIC 15000/14000 series in the compute node.
Virtual Interface cards			
UCSX-V4-PCIME		Internal.	2 x 16G mezz card for M6 Compute Nodes
UCS VIC 14825 (UCSX-V4-Q25GME)		Internal.	4 x 25G mezz card for M6 Compute Nodes
UCS VIC 15422 (UCSX-ME-V5Q50G-D)		Internal.	4 x 25G mezz card for M7 Compute Nodes

UCS VIC 15420 (UCSX-ML-V5Q50G-D)		Internal.	4 x 25G mLOM for Cisco UCS X210c-M7 Compute Node
UCS VIC 15231 (UCSX-ML-V5D200G-D)		Internal.	2 x 100G mLOM for Cisco UCS X210c M7 Compute Node
UCS VIC 1455 (UCSC-PCIE-C25Q-04)		Internal.	4x10/25-Gbps Ethernet and FCoE SFP28
UCS VIC 1467 (UCSC-M-V25-04)		Internal.	4x10/25-Gbps Ethernet and FCoE SFP28
UCS VIC 1477 (UCSC-M-V100-04)		Internal.	2 x 40/100-Gbps Ethernet and FCoE QSFP28
UCS VIC 1495 (UCSC-PCIE-C100-04)		Internal.	2 x 40/100-Gbps Ethernet and FCoE QSFP28
UCS VIC 15235 (UCSC-P-V5D200G)		Internal.	Dual-port 40/100/200-Gbps PCIe
UCS VIC 15238 (UCSC-M-V5D200G)		Internal.	Dual-port 40/100/200-Gbps mLOM

UCS VIC 15425 (UCSC-P-V5Q50G)		Internal.	Quad-port 10/25/50-Gbps PCIe
UCS VIC 15428 (UCSC-M-V5Q50G)		Internal.	Quad -port 10/25/50-Gbps mLOM

Firmware versions for physical appliance:

Table 5 - Firmware for physical appliances

Device	Firmware
UCSX-210C-M6	intersight-ucs-server-210c-m6. 5.2.0.230127.bin
UCSX-210C-M7	intersight-ucs-server-210c-m7. 5.2.0.230127.bin
UCSX-410C-M7	intersight-ucs-server-410c-m7. 5.2.0.230127.bin
UCSC-C220-M6	intersight-ucs-server-c220-m6.4.3.3.240152.bin
UCSC-C225-M6	intersight-ucs-server-c225-m6.4.3.3.240152.bin
UCSC-C240-M6	intersight-ucs-server-c240-m6.4.3.3.240152.bin
UCSC-C245-M6,	intersight-ucs-server-c245-m6.4.3.3.240152.bin
UCSC-C220-M7	intersight-ucs-server-c220-m7.4.3.3.240152.bin
UCSC-C240-M7	intersight-ucs-server-c220-m7.4.3.3.240152.bin
UCS 6400 Series Fabric Interconnects	ucs-intersight-infra-4gfi.4.3.4.240074.bin
UCS 6500 Series Fabric Interconnects	intersight-ucs-infra-5gfi.4.3.4.240074.bin
Cisco Intersight Virtual Appliance and Assist for vSphere	intersight-appliance-installer-vsphere-1.0.9-630.ova
Cisco Intersight Appliance Software Bundle	Intersight-appliance-bundle-1.0.9-677.bin

Firmware upgrade on UCS servers include updates for all components installed on the UCS servers (VICs, IFMs).

1.6 Logical Scope of the TOE

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

1. Security Audit
2. User Data Protection
3. Identification and Authentication
4. Security Management
5. Protection of the TSF
6. Trusted Path

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

1.6.1 Security Audit

Cisco Intersight stores audit information to assist the administrator in monitoring the security state of the TOE as well as troubleshooting various problems that arise throughout the operation of the system. Intersight may be configured to send records to an external syslog server. The remote audit server is outside the TOE boundary. The TOE provides the ability to audit the actions taken by authorized administrators. Audited events include start-up and shutdown, configuration changes, administrative authentication, and administrative log-off. The TOE provides the capability for authorized administrators to review the audit records stored within the TOE.

