Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.6

Security Target

Version: 1.7
Date: March 17, 2023

Table of Contents

Table of Tables

Table of Figures

Document Introduction

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

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.6. 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.

Revision History

Version	Date	Change
0.1	July 15, 2020	Initial Version
0.2	September 11, 2020	Updates in response to OR
0.3	December 11, 2020	Updates in response to OR
0.4	February 1, 2021	Updates in response to additional OR’s
0.5	June 9, 2021	Updates to add DTLS Client
0.6	July 8, 2021	Updates in response to OR
0.7	October 13, 2021	Updates in response to eligibility
0.8	November 2, 2021	Updates in response to ASE package submission
0.9	January 11, 2022	Updates to address certifier OR
1.0	January 27, 2022	Updates to address ORs
1.1	July 7, 2022	Updates to finalize ST
1.2	September 7, 2022	Updates to finalize ST
1.3	November 8, 2022	Updates to finalize ATE Package
1.4	January 12, 2023	Updates to address ATE CBOR4
1.5	February 10, 2023	Updates to address final ORs
1.6	February 14, 2023	Final Updates
1.7	March 17, 2023	Address Final ETR ORs

Security Target Introduction

This Security Target contains the following sections:

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

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

ST and TOE Reference

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

Table 1. ST and TOE Identification

Name	Description
ST Title	Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.6 Security Target
ST Version	1.7
Publication Date	March 17, 2023
Vendor and ST Author	Cisco Systems, Inc.
TOE Reference	Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.6.01

TOE Hardware Models	Cisco 9800-80-K9 Wireless Controller: Cisco 9800-40-K9 Wireless Controller: Cisco 9800-L Wireless Controller: ■ C9800-L-F-K9 ■ C9800-L-C-K9 Cisco Catalyst 9800-CL-K9 Wireless Controller for Private Cloud (vSphere): ■ C9800-CL-K9 Cisco Catalyst 9130 Series Wi-Fi 6 Access Points (x = regulatory domain): ■ C9130AXI-x ■ C9130AXE-x ■ C9130AXE-STA-x Cisco Catalyst 9120 Series Wi-Fi 6 Access Points (x = regulatory domain): ■ C9120AXI-x ■ C9120AXE-x ■ C9120AXP-x Cisco Catalyst 9115 Series Wi-Fi 6 Access Points (x = regulatory domain): ■ C9115AXI-x ■ C9115AXE-x Cisco Catalyst 9105 Series Wi-Fi 6 Access Points (x = regulatory domain): ■ C9105AXI-x ■ C9105AXW-x ■ C9105AXIT-x ■ C9105AXWT-x Cisco Catalyst IW6300 Series Access Points (x = regulatory domain): ■ IW-6300H-AC-X-K9 ■ IW-6300H-DC-X–K9 ■ IW-6300H-DCW-X–K9 Cisco ESW6300 Access Point (x = regulatory domain): ■ ESW-6300-CON-X-K9

	Cisco Aironet 1560 Series Access Points (x = regulatory domain): ■ AIR-AP1562I-x-K9 ■ AIR-AP1562E-x-K9 ■ AIR-AP1562D-x-K9 Cisco Aironet 4800 Access Point (x = regulatory domain): ■ AIR-AP4800-x-K9 ■ AIR-AP4800-x-K9C Cisco Aironet 3800 Series Access Points (x = regulatory domain): ■ AIR-AP3802I-x-K9 ■ AIR-AP3802I-x-K9C ■ AIR-AP3802e-x-K9 ■ AIR-AP3802E-x-K9C ■ AIR-AP3802p-x-K9 ■ AIR-AP3802p-x-K9C Cisco Aironet 2800 Series Access Points (x = regulatory domain): ■ AIR-AP2802I-x-K9 ■ AIR-AP2802I-x-K9C ■ AIR-AP2802E-x-K9 ■ AIR-AP2802E-x-K9C
TOE Software Version	IOS-XE 17.6.01
Keywords	WLAN, Wireless, Access Point

TOE Overview

The TOE combines Wireless LAN Controllers and Access Points to create a WLAN Access System TOE. For wireless clients, the TOE provides secure over-the-air access to an organization's network. For administrator's, the TOE provides central management and administration of the wireless infrastructure within an organization.

TOE Product Type

The TOE is a distributed WLAN network device consisting of at least one Wireless LAN Controller (hereinafter referred to as WLC) and at least one Access Point (hereinafter referred to as AP) to create a WLAN Access System. A WLAN Access System ensures wireless clients are authenticated by a centralized authentication server and provides an encrypted IEEE 802.11 link to protect wireless communications from unauthorized disclosure and/or modification. A WLAN Access System also provides for central management and administration of the wireless infrastructure within an organization.

Required non-TOE Hardware/Software/Firmware

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

Table 2. Required IT Environment Components

Component	Usage/Purpose/Description
Wireless Client	Allows users to establish wireless communications with an organization’s private network through the TOE
EST Server	The EST Server[1] authenticates EST Clients and determines if the EST Client is authorized to receive the certificate it has requested.
Certificate Authority	The Certification Authority is used to provide the TOE, Authentication Server, and Wireless clients with valid certificates. The CA also provides the TOE with a method to check the peer certificate revocation status of devices the TOE communicates with on the wired network. The CA may be adjacent to the EST server or embedded within it.
RADIUS Authentication Server	The purpose of the RADIUS Authentication Server is to authenticate wireless clients using EAP-TLS. FreeRADIUS 3.0.x or higher is required in the IT environment to support RADIUS over TLS (RADsec).
Management Workstation	This includes any IT Environment Management workstation with a TLS web browser client or SSH client installed that is used by the Security Administrator for remote administration over TLS/SSH trusted paths.
Local Console	This includes any IT Environment Console that is directly connected to the Wireless LAN Controller TOE component via the Serial Console Port and is used by the Security Administrator for local TOE administration.
Syslog Server	This includes any syslog server to which the TOE would transmit syslog messages over a trusted channel.
Cisco UCS C-Series M5 Rack Servers (applies only to the Cisco Catalyst 9800-CL Wireless Controller for Private Cloud - vSphere)	Provides the Virtualisation System (VS) including the hypervisor, physical chassis, and supporting software.
DHCP Server (Optional)	Use of a DHCP server allows the AP to automatically discover the IP address of the controller to which it joins.

TOE Description

The Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.6 Target of Evaluation (TOE) provides wireless clients access to resources on an organization's network.

The TOE is comprised of two distinct components:

1. The Access Point (AP) operates at the edge of an organization’s network. The AP contains 2.4 and 5 GHz wireless radios and implements functions from the IEEE 802.11 standard to communicate over-the-air directly to wireless client radios. This

[1] Refer to RFC 7030 for additional information on EST Server

communication includes advertising its presence (known as beacons), responding to requests for available networks (probes), performing 802.11 authentication, association, encryption/decryption, and session management.

2. The Wireless LAN Controller (WLC) is responsible for ensuring wireless clients are authenticated and keys are derived in accordance to the IEEE 802.11 standard.

Refer to Table 3 for a description of the hardware and software compoents that comprise the physical boundary of the TOE.

The TOE uses IEEE 802.1X to ensure Supplicants are authenticated prior to allowing wireless client traffic onto the organization's wired network. Encryption keys for wireless sessions are derived using AES-CCMP for encryption and message integrity with cryptographic key size of 128 bits in accordance with the IEEE 802.11-2012 standard. AES-CCMP-128 bit encryption as specified in 802.11-2012 is more commonly known by its Wi-Fi Alliance certification name, WPA2-Enterprise.

Additionally, the TOE derives wireless encryption keys using AES-CCMP with cryptographic key size of 256 bits and AES-GCMP, with cryptographic key size of 128 and 256 bits in accordance with the IEEE 802.11ac specification.

The WLC is responsible for all management of the APs. Once an AP has registered with the WLC, an internal channel is formed for the purposes of centralized management and configuration of the APs. No local administration is available directly on the APs. The internal channel also protects the distribution of IEEE keys between the WLC and AP.

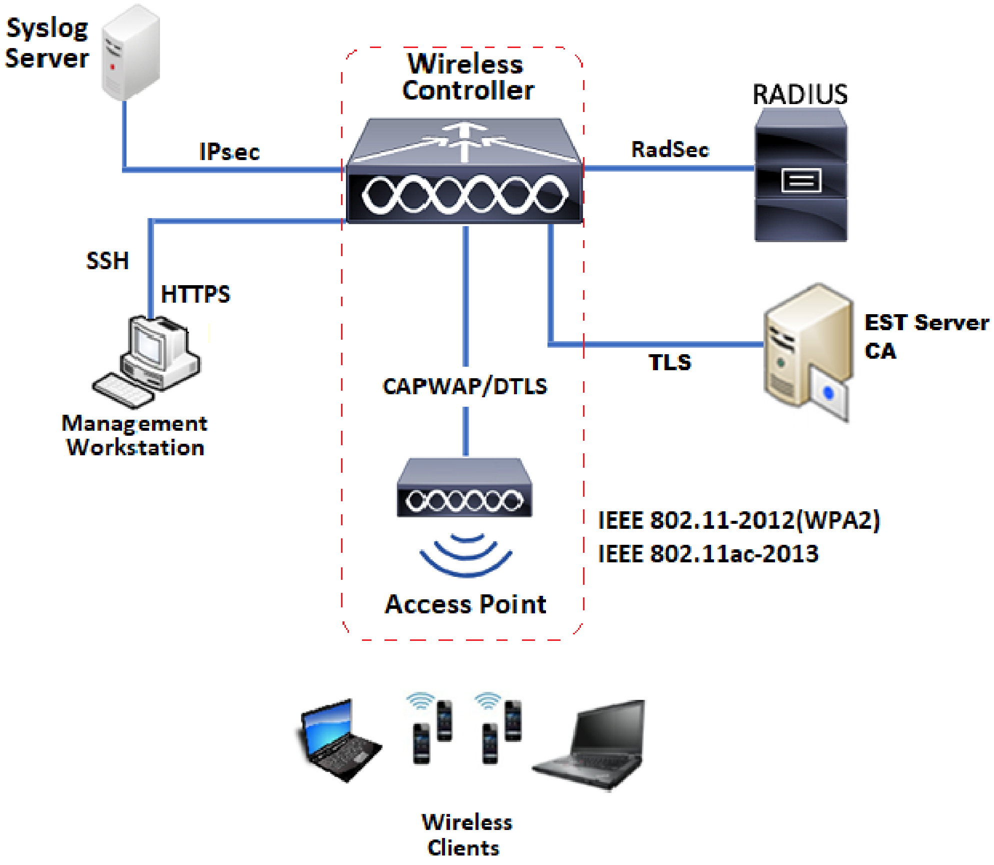
For connections to the Syslog audit server, the WLC authenticates those devices with X.509v3 certificates and protects communication channels with the IPsec protocol. For RADIUS, the WLC protects communication to the RADIUS authentication server with RADsec. Secure remote administration is protected with HTTPS and SSH which is implemented with authentication failure handling.

TOE Evaluated Configuration

The Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.6 TOE is distributed. Deployment of the TOE in its evaluated configuration consists of at least one Wireless LAN Controller (WLC) model and at least one Access Point (AP) model specified in table 3. Extra instances of a WLC or AP TOE component are permitted in the evaluated configuration. The evaluated configuration of Cisco Catalyst 9800-CL (vSphere) follows Use Case 1 in [NDcPP] where a virtual Network Device (vND) runs inside a virtual machine (VM) on purpose-built hardware.

The TOE physical boundary is the WLC and AP components as denoted by hashed red lines in figure 1 below.

Figure 1. TOE and Environment



The WLC can be administered interactively using a local console connection (CLI), or remotely over HTTPS (GUI) or SSH (CLI). Once the APs have registered with a Controller and 'joined' to form the TOE, the APs are entirely managed via the WLC. The TOE does not permit direct local administration of the APs thus fulfilling distributed TOE use case 1 in section 3.1 of [NDcPP].

The operational environment of the TOE will include at least one RADIUS server for authentication of wireless clients. The RADIUS Authentication Server and wireless client (Supplicant) must authenticate each other with EAP-TLS which requires use of X.509 certificates provided by the CA server. The operational environment requires a CA server to provide the TOE, Authentication Server, and Wireless clients with valid X.509 certificates. The environment will also include an audit (syslog) server and a Management Workstation.