1.6.2 User Data Protection

1.6.2.1 Network Separation

1.6.2.1.1 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 Ethernet frames are presented to interfaces within the same VLAN.

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

The FI and VIC hardware requires VLANs to function. When the administrator configures network adapters on a per-server basis, VLANs are specified for each adapter within that server.

1.6.2.2 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 Organizations. A role defines the privileges of a user in the system and the Organization defines the 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 Organizations.

A user is granted write access to desired system resources only if the assigned role grants the access privileges and the assigned Organization 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 Organizations assigned to the user include the Finance organization.

1.6.2.2.1 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 'Account 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 (✔ means the role has access to that function. Blank means no access at all to that function).

Table 6 Privileges and Default Role Assignments

	Default Roles					
Privileges / Permissions	**Account Administrator**	**Read-Only**	**Device Technician**	**Device Administrator**	**User Access Administrator**	**Server Administrator**
Dashboard views	✔	Read-only				✔
Servers Table view	✔	Read-only				✔
HyperFlex Clusters Table view	✔	Read-only				
Fabric Interconnect Table view	✔	Read-only				View details
Storage Table view	✔	Read-only				
Virtualization Table view	✔	Read-only				
Server Profiles	✔	Read-only				Create Server Profiles
Policies	✔	Read-only				Create Server policies
Targets	✔	Read-only	Claim and view target details	Claim, view target details, and delete devices		View target details
Alarms	✔	Read-only				✔
Requests	✔	Read-only	✔	✔		✔
Global Search	✔	Read-only				✔
Settings	✔	View Account Details, generate API keys, and view OAuth Tokens	View Licensing status, Account details, generate API keys, and view OAuth Tokens	View Licensing status, Account details, generate API keys, and view OAuth Tokens	View Sessions, Licensing, Settings, and view OAuth Tokens	View Licensing status, Account details, generate API keys, and view OAuth Tokens
Help	Read-only	Read-only	Read-only	Read-only	Read-only	Read-only
User Profile	✔	Read-only	✔	✔	✔	✔
Cross Launch of Element Managers	✔	Read-only				✔
Audit Logs	✔				✔	

Collect and download Tech Support Bundles	✓					

1.6.2.2.2 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:

- **Account Administrator**—In this role, you can claim targets, cross launch element managers, collect tech support bundles, create profiles and policies, and make configuration changes to the claimed targets or the account.
- **Read-Only**—In this role, you can view details, and status of the claimed targets within the account. However, you cannot make any configuration changes to the claimed targets or the account.
- **Device Technician**—In this role, you can claim a target in Intersight and view a list of the claimed targets in the Targets table view.
- **Device Administrator**—In this role, you can claim a target in Intersight, view a list of the claimed targets, and delete (unclaim) a target.
- **User Access Administrator**—In this role, you can create, edit, and manage user accounts, groups, set up Identity Providers, and Single Sign-On and generate API keys related to this role.
- **Server Administrator**—In this role, you can perform all server actions including firmware upgrade, collect tech support bundles, set server tags, create, edit, and deploy a server profile or policy, and view server details.

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.

1.6.3 Identification and authentication

The TOE supports two methods of authenticating administrator logins to Intersight: a local user database; or a remote authentication server accessed either via LDAPS. Remote authentication may be used to centralize user account management to an external authentication server. The system has a default user account, “admin”, which cannot be modified or deleted. This account is the system administrator account and has full privileges. Each local user account must have a unique username that does not start with a number. For authentication purposes, a password is required for each user account.

1.6.4 Security Management

The TOE can be managed via Intersight via graphical user interface (over TLSv1.2 or TLSv1.3), or command line (over SSHv2) or via virtual console to access Intersight via ESXi). Any of these administrative interfaces can be used in the evaluated configuration of the TOE. 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 the Intersight GUI to perform management tasks for all physical and virtual devices within the TOE.

1.6.4.1 Cisco UCS Hardware Management

An administrator can use Cisco Intersight to manage all hardware within the TOE, including the following:

- UCS X-Series Chassis (not security-relevant to the TSF)
- X-Series and C-Series Servers
- Fabric Interconnects (FI)
- Fans (not security-relevant to the TSF)
- Ports
- Cards / Adapters
- Slots
- I/O modules

1.6.4.2 Cisco UCS Resource Management

An administrator can use Cisco Intersight to create and manage all logical resources within the TOE, 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)

1.6.4.3 Server Administration in a Cisco UCS Instance

A server administrator can use Cisco Intersight to perform server management tasks within the TSF, including the following:

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

1.6.4.4 Network Administration in a Cisco UCS Instance

A network administrator can use Cisco Intersight to perform tasks required to create LAN configuration for any Cisco UCS instance within the TOE, 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

1.6.4.5 Tasks that Cannot be Performed via Cisco Intersight

Cisco Intersight 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 Intersight to manage systems or devices that are outside the TOE. 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 Intersight 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.

1.6.4.6 UCS Secure Access

The TOE provide secure access for remote administration using SSHv2, and TLS1.2 or TLSv1.3. SSHv2 is used to access the command line interface (CLI) and TLS is used to access the WebUI (GUI) via a web browser. SSHv2 authentication uses username and password for authentication.

1.6.5 Protection of the TSF

The TOE internally maintains the date and time. This date and time is used as the timestamp that is applied to audit records generated by the TOE and in validating service requests.

The TOE implements multiple ways to keep the system working as intended in case of failure via the use of redundant paths or using clusters. Clustered connections use dedicated high availability (HA) ports.

The TOE protects all configuration data between FI and UCS using VLAN IDs.

1.6.6 Trusted Path

The TOE allows trusted paths to be established to itself from remote administrators over for CLI access (SSH) or HTTPS for web UI access.

1.7 Excluded Functionality

The following functionality is excluded from the evaluation.

- Stand-alone configuration of the C-Series (Rack Mount) Servers and X-Series Servers are not supported; C-Series servers and X-Series Servers must be managed by Intersight.
- Direct admin interfaces to CIMC (on C-Series, and X-Series servers) are disabled when the servers are integrated to the fabric and managed via Intersight.
- 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.

2 CONFORMANCE CLAIMS

2.1 Common Criteria Conformance Claim

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

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

The claimed assurance package EAL2+ augmented with ALC_FLR.2.

2.2 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.
- Organizational security policies for the TOE as appropriate.

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

3.1 Assumptions

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

Table 7 TOE Assumptions

Assumption	Assumption Definition
A.ADMIN	All authorized administrators are assumed not malicious, will follow TOE administrative guidance, and will not intentionally disrupt the operation of the TOE.
A.BOUNDARY	The TOE 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 TOE components and virtual machines (VM) supporting equipment must have a physical security policy preventing unauthorized physical access. The policy must document physical security controls including access control, physical separation of hardware, and monitoring policies to ensure no unauthorized physical access to TOE components is allowed.
A.POWER	The facility housing the TOE 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 TOE environment providing network connectivity to and from the TOE 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, VM supporting equipment or NTP server communications between the TOE and the remote servers shall be protected.

3.2 Threats

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

Table 8 Threats

Threat Name	Threat Definition
T.NORMAL_USE	A system user (VM user, OS administrator, or Hypervisor administrator) attacks a TOE component 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 a TOE component 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 Cisco Intersight Virtual Appliance 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 TOE resources unknowingly (due to unfamiliarity with the current TOE configuration, or unfamiliarity with TOE administrative guidance) attempts to access or modify attributes of TOE resources 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.