The TOE supports two modes of operation, Local mode and Flex Connect mode. In Local mode, the Access Point processes layer 2 wireless frames which are tunneled to the Controller over an internal channel protected with DTLS. In Local mode the WLC is the single point of ingress and egress for both management (TSF data) and user data traffic. When user data traffic reaches the WLC, it is mapped to a corresponding interface (VLAN) or interface group (VLAN pool) defined as part of the WLAN configuration settings on the WLC.

Flex Connect mode is similar to Local mode in that the AP handles functions from the 802.11 specification. The difference with Flex Connect is it allows an option for user data to be distributed at the egress (wired) port of the AP as IEEE 802.3 Ethernet traffic. This mode allows authenticated wireless clients access to resources local to the AP which is particularly useful in small remote and branch offices across WAN links where only a handful of access points are needed. In Flex Connect mode, the WLC is the point of ingress and egress for management traffic (TSF data) only.

Regardless of either mode it may operate in, the AP is always centrally managed by the WLC and management traffic (TSF data) is secured in an internal channel protected with DTLS. Wireless clients are authenticated by a centralized authentication server when the TOE operates in either Local or Flex Connect mode.

Physical Scope of the TOE

The TOE components are Wireless LAN Controllers and Access Points and each is composed of hardware and software. When components are joined, the TOE forms a Wireless LAN Access System.

The TOE is comprised of the following physical specifications:

Table 3. Hardware Models and Specifications

Hardware Platform	Product ID	Specifications
Cisco Catalyst 9800-80 Wireless Controller 	C9800-80-K9	■ Supports up to 6000 access points, 64,000 clients, and up to 80 Gbps throughput ■ Form factor: 2RU ■ Memory: 64GB, DDR4 ■ Storage: 32 GB eUSB, 2x SSD ■ Control plane CPU: Intel Xeon Silver 4116T ■ Ports: ○ 1x RJ-45 console port ○ 1x USB 3.0 console port ○ 2x USB 3.0 ports ○ 1x RJ-45 management port ○ 1x RJ-45 redundancy port ○ 1x SFP Gigabit Ethernet redundancy port ○ Fixed and module uplink ports
Cisco Catalyst 9800-40 Wireless Controller 	C9800-40-K9	■ Supports up to 2000 access points, 32,000 clients, and up to 40 Gbps throughput ■ Form factor: 1 RU ■ Memory: 32GB, DDR4 ■ Storage: 32 GB eUSB ■ Control plane CPU: Intel Xeon Broadwell D-1548 ■ Ports: ○ 1x RJ-45 console port ○ 1x USB 3.0 console port ○ 2x USB 3.0 ports ○ 1x RJ-45 management port ○ 1x RJ-45 redundancy port ○ 1x SFP Gigabit Ethernet redundancy port ○ 4x 10 GE/1 GE SFP+ or SFP ports
Cisco Catalyst 9800-L Wireless Controller 	C9800-L-F-K9 C9800-L-C-K9	■ Available in Fiber or Copper Uplink ■ Supports up to 5000 access points, 10,000 clients, and up to 10 Gbps throughput. ■ Form factor: 1 RU ■ Memory: 16GB, DDR4 ■ Storage: 32 GB eUSB ■ CPU: Intel Xeon Broadwell D-1563N ■ Ports: ○ 1x RJ-45 management port ○ 1x RJ-45 redundancy port ○ 4x RJ-45 2.5 GE AP ports ○ 1x USB 3.0 console port ○ 1x USB 2.0 Micro-B port ○ 1x RJ-45 console port
Cisco Catalyst 9800-CL Wireless Controller for Private Cloud (vSphere)	C9800-CL-K9	The Cisco Catalyst 9800-CL for Private Cloud (vSphere) is a wireless controllers for VMware ESXi 6.x running on one (1) of following Cisco UCS C-Series M5 Rack Servers in the IT environment:

		 ■ UCSC-C220-M5 ■ UCSC-C240-M5 ■ UCSC-C480-M5 The specifications of VMware ESXi 6.x is dependent on the desired scale and sizing: ■ **Small**: Designed for distributed branches and small campuses supporting up to 1000 Access Points (APs) and 10,000 clients: ○ Minimum Number of vCPUs: 4 ○ Minimum Memory (GB): 8GB ○ Required Storage (GB): 8GB ○ Minimum vNICs: 2 ■ **Medium**: Designed for medium-sized campuses supporting up to 3000 APs and 32,000 clients: ○ Minimum Number of vCPUs: 6 ○ Minimum Memory (GB): 16GB ○ Required Storage (GB): 8GB ○ Minimum vNICs: 2 ■ **Large**: Designed for large enterprises and service providers supporting up to 6000 APs and 64,000 clients: ○ Minimum Number of vCPUs: 10 ○ Minimum Memory (GB): 32GB ○ Required Storage (GB): 8GB ○ Minimum vNICs: 2 The specifications of the UCSC-C220-M5 and UCSC-C240-M5 are: ■ Form factor: 1 RU (C220-M5); 2 RU (C240-M5) ■ Memory: Up to 24 DDR4 DIMMs ■ Ports: ○ 1x RJ-45 console port ○ 2x USB 3.0 ports ○ 1x RJ-45 management port ○ 2x 10GTbase-T ports ○ VGA connector

		○ One KVM console connector (supplies two USB 2.0 connectors, one VGA DB15 video connector, and one serial port (RS232) RJ45 connector) ■ CPU: Intel Xeon Skylake SP (Skylake microarchitecture)[2] The specifications of the UCSC-C480-M5 is: ■ Form factor: 4 RU ■ Memory: Up to 48 DDR4 DIMMs ■ Ports: ○ 1x RJ-45 console port ○ 3x USB 3.0 ports ○ 1x RJ-45 management port ○ 2x 10GTbase-T ports ○ VGA connector ○ Serial port (RS232) ■ CPU: Intel Xeon Skylake SP (Skylake microarchitecture)[2]
Cisco Catalyst 9130 Series Wi-Fi 6 Access Points 	C9130AXI-x[3] C9130AXE-x C9130AXE-STA-x	■ Four radios: ○ 2.4 GHz (4x4), 5 GHz (8x8 and 4x4) ■ Integrated Bluetooth Low Energy (BLE) radio ■ Flexible Radio Assignment (FRA) - allows the access point to intelligently determine the operating mode of serving radios based on the RF environment and traffic demands. ■ Cisco RF Application-Specific Integrated Circuit (ASIC) - a fully integrated Software-Defined Radio (SDR) that can perform advanced RF spectrum analysis and delivers features such as Cisco CleanAir®, Wireless Intrusion Prevention System (WIPS), and Dynamic Frequency Selection (DFS) detection. ■ CPU: Qualcomm IPQ8078 ARMv8 ■ Interfaces: ○ 1x100/1000/2500 Multigigabit Ethernet (RJ-45) ○ RS-232 Console Interface through RJ-45 ○ Recovery push button (enables partial or full system configuration recovery) ○ USB 2.0 Port
Cisco Catalyst 9120 Series Wi-Fi 6 Access Points 	C9120AXI-x C9120AXE-x C9120AXP-x	■ Four radios: ○ A dual band radio with 2.4 GHz (peak gain 4dBi) and 4x4 5 GHz (peak gain 5dBi), ○ A single band 5 GHz (peak gain 5dBi), ○ An omni IoT radio 2.4 GHz (peak gain 3dBi) that can be used with BLE, Zigbee, Thread and other multi-protocol 802.15.4 devices, ○ An auxiliary radio with 2.4 GHz (peak gain 3dBi) and 5 GHz (peak gain 5dBi)\ ■ Integrated Bluetooth Low Energy (BLE) radio ■ Integrated internal antennas, omni directional in azimuth for both 2.4 GHz and 5 GHz ■ CPU: Broadcom BCM49408 ARMv8 ■ Interfaces: ○ 1x100/1000/2500 Multigigabit Ethernet (RJ-45)

[2] The specific CPU used in the CC tested configuration was Intel Xeon Platinum 8160M (Skylake) Linux 5 w/ ESXi 6.7

[3] x = regulatory domain

		○ RS-232 Console Interface through RJ-45 ○ Recovery push button (enables partial or full system configuration recovery) ○ USB 2.0 Port ■ Memory: 2048 MB DRAM, 1024 MB flash
Cisco Catalyst 9115 Series Wi-Fi 6 Access Points 	C9115AXI-x C9115AXE-x	■ Two radios: ○ One 2.4 GHz radio ○ One 5 GHz radio ■ External antennas on the 9115AXE access point model ■ Integrated internal antennas, omni directional in azimuth for both 2.4 GHz (peak gain 3dBi) and 5 GHz (peak gain 4dBi) ■ Memory: 2048 MB DRAM, 1024 MB flash ■ CPU: Broadcom BCM49408 ARMv8 CPU ■ Interfaces: ○ 1x100/1000/2500 Multigigabit Ethernet (RJ-45) ○ RS-232 Console Interface through RJ-45 ○ Recovery push button ○ USB 2.0 Port
Cisco Catalyst 9105 Series Wi-Fi 6 Access Points 	C9105AXI-x C9105AXW-x C9105AXIT-x C9105AXWT-x	■ Two radios: ○ One 2.4 GHz radio ○ One 5 GHz radio ■ Integrated internal antennas ■ CPU: Broadcom BCM47622 ARMv7 CPU ■ Interfaces (C9105AXI): ○ 1x10/100/1000 Base-T (Ethernet) Uplink ○ Management console port (RJ-45) ■ Interfaces (C9105AXW): ○ 1x 100/1000/2500 Base-T (Ethernet) Uplink ○ 3x 10/100/1000 Base-T (Ethernet) Downlink ○ Management console port (RJ-45) ○ USB 2.0 ○ Passthru Port
Cisco Catalyst IW6300 Series Access Points 	IW-6300H-AC-X-K9 IW-6300H-DC-X–K9 IW-6300H-DCW-X–K9	■ Two radios: ○ One 2.4 GHz radio ○ One 5 GHz radio ■ Four Type N antenna connectors for 2.4 GHz radio and 5 GHz 802.11ac radio ■ Ethernet Connectors ○ One 100/1000M SFP for WAN ○ One 10/100/1000M RJ45 for WAN (UPoE or PoE+ in) ○ Two 10/100/1000M RJ45 for LAN (802.3at or 802.3af out) ■ CPU: Marvell Armada 390 88F6920 ARMv7, Radio Chipset 88W8964C

Cisco ESW6300 Access Point 	ESW-6300-CON-X-K9	■ Two radios: ○ 2.4 GHz: 802.11b/g/n, 2x2 MIMO, 2 spatial streams ○ 5 GHz: 802.11a/n/ac, 2x2 MIMO, 2 spatial streams ■ CPU: Marvell Armada 390 88F6920 ARMv7, Radio Chipset 88W8964C
Cisco Aironet 1562 Series Access Points 	AIR-AP1562I-x-K9 AIR-AP1562E-x-K9 AIR-AP1562D-x-K9	○ Two radios: ○ One 2.4 GHz radio ○ One 5 GHz radio ○ 4 External antenna ports on the 1562E access point model ○ 3 Integrated dual-band semi-omnidirectional antennas radome on the 1562I modle, 7 dBi (2.4 GHz), 4 dBi (5 GHz) ○ 2 Integrated dual-band directional antennas radome, on the 1562D model, 9 dBi (2.4 GHz), 10 dBi (5 GHz) ○ CPU: Marvell Armada 390 88F6920 ARMv7, Radio Chipset 88W8964C ○ Interfaces: ○ WAN port 10/100/1000BASE-TEthernet, autosensing (RJ-45), PoE in ○ SFP port (fiber or electrical) ○ Management console port (RJ-45)
Cisco Aironet 4800 Access Point 	AIR-AP4800-x-K9 AIR-AP4800-x-K9C	■ Three radios, One 2.4 GHz/5 GHz flexible radio, one 5 GHz radio, and one special analytics radio. ■ Integrated Bluetooth Low Energy (BLE) radio ■ 25 integrated antennas that perform the following functions: ○ Four dual band 2.4/5 GHz (macro-cell) antennas for wide are client coverage ○ Four single band 5 GHz (micro-cell) antennas for High Density and dual 5 GHz client coverage ○ One Bluetooth antenna used for beaconing ○ One 16 element antenna array (dual and single band antennas) used for WLAN analytics, client location, Wireless Security Monitoring, and Hyperlocation ■ CPU: Marvell Armada 390 88F6920 ARMv7, Radio Chipset 88W8964C ■ Memory: 1024 MB DRAM, 256 MB flash ■ Interfaces: ○ 2 Ethernet ports ○ 100/1000/2500/5000 Multigigabit Ethernet (RJ-45) – IEEE 802.3bz ○ Category 5e cabling ○ Higher-quality 10GBASE-T (Category 6/6a) cabling ○ 100/1000BASE-T autosensing (RJ-45 AUX port)