3.3 Organizational Security Policies

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

4 SECURITY OBJECTIVES

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

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

4.1 Security Objectives for the TOE

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

Table 9 Security Objectives for the Environment

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.
O.ADMIN	The TOE must provide a secure channel for administration.

4.2 Security Objectives for the Environment

All of the assumptions stated in Section 3.1 are considered to be security objectives for the environment. The following are the non-IT security objectives, which, in addition to those assumptions, are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 10 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.BOUNDARY	The TOE 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 TOE. 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 TOE is allowed.
OE.POWER	The operational environment of the TOE shall incorporate a power management strategy using UPS or backup generators to ensure that power continues to flow under any adverse conditions.
OE.REDUNDANT_NET	The operational environment of the TOE shall provide redundant network links to protect against network administrator operator error or network equipment failure.
OE.REMOTE_SERVERS	The operational environment of the TOE shall optionally provide remote authentication servers, Syslog servers, and/or NTP servers, and will protect communications between the TOE and the servers.

5 SECURITY REQUIREMENTS

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

5.1 Conventions

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

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

5.2 TOE Security Functional Requirements

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

Table 11 Security Functional Requirements

Functional Component		
Requirement Class	**SFR**	**Component Name**
FAU: Security Audit	FAU_GEN.1	Audit data generation
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
	FAU_STG.1	Protected audit trail storage
	FAU_STG.4	Prevention of audit data loss
FDP: User Data Protection	FDP_ACC.2	Complete access control
	FDP_ACF.1	Security attribute-based access control
	FDP_IFC.1 (1)	Subset information flow control (1)
	FDP_IFF.1 (1)	Simple security attributes (1)
FIA: Identification and authentication	FIA_ATD.1	User attribute definition
	FIA_SOS.1	Verification of secrets
	FIA_UAU.2	Timing of authentication

	FIA_UAU.5	Multiple authentication mechanisms
	FIA_UID.2	User identification before any action
FMT: Security management	FMT_MOF.1	Management of security functions behavior
	FMT_MSA.1 (1)	Management of security attributes (1)
	FMT_MSA.1 (2)	Management of security attributes (2)
	FMT_MSA.3 (1)	Static attribute initialization (1)
	FMT_MSA.3 (2)	Static attribute initialization (2)
	FMT_MTD.1 (1)	Management of TSF data (1)
	FMT_MTD.1 (2)	Management of TSF data (2)
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
FPT: Protection of the TSF	FPT_FLS.1	Failure with preservation of secure state
	FPT_ITT.2	TSF data transfer separation
	FPT_RCV.2	Automated recovery
	FPT_STM.1	Reliable time stamps
FTP: Trusted Path	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 [***not specified***] level of audit; and
c) [**the events listed in Table 12**].

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

a) Date and time of the auditable event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the ST, [**information specified in column three of Table 12**].

Table 12 Auditable Events

Functional Component	Auditable Event	Additional Audit Record Contents
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 any authentication mechanism on the TOE.	
FDP_ACF.1	Role-based access control requests submitted to Intersight.	The user identity requesting the change and the object being accessed.
FPT_STM.1	Attempts to change the time.	The identity of the authorized administrator performing the operation.

Functional Component	Auditable Event	Additional Audit Record Contents
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) **Event**;
b**) User ID;**
c) Client Address
d) Session ID].

FAU_STG.1 Protected audit trail storage

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

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

FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1 The TSF shall [***overwrite the oldest stored audit records***] and [***no other action]*** 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.

5.2.2.1 FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the [**Role-Based Access Control SFP**] to objects based on the following: [

Subject security attributes:

- **Authenticated Administrators:**
  - **User Identity**
  - **Privilege(s) (the cumulative set of privileges obtained from the roles assigned to the Authenticated Administrator)**
  - **Organization(s)**

Object security attributes:

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

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

- **Authenticated Administrators are granted access to Resources in which the assigned Organization for the Authenticated Administrator and the assigned Organization for the Resource are the same.**
- **Authenticated Administrators assigned Organizations that are different from the Organization assigned to the Resources are not granted access.**
- **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.**
- **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 Organization**)].