		○ Management console port (RJ-45)
Cisco Aironet 3800 Series Access Points 	AIR-AP3802I-x-K9 AIR-AP3802I-x-K9C AIR-AP3802e-x-K9 AIR-AP3802E-x-K9C AIR-AP3802p-x-K9 AIR-AP3802p-x-K9C	■ Two radios, one dedicated 5 GHz radio and a flexible radio that can be configured as a 2.4 GHz radio (default) or as an additional 5 GHz radio. ■ Antennas: ○ The 3802I has 12 cross polarized internal antennas. ○ The 3802E and P models are configured with up to four external dual-band dipole antennas ■ CPU: Marvell Armada 390 88F6920 ARMv7, Radio Chipset 88W8964C ■ Memory: 1024 MB DRAM, 256 MB flash ■ Interfaces: ○ 2 Ethernet ports ○ 100/1000/2500/5000 Multigigabit Ethernet (RJ-45) – IEEE 802.3bz ○ Category 5e cabling ○ Higher-quality 10GBASE-T (Category 6/6a) cabling ○ 100/1000BASE-T autosensing (RJ-45 AUX port) ○ Management console port (RJ-45)
Cisco Aironet 2800 Series Access Points 	AIR-AP2802I-x-K9 AIR-AP2802I-x-K9C AIR-AP2802E-x-K9 AIR-AP2802E-x-K9C	■ Two radios, one dedicated 5 GHz radio and a flexible radio that can be configured as a 2.4 GHz radio (default) or as an additional 5 GHz radio. ■ Antennas: ○ The 3802I has 12 cross polarized internal antennas. ○ The 3802E and P models are configured with up to four external dual-band dipole antennas ■ CPU: Marvell Armada 390 88F6920 ARMv7, Radio Chipset 88W8964C ■ Memory: 1024 MB DRAM, 256 MB flash ■ Interfaces: ○ 2x100/1000BASE-T autosensing (RJ-45 AUX port) ○ Management console port (RJ-45) ○ USB 2.0

The TOE includes the following software available for download on Cisco Software Central at https://software.cisco.com/. Use your Cisco Care Online (CCO) or SMART account to download the software in a binary image format.

Table 4. TOE Software

Platform	Image
Cisco Catalyst 9800-L	C9800-L-universalk9_wlc.17.6.01.SPA.bin
Cisco Catalyst 9800-40	C9800-40-universalk9_wlc.17.6.01.SPA.bin
Cisco Catalyst 9800-80	C9800-80-universalk9_wlc.17.6.01.SPA.bin
Cisco Catalyst 9800 Wireless Controller for Private Cloud - VMware ESXi	C9800-CL-universalk9.17.6.01.ova

The AP software images v17.6.01 are embedded in each WLC v17.06.01 image and are not separately downloaded and installed.

The TOE includes the following Administrative Guidance documentation available for download in PDF format.

Table 5. Administrative Guidance Documentation

#	Title	Link
1	Cisco Catalyst 9800-L Wireless Controller Hardware Installation Guide	https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/9800-L/installation-guide/b-wlc-ig-9800-L.html
2	Cisco Catalyst 9800-40 Wireless Controller Hardware Installation Guide	https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/9800-40/installation-guide/b-wlc-ig-9800-40.html
3	Cisco Catalyst 9800-80 Wireless Controller Hardware Installation Guide	https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/9800-80/installation-guide/b-wlc-ig-9800-80.html
4	Cisco Catalyst 9800-CL Cloud Wireless Controller Installation Guide	https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/9800-cloud/installation/b-c9800-cl-install-guide.html
5	Cisco Catalyst C9800-CL Wireless Controller Virtual Deployment Guide	https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-8/b_c9800_wireless_controller_virtual_dg.html
6	Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide	https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-6/config-guide/b_wl_17_6_cg.html
7	Cisco Catalyst 9800 Wireless Controller Series Deployment Guide	https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-8/b_cisco_catalyst_9800_wireless_controller_series_dg.html
8	Cisco Catalyst 9800 Wireless Controller Series Web UI Deployment Guide	https://www.cisco.com/c/dam/en/us/td/docs/wireless/controller/9800/17-4/deployment-guide/c9800-webui-dg.pdf
9	Understanding Catalyst 9800 Wireless Controllers Configuration Model	https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213911-understand-catalyst-9800-wireless-contro.html
10	Understand FlexConnect on Catalyst 9800 Wireless Controller	https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213945-understand-flexconnect-on-9800-wireless.html
11	C9800 Radio Resource Management Deployment Guide	https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-8/b_C9800_rrm_dg.html
12	Security Configuration Guide, Cisco IOS XE Gibraltar 17.4.x	https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/17-4/configuration_guide/sec/b_174_sec_9500_cg.html
13	Cisco Catalyst 9800 Series Wireless Controller Command Reference, Cisco IOS XE Bengaluru 17.6.x	https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-6/cmd-ref/b_wl_17_6_cr.html
14	Cisco Catalyst 9130AX Series Access Point Getting Started Guide	https://www.cisco.com/c/en/us/td/docs/wireless/access_point/9130ax/quick/guide/ap9130ax-getstart.html
15	Cisco Catalyst 9120AX Series Access Point Getting Started Guide	https://www.cisco.com/c/en/us/td/docs/wireless/access_point/9120ax/quick/guide/ap9120ax-getstart.html

#	Title	Link
16	Cisco Catalyst 9115AX Series Access Point Getting Started Guide	https://www.cisco.com/c/en/us/td/docs/wireless/access_point/9115ax/quick/guide/ap9115ax-getstart.html
17	Cisco Catalyst 9105AX Series Access Point Getting Started Guide	https://www.cisco.com/c/en/us/td/docs/wireless/access_point/9105ax/quick/guide/ap9105axi-getstart.html
18	Cisco Catalyst IW6300 Heavy Duty Series Access Point Hardware Installation Guide	https://www.cisco.com/c/en/us/td/docs/wireless/outdoor_industrial/iw6300/hardware/install/guide/b_iw6300_hig.html
19	Cisco ESW6300 Embedded Services Access Point	https://www.cisco.com/c/en/us/products/collateral/wireless/6300-series-embedded-services-access-points/guide-c07-742909.html
20	Cisco Aironet 1560 Series Outdoor Access Point Hardware Installation Guide	https://www.cisco.com/c/en/us/td/docs/wireless/access_point/1560/installation/guide/1560hig.html
21	Getting Started Guide - Cisco Aironet 2800 Series Access Points	https://www.cisco.com/c/en/us/td/docs/wireless/access_point/2800/quick/guide/ap2800iegetstart.html
22	Getting Started Guide - Cisco Aironet 3800 Series Access Points	https://www.cisco.com/c/en/us/td/docs/wireless/access_point/3800/quick/guide/ap3800iepgetstart.html
23	Cisco Aironet Series 2800/3800 Access Point Deployment Guide	https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-3/b_cisco_aironet_series_2800_3800_access_point_deployment_guide.html
24	Cisco Aironet 4800 Series Access Points Getting Started Guide	https://www.cisco.com/c/en/us/td/docs/wireless/access_point/4800/quick/guide/ap4800getstart.html
25	Cisco Aironet Series 4800 Access Point Deployment Guide	https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-7/b_cisco_aiironet_series_4800_acces_point_deployment_guide.html
26	Cisco Catalyst 9130 Series Access Point Deployment Guide	https://www.cisco.com/c/dam/en/us/td/docs/wireless/controller/9800/17-3/deployment-guide/c9130-ap-dg.pdf
27	Security for VPNs with IPsec Configuration Guide, Cisco IOS XE 17	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnips/configuration/xe-17/sec-sec-for-vpns-w-ipsec-xe-17-book.html
28	Release Notes for Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE Bengaluru 17.6.x	https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-6/release-notes/rn-17-6-9800.html
29	Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.6, CC Configuration Guide, v0.8 February 10, 2023	https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/common-criteria.html

Logical Scope of the TOE

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

- Security Audit
- Communication

- Cryptographic Support
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channels

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

Security Audit

Auditing allows Security Administrators to discover intentional and unintentional issues with the TOE's configuration and/or operation. Auditing of administrative activities provides information that may be used to hasten corrective action should the system be configured incorrectly. Security audit data can also provide an indication of failure of critical portions of the TOE (e.g. a communication channel failure or anomalous activity (e.g. establishment of an administrative session at a suspicious time, repeated failures to establish sessions or authenticate to the TOE) of a suspicious nature.

The TOE provides extensive capabilities to generate audit data targeted at detecting such activity. The TOE generates an audit record for each auditable event. Each security relevant audit event has the date, timestamp, event description, and subject identity. The AP transmits its audit messages to the WLC where they are stored along with the WLC's own audit messages in a circular audit trail configurable by the Security Administrator. All audit logs are transmitted to an external audit server over a trusted channel protected with IPsec.

Communication

The TOE provides a secure internal channel, under control of the Security Administrator, for Access Points to register and join the WLC to form a distributed TOE.

Cryptographic Support

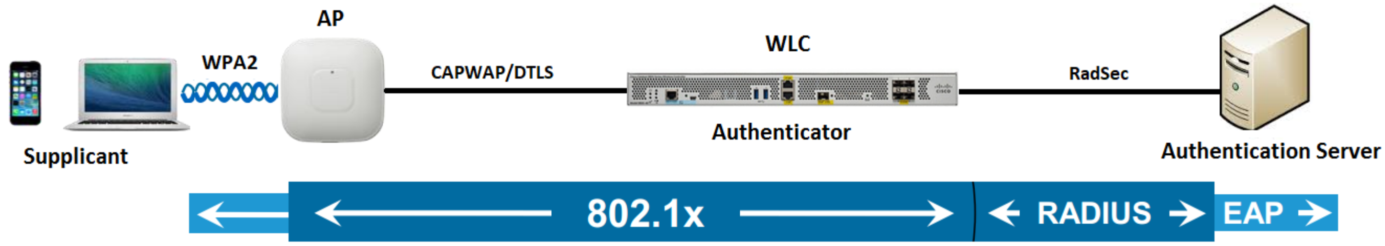
The TOE provides cryptographic functions in order to implement HTTPS, DTLS, SSH, IPsec, WPA2, and IEEE 802.11ac-2013 protocols. The cryptographic algorithm implementation has been validated for CAVP conformance. This includes key generation and random bit generation, key establishment methods, key destruction, and the various types of cryptographic operations to provide AES encryption/decryption, signature verification, hash generation, and keyed hash generation. All cryptography is implemented using the IOS Common Cryptographic Module (IC2M) and CiscoSSL FOM cryptographic modules. IC2M applies to the WLC and CiscoSSL FOM applies the WLC and the AP. Refer to Table 23 for identification of the relevant CAVP certificates.

In addition the IEEE 802.11 implementation has been validated by the Wi-Fi Alliance for WPA2 certification. Refer to Table 22 for identification of the relevant Wi-Fi Alliance certificates.

Identification and Authentication

The TOE facilitates authentication of wireless clients by performing the role of Authenticator in an 802.1X authentication exchange.

Figure 2. TOE's role as 802.1X Authenticator



During the 802.1X authentication exchange, the wireless client software responsible for authentication (hereinafter referred to as a Supplicant) is relayed through the WLC. The 802.1X frames carry EAP authentication packets which are passed through to the RADIUS Authentication Server. The TOE creates a virtual port for each wireless client that is attempting access and blocks access until the RADIUS server returns an authentication success message and 802.11 wireless encryption keys are derived and installed on both the Supplicant and AP. After that point 802.11 wireless data frames from the wireless client are allowed to pass as 802.3 Ethernet frames on the network.

The TOE provides two types of authentication to provide a trusted means for Security Administrators and remote endpoints to interact with a WLAN Access System: X.509v3 certificate-based authentication for remote devices and password-based authentication for Security Administrators. Device-level authentication allows the TOE to establish a secure communication channel with remote endpoints.

Security Administrators have the ability to compose strong passwords (between 8 and 16 characters) which are stored in an obscured form. Additionally, the TOE detects and tracks successive unsuccessful remote authentication attempts and will prevent the offending account from making further attempts until a Security Administrator defined threshold is reached.

Security Management

The TOE provides secure remote administrative interface and local interface to perform security management functions. This includes ability to configure cryptographic functionality; an access banner containing an advisory notice and consent warning message; a session inactivity timer before session termination as well as an ability to update TOE software.

The APs are managed via the WLC. Direct local administration of the APs is not supported.

The TOE provides a Security Administrator role and only the Security Administrator can perform the above security management functions. The TOE prevents attempts to perform remote administration from a wireless client.

Protection of the TSF

The TOE protects critical security data including keys and passwords against tampering by untrusted subjects. The TOE provides reliable timestamps to support monitoring local and remote interactive administrative sessions for inactivity, validating X.509 certificates (to determine if a certificate has expired), denying session establishment of wireless clients (based on time), and to support accurate audit records.

The TOE provides self-tests to ensure it is operating correctly, including the ability to detect software integrity failures. Additionally, the TOE provides an ability to perform software updates and to verify those software updates are from Cisco Systems, Inc.

TOE Access

The TOE monitors both local and remote admin sessions for inactivity and terminates when a threshold time period is reached. Once a session has been terminated the TOE requires the user to re-authenticate.

The TOE is capable of denying wireless client session establishment based on time, day, and WLAN SSID.

The TOE also displays a Security Administrator specified advisory notice and consent warning message prior to initiating identification and authentication for each administrative user.

Trusted Path/Channels

The TOE provides encryption (protection from disclosure and detection of modification) for communication paths between itself and remote endpoints.

In addition, the TOE provides two-way authentication of each endpoint in a cryptographically secure manner, meaning that even if there was a malicious attacker between the two endpoints, any attempt to represent themselves to either endpoint of the communications path as the other communicating party would be detected.

Excluded Functionality

The functionality listed below is not included in the evaluated configuration.

Table 6. Excluded Functionality and Rationale

Function Excluded	Rationale
Non-FIPS 140-2 and CC mode of operation	The TOE includes FIPS and CC modes of operation. The FIPS modes allows the TOE to use only approved cryptography and CC mode removes the ability to use non-PFS ciphersuites for DTLS. FIPS and CC modes of operation must be enabled in order for the TOE to be operating in its evaluated configuration.
WPA and WPA2 with TKIP encryption	Only WPA2-Enterprise along with 802.1X with AES encryption will meet the requirements of the WLAN AS EP.
Cisco Catalyst 9800-CL for public cloud	The Cisco Catalyst 9800-CL for public cloud is an Infrastructure-as-a-Service (IaaS) solution available on the Amazon Web Services (AWS) and Google Cloud Platform (GCP) Marketplace. The Cisco Catalyst 9800-CL for public cloud solution is excluded from the evaluation.
Cisco CleanAir	Cisco CleanAir is a spectrum intelligence solution designed to proactively manage the challenges of a shared wireless spectrum.

Additionally, the TOE includes a number of functions where there are no Security Functional Requirements that apply from the collaborative Protection Profile for Network Devices v2.2e or the WLAN Access System Extended Package v1.0. The excluded functionality does not affect the TOE's conformance to the claimed Protection Profiles.

Conformance Claims

Common Criteria Conformance Claim

The TOE and ST are compliant with the Common Criteria (CC) Version 3.1, Revision 5, dated: April 2017. The TOE and ST are CC Part 2 extended and CC Part 3 conformant.

Protection Profile Conformance Claim

The TOE and ST are exact conformant with the following Protection Profiles

Table 7. Protection Profile Conformance

Protection Profile	Version	Date
collaborative Protection Profile for Network Devices [NDcPP]	2.2e	March 23, 2020
Wireless Local Area Network (WLAN) Access Systems Extended Package [WLAN_EP]	1.0	May 29, 2015

This ST applies the following NIAP Technical Decisions:

Table 8. NIAP Technical Decisions

Number	Title	PP	Applicable	Exclusion Rational
TD0670	NIT Technical Decision for Mutual and Non-Mutual Auth TLSC Testing	[NDcPP]	Yes	
TD0639	NIT Technical Decision for Clarification for NTP MAC Keys	[NDcPP]	Yes	
TD0638	NIT Technical Decision for Key Pair Generation for Authentication	[NDcPP]	Yes	
TD0636	NIT Technical Decision for Clarification of Public Key User Authentication for SSH	[NDcPP]	No	The TOE does not claim FCS_SSHC_EXT.1
TD0635	NIT Technical Decision for TLS Server and Key Agreement Parameters	[NDcPP]	Yes	
TD0634	NIT Technical Decision for Clarification required for testing IPv6	[NDcPP]	Yes	
TD0633	NIT Technical Decision for IPsec IKE/SA Lifetimes Tolerance	[NDcPP]	Yes	
TD0632	NIT Technical Decision for Consistency with Time Data for vNDs	[NDcPP]	Yes	
TD0631	NIT Technical Decision for Clarification of public key authentication for SSH Server	[NDcPP]	Yes	
TD0592	NIT Technical Decision for Local Storage of Audit Records	[NDcPP]	Yes	
TD0591	NIT Technical Decision for Virtual TOEs and hypervisors	[NDcPP]	Yes	
TD0581	NIT Technical Decision for Elliptic curve-based key establishment and NIST SP 800-56Arev3	[NDcPP]	Yes	
TD0580	NIT Technical Decision for clarification about use of DH14 in NDcPPv2.2e	[NDcPP]	Yes	
TD0572	NiT Technical Decision for Restricting FTP_ITC.1 to only IP address identifiers	[NDcPP]	Yes	

Number	Title	PP	Applicable	Exclusion Rational
TD0571	NiT Technical Decision for Guidance on how to handle FIA_AFL.1	[NDcPP]	Yes	
TD0570	NiT Technical Decision for Clarification about FIA_AFL.1	[NDcPP]	Yes	
TD0569	NIT Technical Decision for Session ID Usage Conflict in FCS_DTLSS_EXT.1.7	[NDcPP]	Yes	
TD0564	NiT Technical Decision for Vulnerability Analysis Search Criteria	[NDcPP]	Yes	
TD0563	NiT Technical Decision for Clarification of audit date information	[NDcPP]	Yes	
TD0556	NIT Technical Decision for RFC 5077 question	[NDcPP]	Yes	
TD0555	NIT Technical Decision for RFC Reference incorrect in TLSS Test	[NDcPP]	Yes	
TD0547	NIT Technical Decision for Clarification on developer disclosure of AVA_VAN	[NDcPP]	Yes	
TD0546	NIT Technical Decision for DTLS - clarification of Application Note 63	[NDcPP]	Yes	
TD0538	NIT Technical Decision for Outdated link to allowed-with list	[NDcPP]	Yes	
TD0537	NIT Technical Decision for Incorrect reference to FCS_TLSC_EXT.2.3	[NDcPP]	Yes	
TD0536	NIT Technical Decision for Update Verification Inconsistency	[NDcPP]	Yes	
TD0528	NIT Technical Decision for Missing EAs for FCS_NTP_EXT.1.4	[NDcPP]	No	FCS_NTP_EXT.1 is not claimed.
TD0527	Updates to Certificate Revocation Testing (FIA_X509_EXT.1)	[NDcPP]	Yes	
TD0566	Pre-Shared Keys	[WLAN_EP]	Yes	
TD0559	Modes for AES Data Encryption/Decryption	[WLAN_EP]	Yes	
TD0456	Removal of Low-level Crypto Failure Audit in WLAN AS EP	[WLAN_EP]	Yes	
TD0315	Clarification of test for FCS_CKM.2.1(3)	[WLAN_EP]	Yes	
TD0282	Test Activities added for Key Distribution and Key Generation	[WLAN_EP]	Yes	
TD0271	RADsec as alternative to IPsec	[WLAN_EP]	Yes	

Protection Profile Conformance Claim Rationale

TOE Appropriateness

The TOE provides all of the functionality at a level of security commensurate with that identified in the U.S. Government Protection Profiles.

TOE Security Problem Definition Consistency

The Assumptions, Threats, and Organization Security Policies included in the Security Target represent the Assumptions, Threats, and Organization Security Policies specified in [NDcPP] and [WLAN_EP] for which conformance is claimed verbatim. All concepts covered in the Protection Profile Security Problem Definition are included in the Security Target Statement of Security Objectives Consistency.

The Security Objectives included in the Security Target represent the Security Objectives specified in [NDcPP] and [WLAN_EP] for which conformance is claimed verbatim. All concepts covered in the Protection Profile's Statement of Security Objectives are included in the Security Target.

Statement of Security Requirements Consistency

The Security Functional Requirements included in the Security Target represent the Security Functional Requirements specified in [NDcPP] and [WLAN_EP] for which conformance is claimed verbatim. All concepts covered the Protection Profile's Statement of Security Requirements are included in the Security Target. Additionally, the Security Assurance Requirements included in the Security Target are identical to the Security Assurance Requirements included in the claimed Protection Profiles.

Security Problem Definition

This section identifies the following:

- Assumptions about the TOE's operational 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.
- Threats addressed by the TOE and the IT Environment.
- Organizational Security Policies imposed by an organization on the TOE to address its security needs.

The security problem definition below has been drawn verbatim from [NDcPP] and [WLAN_EP].

Assumptions

Table 9. TOE Assumptions

Assumption	Assumption Definition
A.PHYSICAL_PROTECTION	The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. For vNDs, this assumption applies to the physical platform on which the VM runs.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/ services that could be deemed as general purpose computing. For example the device should not provide computing platform for general purpose applications (unrelated to networking functionality). If a virtual TOE evaluated as a pND, following Case 2 vNDs as specified in Section 1.2, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of a distributed TOE run inside more than one virtual machine (VM) on a single VS. In Case 2 vND, no non-TOE guest VMs are allowed on the platform.
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs for particular types of Network Devices (e.g., firewall).

A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
A.REGULAR_UPDATES	The Network Device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside.
A.COMPONENTS_RUNNING (applies to distributed TOEs only)	For distributed TOEs it is assumed that the availability of all TOE components is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. It is also assumed that in addition to the availability of all components it is also checked as appropriate that the audit functionality is running properly on all TOE components.
A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.
A.VS_TRUSTED_ADMINISTRATOR (applies to vNDs only)	The Security Administrators for the VS are assumed to be trusted and to act in the best interest of security for the organization. This includes not interfering with the correct operation of the device. The Network Device is not expected to be capable of defending against a malicious VS Administrator that actively works to bypass or compromise the security of the device.
A.VS_REGULAR_UPDATES (applies to vNDs only)	The VS software is assumed to be updated by the VS Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.VS_ISOLATON (applies to vNDs only)	For vNDs, it is assumed that the VS provides, and is configured to provide sufficient isolation between software running in VMs on the same physical platform. Furthermore, it is assumed that the VS adequately protects itself from software running inside VMs on the same physical platform.

A.VS_CORRECT_CONFIGURATION (applies to vNDs only)	For vNDs, it is assumed that the VS and VMs are correctly configured to support ND functionality implemented in VMs.
A.CONNECTIONS	It is assumed that the TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.

Threats

Table 10. Threats

Threat	Threat Definition
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	Threat agents may attempt to gain Administrator access to the Network Device by nefarious means such as masquerading as an Administrator to the device, masquerading as the device to an Administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between Network Devices. Successfully gaining administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.
T.WEAK_CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
T.UNTRUSTED_COMMUNICATION_CHANNELS	Threat agents may attempt to target Network Devices that do not use standardized secure tunneling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the Network Device itself.
T.WEAK_AUTHENTICATION_ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g., shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the Network Device itself could be compromised.

T.UPDATE_COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
T.UNDETECTED_ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the Network Device without Administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the Administrator would have no knowledge that the device has been compromised.
T.SECURITY_FUNCTIONALITY_COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the Network Device and its critical data. The compromise of credentials include replacing existing credentials with an attacker’s credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker.
T.PASSWORD_CRACKING	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other Network Devices.
T.SECURITY_FUNCTIONALITY_FAILURE	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.
T.NETWORK_DISCLOSURE	Sensitive information on a protected network might be disclosed resulting from ingress- or egress-based actions
T.NETWORK_ACCESS	Unauthorized access may be achieved to services on a protected network from outside that network.
T.TSF_FAILURE	Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
T.DATA_INTEGRITY	A malicious party attempts to change the data being sent - resulting in loss of integrity.
T.REPLAY_ATTACK	If malicious or external IT entities are able to gain access to the network, they may have the ability to capture information traversing throughout the network and send them on to the intended receiver.

Organizational Security Policies

Table 11. Organizational Security Policies

Policy Name	Policy Definition

P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

Security Objectives

This section 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.