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: Ethernet frames
Operations: Permit or deny Ethernet communication].

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**].

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: [

a) login id;
b) password;
c) role;
d) organization;]

FIA_SOS.1 Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [**the following metrics by containing:**

- **At least the admin-defined number of characters;**
- **At least the admin-defined number of upper-case letters;**
- **At least the admin-defined number of lower-case letters;**
- **At least the admin-defined number of numeric characters;**
- **At least the admin-defined number of special characters**].

FIA_UAU.2 User authentication before any action

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

FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.5.1 The TSF shall provide [

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

] to support user authentication.

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

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 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 behaviour 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 [***modify,*** [***none***]] the security attributes [**sending and receiving VLAN interface and VLAN ID in frame header specified in VLAN policies**] to [**Account Administrator, Server Administrator, and any custom role holding Server Policies or Policies privilege**].

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

FMT_MSA.1.1(2) 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 [**Account Administrator, User Access Administrator**].

FMT_MSA.3(1) Static attributes 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 [**Account Administrator, Server Administrator, and any custom role holding Server Policies or Policies privilege**] to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3(2) Static attributes initialisation (2)

FMT_MSA.3.1(2) 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(2) The TSF shall allow [**Account Administrator, User Access Administrator**] to specify alternative initial values to override the default values when an object or information is created.

5.2.4.6 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 [**Account Administrator, User Access Administrator**].

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 [**Account Administrator**].

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 [

- **Account Administrator**
- **Read-Only**
- **Device Technician**
- **Device Administrator**
- **User Access Administrator**
- **Server Administrator**
- **custom roles**].

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

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.

5.2.5.2 FPT_ITT.2 TSF data transfer separation

FPT_ITT.2.1 The TSF shall protect TSF data from [***disclosure, modification***] 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 and Servers).

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.

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 [***remote***] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [***modification, disclosure***].

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

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

5.3 TOE SFR Dependencies Rationale for SFRs

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 13 SFR Dependency Rationale

SFR	Dependency	Rationale
FAU_GEN.1	FPT_STM.1	Met by FPT_STM.1
FAU_SAR.1	FAU_GEN.1	Met by FAU_GEN.1
FAU_SAR.3	FAU_SAR.1	Met by FAU_SAR.1
FAU_STG.1	FAU_GEN.1	Met by FAU_GEN.1
FAU_STG.4	FAU_STG.1	Met by FAU_STG.1
FDP_ACC.2	FDP_ACF.1	Met by FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	Met by FDP_ACC.2 Met by FMT_MSA.3
FDP_IFC.1(1)	FDP_IFF.1	Met by FDP_IFF.1(1)
FDP_IFF.1(1)	FDP_IFC.1 FMT_MSA.3	Met by FDP_IFC.1 (1) Met by FMT_MSA.3 (1)
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 Met by FMT_SMF.1N/A
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_ACC.1 Met by FMT_SMR.1 Met by FMT_SMF.1
FMT_MSA.3(1)	FMT_MSA.1 FMT_SMR.1	Met by FMT_SMR.1 Met by FMT_MSA.1(1)
FMT_MSA.3(2)	FMT_MSA.1 FMT_SMR.1	Met by FMT_SMR.1 Met by FMT_MSA.1(2)
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

SFR	Dependency	Rationale
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_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 Security Assurance Requirements

5.4.1 SAR Requirements

The TOE assurance requirements for this ST are EAL2 Augmented with ALC_FLR.2 derived from Common Criteria version 3.1, Revision 5. The assurance requirements are summarized in the table below.

Table 14: 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
	ALC_FLR.2	Flaw reporting 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

5.4.2 Security Assurance Requirements Rationale

This Security Target claims conformance to EAL2 Augmented with ALC_FLR.2. 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 15: 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	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_CMS.2	
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.