Security Objectives for the TOE

The following table identifies the Security Objectives for the TOE. These security objectives reflect the stated intent to counter identified threats and/or comply with any security policies. The security objectives below have been drawn verbatim from [NDcPP] and [WLAN_EP].

Table 12. Security Objectives for the TOE

Environment Security Objective	TOE Security Objective Definition
O.CRYPTOGRAPHIC_FUNCTIONS	The TOE will provide means to encrypt and decrypt data as a means to maintain confidentiality and allow for detection and modification of TSF data that is transmitted outside of the TOE.
O.AUTHENTICATION	The TOE will provide a means to authenticate the user to ensure they are communicating with an authorized external IT entity.
O.FAIL_SECURE	Upon a self-test failure, the TOE will shutdown to ensure data cannot be passed while not adhering to the security policies configured by the administrator.
O.SYSTEM_MONITORING	The TOE will provide a means to audit events specific to WLAN functionality and security.
O.TOE_ADMINISTRATION	The TOE will provide the functions necessary to address failed authentication attempts by a remote administrator.

Security Objectives for the Environment

The following table identifies the Security Objectives for the Environment. These security objectives reflect the stated intent to counter identified threats and/or comply with any security policies. The security objectives below have been drawn verbatim from [NDcPP] and [WLAN_EP].

Table 13. Security Objectives for the Environment

Environment Security Objective	IT Environment Security Objective Definition
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE. Note: For vNDs the TOE includes only the contents of the its own VM, and does not include other VMs or the VS.
OE.NO_THRU_TRAFFIC_PROTECTION	The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.

OE.TRUSTED_ADMIN	Security Administrators are trusted to follow and apply all guidance in a trusted manner. For vNDs, this includes the VS Administrator responsible for configuring the VMs that implement ND functionality. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are assumed to monitor the revocation status of all certificates in the TOE's trust store and to remove any certificate from the TOE's trust store in case such certificate can no longer be trusted.
OE.UPDATES	The TOE firmware and software is updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
OE.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.
OE.COMPONENTS_RUNNING (applies to distributed TOEs only)	For distributed TOEs the Security Administrator ensures that the availability of every TOE component is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. The Security Administrator also ensures that it is checked as appropriate for every TOE component that the audit functionality is running properly.
OE.RESIDUAL_INFORMATION	The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment. For vNDs, this applies when the physical platform on which the VM runs is removed from its operational environment.
OE.VM_CONFIGURATION (applies to vNDs only)	For vNDs, the Security Administrator ensures that the VS and VMs are configured to ■ reduce the attack surface of VMs as much as possible while supporting ND functionality (e.g., remove unnecessary virtual hardware, turn off unused inter-VM communications mechanisms), and ■ correctly implement ND functionality (e.g., ensure virtual networking is properly configured to support network traffic, management channels, and audit reporting). The VS should be operated in a manner that reduces the likelihood that vND operations are adversely affected by virtualisation features such as cloning, save/restore, suspend/resume, and live migration. If possible, the VS should be configured to make use of features that leverage the VS's privileged position to provide additional security functionality. Such features could include malware detection through VM introspection, measured VM boot, or VM snapshot for forensic analysis.

OE.CONNECTIONS	TOE administrators will ensure that the TOE is installed in a manner that will allow the TOE to effectively enforce its policies on network traffic flowing among attached networks.

Security Requirements

This section identifies the Security Functional Requirements for the TOE. The Security Functional Requirements in this section are drawn from [CC_PART2], [NDcPP], [WLAN_EP], and NIAP Technical Decisions.

Conventions

[CC_PART1] defines operations on Security Functional Requirements. This document uses the following conventions to identify the operations permitted by [NDcPP], [WLAN_EP] and NIAP Technical Decisions.

Table 14. Security Requirement Conventions

Convention	Indication
Assignment	Indicated with *italicized* text
Refinement	Indicated with **bold** text and ~~strikethroughs~~
Selection	Indicated with underlined text
Assignment within a Selection	Indicated with *italicized and underlined* text
Iteration	indicated by adding a string starting with '/' (e.g. 'FCS_COP.1/Hash')

Where operations were completed in the [NDcPP] itself, the formatting used in the [NDcPP] has been retained. Formatting used in [NDcPP] and [WLAN] that is inconsistent with the listed conventions has not been retained in the ST.

The TOE Security Functional Requirements are identified in the following table are described in more detail in the following subsections.

Table 15. Security Functional Requirements

Class Name	Component Identification	Component Name	Drawn From
FAU: Security Audit	FAU_GEN.1	Audit data generation	[NDcPP], [WLAN_EP]
	FAU_GEN.2	User Identity Association	[NDcPP]
	FAU_GEN_EXT.1	Security Audit Generation	[NDcPP]
	FAU_STG.1	Protected Audit Trail Storage	[NDcPP]
	FAU_STG_EXT.1	Protected Audit Event Storage	[NDcPP]
	FAU_STG_EXT.4	Protected Local Audit Event Storage for Distributed TOEs	[NDcPP]
	FAU_STG_EXT.5	Protected Remote Audit Event Storage for Distributed TOEs	[NDcPP]

Class Name	Component Identification	Component Name	Drawn From
FCO: Communication	FCO_CPC_EXT.1	Component Registration Channel Definition	[NDcPP]
FCS: Cryptographic Support	FCS_CKM.1/KeyGen	Cryptographic Key Generation	[NDcPP]
	FCS_CKM.2/KeyEst	Cryptographic Key Establishment (Refined)	[NDcPP]
	FCS_CKM.1/WPA2	Cryptographic Key Generation (Symmetric Keys for WPA2 Connections)	[WLAN_EP]
	FCS_CKM.2/PMK	Cryptographic Key Distribution (PMK)	[WLAN_EP]
	FCS_CKM.2/GTK	Cryptographic Key Distribution (GTK)	[WLAN_EP]
	FCS_CKM.2/PTK	Cryptographic Key Distribution	[WLAN_EP]
	FCS_CKM.4	Cryptographic Key Destruction	[NDcPP]
	FCS_COP.1/DataEncryption	Cryptographic Operation (AES Data Encryption/Decryption)	[NDcPP], [WLAN_EP]
	FCS_COP.1/SigGen	Cryptographic Operation (Signature Generation and Verification)	[NDcPP]
	FCS_COP.1/Hash	Cryptographic Operation (Hash Algorithm)	[NDcPP]
	FCS_COP.1/KeyedHash	Cryptographic Operation (Keyed Hash Algorithm)	[NDcPP]
	FCS_RBG_EXT.1	Random Bit Generation	[NDcPP]
	FCS_IPSEC_EXT.1	IPsec Protocol	[NDcPP]
	FCS_SSHS_EXT.1	SSH Server Protocol	[NDcPP]
	FCS_RADSEC_EXT.1	RADsec	[WLAN_EP]
	FCS_TLSC_EXT.1/RADsec	TLS Client Protocol Without Mutual Authentication	[NDcPP]
	FCS_TLSC_EXT.1/EST	TLS Client Protocol Without Mutual Authentication	[NDcPP]
	FCS_TLSC_EXT.2	TLS Client Support for Mutual Authentication	[NDcPP]
	FCS_DTLSS_EXT.1	DTLS Server Protocol without Mutual Authentication	[NDcPP]
	FCS_DTLSC_EXT.1	DTLS Client Protocol without Mutual Authentication	[NDcPP]

Class Name	Component Identification	Component Name	Drawn From
	FCS_HTTPS_EXT.1	HTTPS Protocol	[NDcPP]
	FCS_TLSS_EXT.1	TLS Server Protocol	[NDcPP]
FIA: Identification and authentication	FIA_AFL.1	Authentication Failure Management	[NDcPP]
	FIA_PMG_EXT.1	Password Management	[NDcPP]
	FIA_PSK_EXT.1	Extended: Pre-Shared Key Composition	[WLAN_EP]
	FIA_UIA_EXT.1	User Identification and Authentication	[NDcPP]
	FIA_UAU_EXT.2	Password-based Authentication Mechanism	[NDcPP]
	FIA_UAU.6	Re-authenticating	[WLAN_EP]
	FIA_UAU.7	Protected Authentication Feedback	[NDcPP]
	FIA_8021X_EXT.1	Extended: 802.1X Port Access Entity (Authenticator) Authentication	[WLAN_EP]
	FIA_X509_EXT.1/Rev	X.509 Certificate Validation	[NDcPP]
	FIA_X509_EXT.1/ITT	X.509 Certificate Validation	[NDcPP]
	FIA_X509_EXT.2	X.509 Certificate Authentication	[NDcPP]
	FIA_X509_EXT.3	X.509 Certificate Requests	[NDcPP]
FMT: Security management	FMT_MOF.1/ManualUpdate	Management of security functions behaviour	[NDcPP]
	FMT_MOF.1/Services	Management of security functions behaviour	[NDcPP]
	FMT_MOF.1/Functions	Management of security functions behaviour	[NDcPP]
	FMT_MTD.1/CoreData	Management of TSF Data	[NDcPP]
	FMT_MTD.1/CryptoKeys	Management of TSF Data	[NDcPP]
	FMT_SMF.1	Specification of Management Functions	[NDcPP]
	FMT_SMR.1	Security Management Roles	[WLAN_EP]
	FMT_SMR.2	Restrictions on Security Roles	[NDcPP]

Class Name	Component Identification	Component Name	Drawn From
FPT: Protection of the TSF	FPT_SKP_EXT.1	Extended: Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)	[NDcPP]
	FPT_APW_EXT.1	Extended: Protection of Administrator Passwords	[NDcPP]
	FPT_FLS.1	Failure with preservation of secure state	[WLAN_EP]
	FPT_ITT.1	Basic Internal TSF Data Transfer Protection	[NDcPP]
	FPT_STM_EXT.1	Reliable Time Stamps	[NDcPP]
	FPT_TUD_EXT.1	Trusted update	[NDcPP]
	FPT_TST_EXT.1	TSF Testing (Extended)	[NDcPP], [WLAN_EP]
FTA: TOE Access	FTA_SSL_EXT.1	TSF-initiated Session Locking	[NDcPP]
	FTA_SSL.3	TSF-initiated Termination	[NDcPP]
	FTA_SSL.4	User-initiated Termination	[NDcPP]
	FTA_TAB.1	Default TOE Access Banners	[NDcPP]
	FTA_TSE.1	TOE Session Establishment	[WLAN_EP]
FTP: Trusted path/channels	FTP_ITC.1	Inter-TSF trusted channel	[NDcPP], [WLAN_EP]
	FTP_TRP.1/Admin	Trusted Path	[NDcPP]

Class: 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) All administrator actions comprising:

- *Administrative login and logout (name of user account shall be logged if individual user accounts are required for Administrators).*
- *Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).*
- *Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).*
- *Resetting passwords (name of related user account shall be logged).*

- *[Starting and stopping services]*;

d) Specifically defined auditable events listed in Table 16.

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the cPP/ST, [*information specified in column three of Table 16*].

Table 16. Auditable Events

SFR	Auditable Event	Additional Audit Record Contents
FAU_GEN.1	None.	None.
FAU_GEN.2	None.	None.
FAU_GEN_EXT.1	None.	None.
FAU_STG.1	None.	None.
FAU_STG_EXT.1	None.	None.
FAU_STG_EXT.4	None.	None.
FAU_STG_EXT.5	None.	None.
FCO_CPC_EXT.1	Enabling communications between a pair of components. Disabling communications between a pair of components.	Identities of the endpoints pairs enabled or disabled.
FCS_CKM.1/KeyGen	None.	None.
FCS_CKM.1/WPA2	None.	None.
FCS_CKM.2/KeyEst	None.	None.
FCS_CKM.2/PMK	None.	None.
FCS_CKM.2/GTK	None.	None.
FCS_CKM.2/PTK	None.	None.
FCS_CKM.4	None.	None.
FCS_COP.1/DataEncryption	None.	None.
FCS_COP.1/SigGen	None.	None.
FCS_COP.1/Hash	None.	None.
FCS_COP.1/KeyedHash	None.	None.
FCS_RBG_EXT.1	None.	None.

SFR	Auditable Event	Additional Audit Record Contents
FCS_IPSEC_EXT.1	Failure to establish an IPsec SA. Protocol failures. Establishment/Termination of an IPsec SA. Negotiation "down" from an IKEv2 to IKEv1 exchange.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.
FCS_RADSEC_EXT.1	None.	None.
FCS_TLSC_EXT.1/RADsec	Failure to establish an TLS session	Reason for failure.
FCS_TLSC_EXT.1/EST	Failure to establish an TLS session	Reason for failure.
FCS_TLSC_EXT.2	None.	None.
FCS_DTLSS_EXT.1	Failure to establish a DTLS session	Reason for failure
	Detected replay attacks	Identity (e.g., source IP address) of the source of the replay attack.
FCS_DTLSC_EXT.1	Failure to establish a DTLS session	Reason for failure
FCS_SSHS_EXT.1	Failure to establish an SSH session	Reason for failure.
FCS_HTTPS_EXT.1	Failure to establish an HTTPS session.	Reason for failure.
FCS_TLSS_EXT.1	Failure to establish an TLS session	Reason for failure.
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded. The reaching of the threshold for the unsuccessful authentication attempts and the actions taken (e.g., disabling of an account) and the subsequent, if appropriate, restoration to the normal state (e.g., re-enabling of a terminal).	Origin of the attempt (e.g., IP address).
FIA_PMG_EXT.1	None.	None.
FIA_PSK_EXT.1	None.	None.
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU_EXT.2	All use of the identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.6	Attempts to re-authenticate	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	None.
FIA_8021X_EXT.1	Attempts to access to the 802.1X controlled port prior to successful completion of the authentication exchange.	Provided client identity (MAC address).

SFR	Auditable Event	Additional Audit Record Contents
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate Any addition, replacement or removal of trust anchors in the TOE's trust store.	Reason for failure of certificate validation Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store.
FIA_X509_EXT.1/ITT	Unsuccessful attempt to validate a certificate Any addition, replacement or removal of trust anchors in the TOE's trust store.	Reason for failure of certificate validation Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store.
FIA_X509_EXT.2	None.	None.
FIA_X509_EXT.3	None.	None.
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	None.
FMT_MOF.1/Services	None.	None.
FMT_MOF.1/Functions	None.	None.
FMT_MTD.1/CoreData	None.	None.
FMT_MTD.1/CryptoKeys	None.	None.
FMT_SMF.1	All management activities of TSF data.	None.
FMT_SMR.1	None.	None.
FMT_SMR.2	None.	None.
FPT_SKP_EXT.1	None.	None.
FPT_APW_EXT.1	None.	None.
FPT_FLS.1	Failure of the TSF.	Indication that the TSF has failed with the type of failure that occurred.
FPT_ITT.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process.	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).
FPT_TST_EXT.1	Execution of this set of TSF-self-tests. Detected integrity violations.	For integrity violations, the TSF code file that caused the integrity violation.
FPT_TUD_EXT.1	Initiation of update. result of the update attempt (success or failure)	None.
FTA_SSL_EXT.1	The termination of a local session by the session locking mechanism.	None.

SFR	Auditable Event	Additional Audit Record Contents
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.
FTA_SSL.4	The termination of an interactive session.	None.
FTA_TAB.1	None.	None.
FTA_TSE.1	Denial of a session establishment due to the session establishment mechanism.	Reason for denial, origin of establishment attempt.
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions. Failed attempts to establish a trusted channel (including IEEE 802.11). Detection of modification of channel data.	Identification of the initiator and target of failed trusted channels establishment attempt. Identification of the initiator and target of channel.
FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failures of the trusted path functions.	None.

FAU_GEN.2 – User Identity Association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FAU_GEN_EXT.1 – Security Audit Generation

FAU_GEN_EXT.1.1 The TSF shall be able to generate audit records for each TOE component. The audit records generated by the TSF of each TOE component shall include the subset of security relevant audit events which can occur on the TOE component.

FAU_STG.1 – Protected Audit Trail Storage

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

FAU_STG.1.2 The TSF shall be able to prevent unauthorised modifications to the stored audit records in the audit trail.

FAU_STG_EXT.1 – Protected Audit Event Storage

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to an external IT entity using a trusted channel according to FTP_ITC.1.

FAU_STG_EXT.1.2 The TSF shall be able to store generated audit data on the TOE itself. In addition [

- The TOE shall be a distributed TOE that stores audit data on the following TOE components: [*WLC*],
- The TOE shall be a distributed TOE with storage of audit data provided externally for the following TOE components: [*the AP transmits its generated audit data to the WLC for storage*].

]

FAU_STG_EXT.1.3 The TSF shall [overwrite previous audit records according to the following rule: [*oldest audit records are overwritten*]] when the local storage space for audit data is full.

FAU_STG_EXT.4 – Protected Local Audit Event Storage for Distributed TOEs

FAU_STG_EXT.4.1 The TSF of each TOE component which stores security audit data locally shall perform the following actions when the local storage space for audit data is full: [*action as defined in Table 17 according to the following:* [*overwrite previous audit records according to the following rule:* [*oldest audit records are overwritten first*]]].

Table 17. TOE Component Storing Audit Data Locally

TOE Component	Action When Storage Space Is Full
WLC	Overwrite

FAU_STG_EXT.5 – Protected Remote Audit Event Storage for Distributed TOEs

FAU_STG_EXT.5.1 Each TOE component which does not store security audit data locally shall be able to buffer security audit data locally until it has been transferred to another TOE component that stores or forwards it. All transfer of audit records between TOE components shall use a protected channel according to [FPT_ITT.1].

Class: Communication Partner Control (FCO)

FCO_CPC_EXT.1 – Component Registration Channel Definition

FCO_CPC_EXT.1.1 The TSF shall require a Security Administrator to enable communications between any pair of TOE components before such communication can take place.

FCO_CPC_EXT.1.2 The TSF shall implement a registration process in which components establish and use a communications channel that uses [*A channel that meets the secure channel requirements in FPT_ITT.1*] for at least TSF data.

FCO_CPC_EXT.1.3 The TSF shall enable a Security Administrator to disable communications between any pair of TOE components.

Class: Cryptographic Support (FCS)

FCS_CKM.1/KeyGen – Cryptographic Key Generation

FCS_CKM.1.1/KeyGen Refinement: The TSF shall generate **asymmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm: [

- RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.3;
- ECC schemes using ‘NIST curves’ [P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.4;
- FFC schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.1

] ~~and specified cryptographic key sizes [assignment: *cryptographic key sizes]* that meet the following: [assignment: *list of standards*~~].

FCS_CKM.2/KeyEst – Cryptographic Key Establishment (Refinement)

FCS_CKM.2.1/KeyEst The TSF shall **perform** cryptographic **key establishment** in accordance with a specified cryptographic key **establishment** method: [

- RSA-based key establishment schemes that meet the following: RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 3447, “Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1”;

- Elliptic curve-based key establishment schemes that meets the following: NIST Special Publication 800-56A Revision 2, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”;

- Finite field-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 2, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”;

] ~~that meets the following: [assignment: *list of standards*]~~.

FCS_CKM.1/WPA2 – Cryptographic Key Generation (Symmetric Keys for WPA2 Connections)

FCS_CKM.1.1/WPA2 Refinement: The TSF shall generate **symmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm **[*PRF-384*] and** [PRF-704] and specified cryptographic key sizes [**128 bits**] **and** [256 bits] **using a Random Bit Generator as specified in FCS_RBG_EXT.1** that meet the following: **[IEEE 802.11-2012] and** [IEEE 802.11ac-2014].

FCS_CKM.2/PMK – Cryptographic Key Distribution (PMK)

FCS_CKM.2.1/PMK Refinement: The TSF shall **receive the 802.11 Pairwise Master Key (PMK)** in accordance with a specified cryptographic key distribution method: [***from the 802.1X Authorization Server***] that meets the following: [***IEEE 802.11-2012***] **and does not expose the cryptographic keys.**

FCS_CKM.2/GTK – Cryptographic Key Distribution (GTK)

FCS_CKM.2.1/GTK Refinement: The TSF shall distribute **Group Temporal Key (GTK)** in accordance with a specified cryptographic key distribution method: [**AES Key Wrap in an EAPOL-Key frame**] that meets the following: [**NIST SP 800-38F, IEEE 802.11-2012 for the packet format and timing considerations**] **and does not expose the cryptographic keys**.

FCS_CKM.2/PTK – Cryptographic Key Distribution

FCS_CKM.2.1/PTK Refinement: The TSF shall distribute **the IEEE 802.11 keys** in accordance with a specified cryptographic key distribution method: [**FPT_ITT**] that meets the following: [**FCS_COP security strength] and does not expose the cryptographic keys**.

Application Note: This requirement refers to the PTK derived by the WLC (Authenticator) and distributed to the AP.

FCS_CKM.4 – Cryptographic Key Destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method

- *For plaintext keys in volatile storage, the destruction shall be executed by a* [single overwrite consisting of [zeroes, a new value of the key]]*;*

- *For plaintext keys in non-volatile storage, the destruction shall be executed by the invocation of an interface provided by a part of the TSF that* [
    - logically addresses the storage location of the key and performs a [single-pass]overwrite consisting of [zeroes, a new value of the key]]*;*

that meets the following: *No Standard.*

FCS_COP.1/DataEncryption – Cryptographic Operation (AES Data Encryption/Decryption)

FCS_COP.1.1/DataEncryption Refinement: The TSF shall perform encryption/decryption in accordance with a specified cryptographic algorithm AES used in **CBC, CCMP**, and [GCM, **GCMP**] **modes** and cryptographic key sizes **128 bits and** [256-bits] that met the following: AES as specified in ISO 18033-3, **CBC as specified in ISO 10116, CCMP as defined in NIST SP800-38C and IEEE 802.11-2012, [***GCM as specified in ISO 19772,* ***GCMP as specified in NIST SP800-38D and IEEE 802.11ac-2013***].

FCS_COP.1/SigGen – Cryptographic Operation (Signature Generation and Verification)

FCS_COP.1.1/SigGen The TSF shall perform *cryptographic signature services (generation and verification*) in accordance with a specified cryptographic algorithm

[

- RSA Digital Signature Algorithm and cryptographic key sizes (modulus) [*2048 bits or greater*],
- Elliptic Curve Digital Signature Algorithm and cryptographic key sizes [*256, 384 bits*]

]

that meet the following:

[

- For RSA schemes: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3,
- For ECDSA schemes: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 6 and Appendix D, Implementing “NIST curves” [P-256, P-384]; ISO/IEC 14888-3, Section 6.4

].

FCS_COP.1/Hash – Cryptographic Operation (Hash Algorithm)

FCS_COP.1.1/Hash The TSF shall perform *cryptographic hashing services* in accordance with a specified cryptographic algorithm [SHA-1, SHA-256, SHA-384, SHA-512] ~~and cryptographic key sizes [*assignment: cryptographic key sizes*~~] and **message digest sizes** [**160, 256, 384, 512**] **bits** that meet the following: *ISO/IEC 10118-3:2004.*

FCS_COP.1/KeyedHash – Cryptographic Operation (Keyed Hash Algorithm)

FCS_COP.1.1/KeyedHash The TSF shall perform *keyed-hash message authentication* in accordance with a specified cryptographic algorithm [*HMAC-SHA1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512*] and cryptographic key sizes [*160, 256, 384, 512*] **and message digest sizes** [**160, 256, 384, 512**] **bits** that meet the following: *ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”*.

FCS_RBG_EXT.1 – Random Bit Generation

FCS_RBG_EXT.1.1 The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using [CTR_DRBG (AES)].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [[*1*] platform-based noise source] with a minimum of [*256 bits*] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 “Security Strength Table for Hash Functions”, of the keys and hashes that it will generate.

FCS_IPSEC_EXT.1 – IPsec Protocol

FCS_IPSEC_EXT.1.1 The TSF shall implement the IPsec architecture as specified in RFC 4301.

FCS_IPSEC_EXT.1.2 The TSF shall have a nominal, final entry in the SPD that matches anything that is otherwise unmatched, and discards it.

FCS_IPSEC_EXT.1.3 The TSF shall implement [transport mode, tunnel mode].

FCS_IPSEC_EXT.1.4 The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using the cryptographic algorithms [AES-GCM-128 (RFC 4106), AES-GCM-256 (RFC 4106)] together with a Secure Hash Algorithm (SHA)-based HMAC [no HMAC algorithm].

FCS_IPSEC_EXT.1.5 The TSF shall implement the protocol: [

- IKEv2 as defined in RFC 5996 and [with no support for NAT traversal] and [RFC 4868 for hash functions]

].

FCS_IPSEC_EXT.1.6 The TSF shall ensure the encrypted payload in the [IKEv2] protocol uses the cryptographic algorithms [AES-GCM-128, AES-GCM-256 (specified in RFC 5282)].