Component	How the requirement will be met
ALC_FLR.2	Cisco documents the flaw remediation and reporting procedures so that security flaw reports from TOE users can be appropriately acted upon, and TOE users can understand how to submit security flaw reports to the developer.
ATE_COV.1	The Test document(s) consist of a test plan describes the test configuration, the approach to testing, and how the subsystems/modules and TSFI (TOE security function interfaces) has been tested against its functional specification and design as described in the TOE design and the security architecture description. The test document(s) also include the test cases/procedures that show the test steps and expected results, specify the actions and parameters that were applied to the interfaces, as well as how the expected results should be verified and what they are. Actual results are also included in the set of Test documents.
ATE_FUN.1	
ATE_IND.2	Cisco will provide the TOE for testing.
AVA_VAN.2	Cisco will provide the TOE for testing.

6 TOE SUMMARY SPECIFICATION

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 16 How TOE SFRs Measures

<table>
<tr><th>TOE SFRs</th><th>How the SFR is Met</th></tr>
<tr><td>FAU_GEN.1</td><td>
<b>Intersight:</b>
<p>Shutdown and start-up of the audit functions are logged by events for rebooting TOE components, and the events when TOE components complete POST. Audit is enabled whenever the TOE is on. The TOE also records an audit record whenever the TOE (and audit functionality) is Shutdown.</p>
<p>Intersight 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:</p>
<table>
<tr><td>Dec 15 2023 7:52:56 AM</td><td>User admin@local</td><td>System</td><td>Reason: Incorrect Password</td></tr>
</table>
<p>The auditable events include:</p>
<table>
<tr><th>Auditable Events</th><th>Rationale</th></tr>
<tr><td>Successful modifications to user role assignments and modifications to mappings between roles and privileges.</td><td>Successful modifications to users/roles/privileges are logged in the local audit log. Failed attempts to make such modifications are not logged.</td></tr>
<tr><td>Successful and failed use of the user authentication mechanism.</td><td>All login attempts are logged. Successful and failed attempts are logged to the local audit log, and optionally to a remote syslog server (using syslog in plaintext).</td></tr>
<tr><td>Successful role-based access control requests submitted via the Intersight.</td><td>Successful changes to configuration data is logged to the local admin log.</td></tr>
<tr><td>Successful and failed attempts to change to the time.</td><td>Successful and failed attempts to change the system time and any time-related parameters including time zone or NTP server configuration are logged in the local audit log, and optionally to a remote syslog server. Manual setting of the clock can only be performed via the CLI.</td></tr>
<tr><td>Successful and failed attempts to use the trusted path functions.</td><td>Successful and failed use of SSHv2 is logged only to a remote syslog server.</td></tr>
</table>
</td></tr>
<tr><td>FAU_SAR.1</td><td>Intersight allows all administrative accounts to review the local audit store. These audit records are available to the authorized (authenticated) administrator through the administrative GUI.</td></tr>
<tr><td>FAU_SAR.3</td><td>Intersight stores the events in order by date, by default showing the most recent events at the top. The Intersight GUI allows for sorting and filtering based on: Event, User ID, Client Address and Session ID.</td></tr>
</table>

TOE SFRs	How the SFR is Met
FAU_STG.1	Audit records can be viewed by the authorized administrator via the Intersight GUI. Audit records are stored on Intersight 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 Intersight admin interfaces. The file contents cannot be altered.
FAU_STG.4	When local audit stores become full the oldest audit records will be deleted when new records are written, preserving a continuous audit trail. The TOE supports transmission of audit records to a remote audit server to provide more long-term storage of audit trails.

FDP_IFC.1(1)
and
FDP_IFF.1(1)
	Network interfaces are grouped into VLANs, so Layer 2 broadcast frames will be issued to only interfaces within that VLAN. Ethernet frames will be tagged with a VLAN ID indicating which VLAN they are allowed to access. The TOE will enforce VLAN separation by only allowing fames to traverse ports that match the VLAN ID in the frame header. VLAN traffic will not be forwarded to interfaces not in that VLAN.