FCS_IPSEC_EXT.1.7 The TSF shall ensure that: [

- IKEv2 SA lifetimes can be configured by an Security Administrator based on [
  - length of time, where the time values can be configured within [*2 minutes to 24*] hours]

].

FCS_IPSEC_EXT.1.8 The TSF shall ensure that: [

- IKEv2 Child SA lifetimes can be configured by an Security Administrator based on [
  - number of bytes;
  - length of time, where the time values can be configured within [*2 minutes to 8*] hours]

].

FCS_IPSEC_EXT.1.9 The TSF shall generate the secret value x used in the IKE Diffie-Hellman key exchange ("x" in g^x mod p) using the random bit generator specified in FCS_RBG_EXT.1, and having a length of at least [*128 (for DH Group 19), 192 (for DH Group 20)*] bits.

FCS_IPSEC_EXT.1.10 The TSF shall generate nonces used in [IKEv2] exchanges of length [

- at least 128 bits in size and at least half the output size of the negotiated pseudorandom function (PRF) hash

].

FCS_IPSEC_EXT.1.11 The TSF shall ensure that all IKE protocols implement DH Group(s) [19 (256-bit Random ECP), 20 (384-bit Random ECP)].

FCS_IPSEC_EXT.1.12 The TSF shall be able to ensure by default that the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [IKEv2 IKE_SA] connection is greater than or equal to the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [IKEv2 CHILD_SA] connection.

FCS_IPSEC_EXT.1.13 The TSF shall ensure that all IKE protocols perform peer authentication using [ECDSA, RSA] that use X.509v3 certificates that conform to RFC 4945 and [Pre-shared Keys].

FCS_IPSEC_EXT.1.14 The TSF shall only establish a trusted channel if the presented identifier in the received certificate matches the configured reference identifier, where the presented and reference identifiers are of the following fields and types: [SAN: IP address, SAN: Fully Qualified Domain Name (FQDN)] and [no other reference identifier type].

FCS_SSHS_EXT.1 – SSH Server Protocol

FCS_SSHS_EXT.1.1 The TSF shall implement the SSH protocol that complies with RFC(s) 4251, 4252, 4253, 4254 [4344, 5656, 6668, 8308 section 3.1, 8332].

FCS_SSHS_EXT.1.2 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, [password based].

FCS_SSHS_EXT.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than [*32,767*] bytes in an SSH transport connection are dropped.

FCS_SSHS_EXT.1.4 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: [aes128-cbc, aes256-cbc].

FCS_SSHS_EXT.1.5 The TSF shall ensure that the SSH public-key based authentication implementation uses [rsa-sha2-256, rsa-sha2-512] as its public key algorithm(s) and rejects all other public key algorithms.

FCS_SSHS_EXT.1.6 The TSF shall ensure that the SSH transport implementation uses [hmac-sha2-256, hmac-sha2-512] as its MAC algorithm(s) and rejects all other MAC algorithm(s).

FCS_SSHS_EXT.1.7 The TSF shall ensure that [ecdh-sha2-nistp256] and [ecdh-sha2-nistp384, ecdh-sha2-nistp521] are the only allowed key exchange methods used for the SSH protocol.

FCS_SSHS_EXT.1.8 The TSF shall ensure that within SSH connections the same session keys are used for a threshold of no longer than one hour, and each encryption key is used to protect no more than one gigabyte of data. After any of the thresholds are reached, a rekey needs to be performed.

FCS_RADSEC_EXT.1 – RADsec

FCS_RADSEC_EXT.1.1 – The TSF shall implement RADIUS over TLS as specified in RFC 6614 to communicate securely with a RADIUS server.

FCS_RADSEC_EXT.1.2 – The TSF shall perform peer authentication using [X.509v3 certificates].

Application Note: *This requirement has applied NIAP TD-0271*

FCS_TLSC_EXT.1/RADsec – TLS Client Protocol Without Mutual Authentication

FCS_TLSC_EXT.1.1/RADsec The TSF shall implement [*TLS 1.2 (RFC 5246)*] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites

[

○ TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268

]

and no other ciphersuites.

FCS_TLSC_EXT.1.2/RADsec The TSF shall verify that the presented identifier matches: [the reference identifier per RFC 6125 section 6, IPv4 address in SAN] and no other attribute types.

FCS_TLSC_EXT.1.3/RADsec When establishing a trusted channel, by default the TSF shall not establish a trusted channel if the server certificate is invalid. The TSF shall also [

- Not implement any administrator override mechanism

].

FCS_TLSC_EXT.1.4/RADsec The TSF shall [not present the Supported Elliptic Curves Extension] in the Client Hello.

Application Note: *This iteration of FCS_TLSC_EXT.1 applies to TLS 1.2 connections to a RADsec server*

FCS_TLSC_EXT.1/EST – TLS Client Protocol Without Mutual Authentication

FCS_TLSC_EXT.1.1/EST The TSF shall implement [*TLS 1.2 (RFC 5246)*] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites

[

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246

]

and no other ciphersuites.

FCS_TLSC_EXT.1.2/EST The TSF shall verify that the presented identifier matches [the reference identifier per RFC 6125 section 6, IPv4 address in SAN] and no other attribute types.

FCS_TLSC_EXT.1.3/EST When establishing a trusted channel, by default the TSF shall not establish a trusted channel if the server certificate is invalid. The TSF shall also [

- Not implement any administrator override mechanism

].

FCS_TLSC_EXT.1.4/EST The TSF shall [present the Supported Elliptic Curves/Supported Groups Extension with the following curves/groups: [secp256r1, secp384r1, secp521r1] and no other curves/groups] in the Client Hello.

Application Note: *This iteration of FCS_TLSC_EXT.1 applies to TLS 1.2 connections to an EST server*

FCS_TLSC_EXT.2 – TLS Client Support for Mutual Authentication

FCS_TLSC_EXT.2.1 The TSF shall support TLS communication with mutual authentication using X.509v3 certificates.

FCS_DTLSS_EXT.1 – DTLS Server Protocol Without Mutual Authentication

FCS_DTLSS_EXT.1.1 The TSF shall implement [DTLS 1.2 (RFC 6347] supporting the following ciphersuites:

[

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289

- TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268

]

and no other cipersuites.

FCS_DTLSS_EXT.1.2 The TSF shall deny connections from clients requesting *none*.

FCS_DTLSS_EXT.1.3 The TSF shall not proceed with a connection handshake attempt if the DTLS Client fails validation.

FCS_DTLSS_EXT.1.4 The TSF shall perform key establishment for TLS using [Diffie-Hellman parameters with size [2048 bits], ECDHE curves [secp384r1] and no other curves].

FCS_DTLSS_EXT.1.5 The TSF shall [silently discard the record] if a message received contains an invalid MAC.

FCS_DTLSS_EXT.1.6 The TSF shall detect and silently discard replayed messages for:

- DTLS records previously received.
- DTLS records too old to fit in the sliding window.

FCS_DTLSS_EXT.1.7 The TSF shall support [session resumption based on session IDs according to RFC 5246 (TLS1.2)].

.

FCS_DTLSC_EXT.1 – DTLS Client Protocol Without Mutual Authentication

FCS_DTLSC_EXT.1.1 The TSF shall implement [DTLS 1.2 (RFC 6347)] supporting the following ciphersuites

[

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268

].

FCS_DTLSC_EXT.1.2 The TSF shall verify that the presented identifier matches [the identifier per RFC 5280 Appendix A using [id-at-commonName] and no other attribute types].

FCS_DTLSC_EXT.1.3 When establishing a trusted channel, by default the TSF shall not establish a trusted channel if the server certificate is invalid. The TSF shall also [

- Not implement any administrator override mechanism

].

FCS_DTLSC_EXT.1.4 The TSF shall [present the Supported Elliptic Curves/Supported Groups Extension with the following curves/groups: [secp256r1, secp384r1, secp521r1] and no other curves/groups] in the Client Hello.

FCS_HTTPS_EXT.1 – HTTPS Protocol

FCS_HTTPS_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2 The TSF shall implement HTTPS using TLS.

FCS_HTTPS_EXT.1.3 If a peer certificate is presented, the TSF shall [*not require client authentication*] if the peer certificate is deemed invalid.

FCS_TLSS_EXT.1 – TLS Server Protocol Without Mutual Authentication

FCS_TLSS_EXT.1.1 The TSF shall implement [*TLS 1.2 (RFC 5246)*] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites:

- [
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
  - TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
  - TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246
  - TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
  - TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
  - TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
  - TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268

  ]

  and no other ciphersuites.

FCS_TLSS_EXT.1.2 The TSF shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0, and [TLS 1.1].

FCS_TLSS_EXT.1.3 The TSF shall perform key establishment for TLS using [*RSA with key size* [2048 bits], *ECDHE curves* [*secp256r, secp384r1*] *and no other curves*].

FCS_TLSS_EXT.1.4 The TSF shall support [session resumption based on session tickets according to RFC 5077].

Class: Identification and Authentication (FIA)

FIA_AFL.1 – Authentication Failure Management

FIA_AFL.1.1 The TSF shall detect when an Administrator configurable positive integer within [*1-25*] unsuccessful authentication attempts occur related to *Administrators attempting to authenticate remotely using a password*.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met, the TSF shall [prevent the offending remote Administrator from successfully establishing remote session using any authentication method that involves a password until [*unblocking action*] is taken by an Administrator; prevent the offending Administrator from successfully establishing remote session using any authentication method that involves a password until an Administrator defined time period has elapsed].

FIA_PMG_EXT.1 – Password Management

FIA_PMG_EXT.1.1 The TSF shall provide the following password management capabilities for administrative passwords:

1. Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”[*Additional Special Characters listed in Table 18*]];

Table 18. Additional Password Special Characters

Special Character	Name
	Space
;	Semicolon
:	Colon
"	Double Quote
‘	Single Quote
|	Vertical Bar
+	Plus
-	Minus
=	Equal Sign
.	Period
,	Comma
/	Slash
\	Backslash
<	Less Than
>	Greater Than
_	Underscore
`	Grave accent (backtick)
~	Tilde
{	Left Brace
}	Right Brace

2. Minimum password length shall be configurable to between [*8*] and [*16*] characters.

FIA_PSK_EXT.1 – Extended: Pre-Shared Key Composition

FIA_PSK_EXT.1.1 The TSF shall be able to use pre-shared keys for [IPsec].

FIA_PSK_EXT.1.2 The TSF shall be able to accept text-based pre-shared keys that:

- are 22 characters and [no other lengths];
- composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”).

FIA_PSK_EXT.1.3 The TSF shall be able to [accept] bit-based pre-shared keys.

FIA_UIA_EXT.1 – User Identification and Authentication

FIA_UIA_EXT.1.1 The TSF shall allow the following actions prior to requiring the non-TOE entity to initiate the identification and authentication process:

- Display the warning banner in accordance with FTA_TAB.1;
- [no other actions]

FIA_UIA_EXT.1.2 The TSF shall require each administrative user to be successfully identified and authenticated before allowing any other TSF-mediated action on behalf of that administrative user.

FIA_UAU_EXT.2 – Password-based Authentication Mechanism

FIA_UAU_EXT.2.1 The TSF shall provide a local [password-based, SSH public key-based] authentication mechanism to perform local administrative user authentication.

FIA_UAU.6 – Re-authenticating

FIA_UAU.6.1 The TSF shall re-authenticate the administrative user under the conditions: when the user changes their password, [no other conditions].

FIA_UAU.7 – Protected Authentication Feedback

FIA_UAU.7.1 The TSF shall provide only *obscured feedback* to the administrative user while the authentication is in progress **at the local console**.

FIA_8021X_EXT.1 – Extended: 802.1X Port Access Entity (Authenticator) Authentication

FIA_8021X_EXT.1.1 The TSF shall conform to IEEE Standard 802.1X for a Port Access Entity (PAE) in the “Authenticator” role.

FIA_8021X_EXT.1.2 The TSF shall support communications to a RADIUS authentication server conforming to RFCs 2865 and 3579.

FIA_8021X_EXT.1.3 The TSF shall ensure that no access to its 802.1X controlled port is given to the wireless client prior to successful completion of this authentication exchange.

FIA_X509_EXT.1/Rev – X.509 Certificate Validation

FIA_X509_EXT.1.1/Rev The TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certificate path validation **supporting a minimum path length of three certificates.**
- The certificate path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [a Certificate Revocation List (CRL) as specified in RFC 5759 Section 5].

- The TSF shall validate the extendedKeyUsage field according to the following rules:
  - Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.
  - Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.
  - Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.
  - OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.