FDP_ACC.2 and FDP_ACF.1	The TOE implements an extensive Role-Based Access Control (RBAC) system for administrative access to the TOE. The TOE implements six 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, role assignments, and Organization assignments. The Organization attribute defines system resources that the administrator can access. If a resource is assigned a different Organization 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	Intersight 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, • Role, and • Organization. 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 administratively-configurable requirements, defined as a minimum number of: • At least twelve characters long • At least three of the following: lower case letters, upper case letters, digits, special characters • Must not be identical to the username or reverse username • Does not contain the following symbols: $ (dollar sign), ? (question mark), and = (equals sign) • Does not contain more than three repeating characters, such as aaabbb • Does not contain dictionary words • Should not be blank

TOE SFRs	How the SFR is Met
	This requirement applies to the local password database and on the password selection functions provided by the TOE, but the TOE cannot enforce password complexity requirements for passwords stored on remote AAA (LDAP) servers.
FIA_UID.2 and FIA_UAU.2	By default, Intersight uses its local user 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 GUI.
FIA_UAU.5	Intersight may be configured for local or remote authentication. In the case of local authentication, account passwords are verified against hashes stored the /etc/shadow system file. In the case of remote authentication, user credentials are passed to a remote LDAPS 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.
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)
	The TOE access policies are configured to protect the TOE 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 until roles are explicitly assigned by an authorized administrator.
	The TOE provides the following access to TOE administrative functionality:
	A. Accounts with the privileges associated with the Account Administrator and Server Administrator roles, and any custom role holding Server Policies or Policies privilege have the ability to modify VLAN Policies
	B. 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)
	Restrictive default values are provided for VLANs, and role-based access control.
	No information flows are allowed for traffic (VLAN) unless the traffic the attribute combination of receiving/sending interface and VLAN 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 TOE 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 Account Administrator, User Access Administrator role can modify security attributes (Username, Password, Role, and Organization), with the limitation that the assignment of organizations is restricted to only those in the Organization of the user assigning the organizations. The TOE only allows users with the Account Administrator role to set the TOE time.

FMT_SMF.1	The TOE restricts the ability to enter privileged configuration operations to those users holding the correct privilege from their assigned role(s). The TOE provides the ability manage the operation of the TOE, audit trail, administrative access, administrative users and timestamps. Administrators can configure:

TOE SFRs	How the SFR is Met
	• 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 services (LDAPS). • Timestamps: Manually set the local system time or add/remove one or more NTP servers.
FMT_SMR.1	Table 6 Privileges and Default Role Assignments (ST section 1.6) lists the privileges associated with management capabilities and default roles supported by the TOE. Other privileges exist in Intersight that can be assigned to roles as needed to define custom roles, but the other privileges defined in Intersight 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).
FPT_FLS.1	The TOE can be deployed with redundant network paths, and/or with the Fabric Interconnects in a clustered configuration such that failure of one 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 Intersight, Fabric Interconnects and Servers is protected by use of TLS.
FPT_RCV.2	When a stand-alone Fabric Interconnect (FI) fails, or a cluster of FI fails, the FI can be administered via local console connection 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 TOE 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.

TOE SFRs	How the SFR is Met
FTP_TRP.1	Intersight protect remote command line access to management functions using the SSH protocol for authentication, integrity protection and confidentiality. Intersight protects remote web-based access to management functions using the TLS (TLS1.2 or TLSv1.3) between itself and the web browser used by the remote administrator. Fabric Interconnects protect remote command line access to management functions using the SSH protocol for authentication, integrity protection and confidentiality. Fabric Interconnects protect remote web-based access to management functions using the TLS (TLS1.2 or TLSv1.3) between itself and the web browser used by the administrator.

6.2 TOE Bypass and interference/logical tampering Protection Measures

The TOE consists of a hardware and software solution. The TOE 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 interfaces. The CLI interfaces achieve a trusted path via SSH. The GUI interfaces achieve a trusted path via TLS. There are no undocumented interfaces for managing the product.

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

No processes outside of the TOE 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 TOE provides a secure domain for its operation. Each TOE component has its own resources that other components within the same 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 TOE. Both communication types including data plane communication and, control plane communications are mediated by the TOE. Data plane communication refers to datacentre 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 includes the Cisco Intersight software, IMM software (on the FI), and UCS server firmware on the X-Series and C-Series servers. This software and firmware includes server and client components. All software and firmware components resident within the TOE hardware and is protected by the mechanisms described above.

7 RATIONALE

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

7.1 Rationale for TOE Security Objectives

Table 17 Summary of Mappings between Threats, Policies and the Security Objectives

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

Table 18 Rationale for Mapping of Threats, Policies and the Security Objectives for the TOE

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

Objective	Rationale for Coverage
	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.ADMIN	This security objective counters the threat T.SNIFF by providing a secure channel for administration.

7.2 Rationale for the Security Objectives for the Environment

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

Table 19 Mappings of Assumptions and the Security Objectives for the OE

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

Table 20 Rationale for Mapping of Threats, Policies and Objectives for the OE

Assumptions	Rationale for Coverage of Environmental Objectives
OE.ADMIN	This security objective satisfies A.ADMIN by ensuring that competent and trusted administrators manage the TOE.
OE.BOUNDARY	This security objective satisfies A.BOUNDARY by ensuring that the TOE is separated from public networks by an application aware firewall.
OE.PHYSICAL	This security objective satisfies A.PHYSICAL by ensuring that the TOE is physically protected from unauthorized access.

Assumptions	Rationale for Coverage of Environmental Objectives
OE.POWER	This security objective satisfies A.POWER by ensuring that the TOE has sufficient power to operate.
OE.REDUNDANT_NET	This security objective satisfies A.REDUNDANT_NET by ensuring network availability.
OE.REMOTE_SERVERS	This security objective satisfies A. REMOTE_SERVERS by protecting communications between the TOE and optional remote servers.

7.3 Rationale for requirements/TOE Objectives

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

Table 21 Security Objective to Security Requirements Mappings

SFR	O.IDAUTH	O.ENCRYP	O.AUDREC	O.ACCOUN	O.SECFUN	O.VLANSEC	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		
FDP_ACC.2					X		
FDP_ACF.1					X		
FDP_IFC.1(1)						X	
FDP_IFF.1(1)						X	
FIA_ATD.1	X						
FIA_SOS.1	X						
FIA_UAU.2	X						
FIA_UAU.5	X						
FIA_UID.2	X						
FMT_MOF.1					X		
FMT_MSA.1(1)					X		
FMT_MSA.1(2)					X		
FMT_MSA.3(1)					X		
FMT_MSA.3(2)					X		
FMT_MTD.1(1)					X		
FMT_MTD.1(2)					X		
FMT_SMF.1					X		
FMT_SMR.1					X		
FPT_FLS.1					X		

SFR	O.IDAUTH	O.ENCRYP	O.AUDREC	O.ACCOUN	O.SECFUN	O.VLANSEC	O.ADMIN
FPT_ITT.2					X		X
FPT_RCV.2					X		
FPT_STM.1			X				
FTP_TRP.1		X					X

Table 22 Summary of Mappings between IT Security Objectives and SFRs

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

SFR	Rationale
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_MOF.1	This component ensures that the TSF restrict abilities to determine the behavior of, disable, enable, modify the behavior of functions as defined in FMT_SMF.1to the administrative roles defined in FMT_SMR.1. This component traces back to and aids in meeting the following objectives: O.SECFUN.
FMT_MSA.1(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 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 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.

SFR	Rationale
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_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 ANNEX A: REFERENCES

The following documentation was used to prepare this ST:

Table 23: References

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