FIA_X509_EXT.1.2/Rev The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

FIA_X509_EXT.1/ITT – X.509 Certificate Validation

FIA_X509_EXT.1.1/ITT The TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certificate path validation **supporting a minimum path length of two certificates.**
- The certificate path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [no revocation method].
- The TSF shall validate the extendedKeyUsage field according to the following rules:
  - Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.
  - Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.
  - OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.

FIA_X509_EXT.1.2/ITT The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

FIA_X509_EXT.2 – X.509 Certificate Authentication

FIA_X509_EXT.2.1 The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [IPsec, DTLS, TLS], and [no additional uses].

FIA_X509_EXT.2.2 When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall [not accept the certificate, accept the certificate].

FIA_X509_EXT.3 – X.509 Certificate Requests

FIA_X509_EXT.3.1 The TSF shall generate a Certification Request as specified by RFC 2986 and be able to provide the following information in the request: public key and [Common Name, Organization, Organizational Unit, Country].

FIA_X509_EXT.3.2 The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.

Class: Security Management (FMT)

FMT_MOF.1/ManualUpdate – Management of Security Functions Behavior

FMT_MOF.1.1/ManualUpdate The TSF shall restrict the ability to enable the functions *to perform manual update* to *Security Administrators*.

FMT_MOF.1/Services – Management of Security Functions Behavior

FMT_MOF.1.1/Services The TSF shall restrict the ability to enable and disable **start and stop** ~~the functions~~ **services** to *Security Administrators*.

FMT_MOF.1/Functions – Management of Security Functions Behavior

FMT_MOF.1.1/Functions The TSF shall restrict the ability to [*modify the behaviour of*] the functions [*transmission of audit data to an external IT entity*] to *Security Administrators*.

FMT_MTD.1/CoreData – Management of TSF Data

FMT_MTD.1.1/CoreData The TSF shall restrict the ability to *manage* the *TSF data* to *Security Administrators*.

FMT_MTD.1/CryptoKeys – Management of TSF Data

FMT_MTD.1.1/CryptoKeys The TSF shall restrict the ability to *manage* the *cryptographic keys to Security Administrators*.

FMT_SMF.1 – Specification of Management Functions

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

- *Ability to administer the TOE locally and remotely;*
- *Ability to configure the access banner;*
- *Ability to configure the session inactivity time before session termination or locking;*
- *Ability to update the TOE, and to verify the updates using [digital signature] capability prior to installing those updates;*
- *Ability to configure the authentication failure parameters for FIA_AFL.1;*

  [

  - *Ability to start and stop services;*
  - *Ability to configure audit behavior (e.g. changes to storage locations for audit; changes to behaviour when local audit storage space is full);*
  - *Ability to modify the behaviour of the transmission of audit data to an external IT entity;*
  - *Ability to manage the cryptographic keys;*
  - *Ability to configure the cryptographic functionality;*
  - *Ability to configure thresholds for SSH rekeying;*
  - *Ability to configure the lifetime for IPsec SAs;*
  - *Ability to configure the interaction between TOE components;*

- *Ability to re-enable an Administrator account*;
- *Ability to set the time which is used for time-stamps*;
- *Ability to configure the reference identifier for the peer*;
- *Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors*;
- *Ability to import X.509v3 certificates to the TOE's trust store;*
- *Ability to manage the trusted public keys database*

]

FMT_SMR.1 – Specification Management Roles

FMT_SMR.1.3 The TSF shall ensure that the ability to remotely administer the TOE from a wireless client shall be disabled by default.

FMT_SMR.2 – Restrictions on Security Roles

FMT_SMR.2.1 The TSF shall maintain the roles:

- *Security Administrator*.

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

FMT_SMR.2.3 The TSF shall ensure that the conditions

- *The Security Administrator role shall be able to administer the TOE locally;*
- *The Security Administrator role shall be able to administer the TOE remotely*

are satisfied.

Class: Protection of the TSF (FPT)

FPT_SKP_EXT.1 – Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

FPT_APW_EXT.1 – Protection of Administrator Passwords

FPT_APW_EXT.1.1 The TSF shall store administrative passwords in non-plaintext form.

FPT_APW_EXT.1.2 The TSF prevent the reading of plaintext administrative passwords.

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 the power-on self-tests.

FPT_STM_EXT.1 – Reliable Time Stamps

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

FPT_STM_EXT.1.2 The TSF shall [allow the Security Administrator to set the time].

FPT_TST_EXT.1 – TSF Testing

FPT_TST_EXT.1.1 Refinement: The TSF shall run a suite of the following self-tests during initial start-up (on power on) and [*at the request of the authorized ~~user~~ Administrator*] to demonstrate the correct operation of the TSF: [*FIPS 140-2 standard power-up self-tests and software/firmware integrity test*].

FPT_TST_EXT.1.2 The TSF shall provide the capability to verify the integrity of stored TSF executable code when it is loaded for execution through the use of the TSF-provided cryptographic service specified in **FCS_COP.1/SigGen**.

FPT_TUD_EXT.1 – Trusted Update

FPT_TUD_EXT.1.1 The TSF shall provide *Security Administrators* the ability to query the currently executing version of the TOE firmware/software and [the most recently installed version of the TOE firmware/software].

FPT_TUD_EXT.1.2 The TSF shall provide *Security Administrators* the ability to manually initiate updates to TOE firmware/software and [no other update mechanism].

FPT_TUD_EXT.1.3 The TSF shall provide means to authenticate firmware/software updates to the TOE using a [digital signature] prior to installing those updates.

FPT_ITT.1 – Basic Internal TSF Data Transfer Protection

FPT_ITT.1.1 The TSF shall protect TSF data from disclosure and **detect its** modification when it is transmitted between separate parts of the TOE **through the use of** [**DTLS**].

Class: TOE Access (FTA)

FTA_SSL_EXT.1 – TSF-initiated Session Locking

FTA_SSL_EXT.1.1 The TSF shall, for local interactive sessions, [terminate the session] after a Security Administrator-specified time period of inactivity.

FTA_SSL.3 – TSF-initiated Termination

FTA_SSL.3.1 The TSF shall terminate **a remote** interactive session after a *Security Administrator-configurable time interval of session inactivity*.

FTA_SSL.4 – User-initiated Termination

FTA_SSL.4.1 The TSF shall allow **Administrator**-initiated termination of the **Administrator**'s own interactive session.

FTA_TAB.1 – Default TOE Access Banners

FTA_TAB.1.1 Before establishing **an administrative use**r session the TSF shall display **a Security Administrator-specified** advisory **notice and consent** warning message regarding use of the TOE.

FTA_TSE.1 – TOE Session Establishment

FTA_TSE.1.1 Refinement: The TSF shall be able to deny establishment of **a wireless client** session based on **TOE interface, time, day**, [*no other attributes*].

Application Note: *TOE Interface refers to the WLAN SSID the client is attempting to use.*

Class: Trusted Path/Channels (FTP)

FTP_ITC.1 – Inter-TSF Trusted Channel

FTP_ITC.1.1 Refinement: The TSF shall **be capable of using IEEE 802.11-2012(WPA2), IEEE 802.1X**, [**IPsec, Radius over TLS**], and [TLS] **to** provide a trusted communication channel between itself and **authorized IT entities supporting the following capabilities: WLAN clients, audit servers, 802.1X authentication servers and** [***EST Server***] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

FTP_ITC.1.2 The TSF shall permit **the TSF or the authorized IT entities** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [

- *Syslog server over IPsec*
- *RADIUS Authentication over TLS (RADsec)*
- *Certificate enrollment over TLS*]

Application Note: *This requirement has applied NIAP TD-0271*

FTP_TRP.1/Admin – Trusted Path

FTP_TRP.1.1/Admin The TSF shall **be capable of using** [**SSH, HTTPS**] **to** provide a communication path between itself and **authorized** remote **Administrators** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **disclosure and provides detection of modification of the channel data**.

FTP_TRP.1.2/Admin The TSF shall permit remote **Administrators** to initiate communication via the trusted path.

FTP_TRP.1.3/Admin The TSF shall require the use of the trusted path for *initial Administrator authentication and all remote administration actions*.

TOE SFR Dependencies Rationale

The Security Functional Requirements included in the ST represent all mandatory, optional, and selection-based SFRs specified in [NDcPP] and [WLAN_EP] against which exact compliance is claimed.

All dependency rationale in the ST are considered to be identical to those that are defined in the claimed PP.

Security Assurance Requirements

The TOE assurance requirements for this ST are taken directly from the NDcPP which are derived from [CC_PART3]. The assurance requirements are summarized in the table below.

Table 19. Assurance Requirements

Assurance Class	Components	Description
Security Target (ASE)	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.1	Security objectives for the operational environment
	ASE_REQ.1	Stated security requirements
	ASE_SPD.1	Security Problem Definition

	ASE_TSS.1	TOE summary specification
Development (ADV)	ADV_FSP.1	Basic functional specification
Guidance Documents (AGD)	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life Cycle Support (ALC)	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM coverage
Tests (ATE)	ATE_IND.1	Independent testing – conformance
Vulnerability Assessment (AVA)	AVA_VAN.1	Vulnerability survey

Security Assurance Requirements Rationale

The Security Assurance Requirements (SARs) in this Security Target represent the SARs identified in the [NDcPP] and [WLAN_EP]. As such, the [NDcPP] and [WLAN_EP] SAR rationale is deemed acceptable since the PPs themselves have been approved.

Assurance Measures

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

Table 20. Assurance Measures

Assurance Component	Rationale
ASE_INT.1 ASE_CCL.1 ASE_OBJ.1 ASE_ECD.1 ASE_REQ.1 ASE_SPD.1 ASE_TSS.1	Cisco provided this Security Target document.
ADV_FSP.1	No additional “functional specification” documentation was provided by Cisco to satisfy the Evaluation Activities.
AGD_OPE.1 AGD_PRE.1	Cisco will provide the guidance documents with the ST.
ALC_CMC.1 ALC_CMS.1	Cisco will identify the TOE such that it can be distinguished from other products or versions from the Cisco and can be easily specified when being procured by an end user.
ATE_IND.1	Cisco will provide the TOE for testing.
AVA_VAN.1	Cisco will provide the TOE for Vulnerability Analysis.

TOE Summary Specification

The table below identifies and describes how the Security Functional Requirements identified above are met by the TOE.

Table 21. TSS Rationale

TOE SFR	Component Implemented	Rationale
FAU_GEN.1 FAU_GEN_EXT.1	WLC, AP	The TOE generates an audit record whenever an audited event occurs. The types of events that cause audit records to be generated include cryptographic related events, events related to the enforcement of information flow policies, identification and authentication related events, and administrative events. When generating or deleting a cryptographic key the TOE will record an audit event in the audit log indicating the key with its associated label that was generated or deleted from key storage. A mapping is provided in table 25 to show which auditable events are covered by which components of the TOE. Each event is specified in the audit log enough detail to identify the user for which the event is associated, when the event occurred, where the event occurred, the outcome of the event, and the type of event that occurred.
FAU_GEN.2	WLC, AP	The TOE associates each auditable event with the user or entity that triggered the event. For a human user, a user identity, or related session ID would be included in the audit record. For an IT entity or device, the IP address, MAC address, host name, or other configured identification is presented.

<table>
<tr><th>TOE SFR</th><th>Component Implemented</th><th>Rationale</th></tr>
<tr><td>FAU_STG_EXT.1
FAU_STG.1</td><td>WLC, AP</td><td>
<p>The Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.6 TOE is distributed. After the AP joins the WLC to form a distributed TOE the AP will transmit its audit messages to the WLC over the secure DTLS channel described in FPT_ITT.1. A mapping between the transmitting and storing TOE components is provided below.</p>
<table>
<tr><th>Transmitting Component</th><th>Storing Component</th></tr>
<tr><td>AP</td><td>WLC</td></tr>
</table>
<p>Audit data from the AP is buffered until its contents has been transferred to the WLC where it is stored locally. Under normal operating conditions the AP transmission buffer will never become exhausted. Should an unlikely event occur where the transmission buffer becomes exhausted, the oldest message in the buffer will be overwritten to accommodate the new message.</p>
<p>The WLC, which is the component that stores audit data locally, will transmit all audit messages in real-time to a specified, external syslog server. The WLC protects communications with an external syslog server using IPsec. The WLC is capable of detecting if the IPsec connection fails. The TOE also stores a limited set of audit records locally on the TOE and continues to do so if the communication with the syslog server goes down. If the IPsec connection inadvertently fails, the TOE will buffer between 4096-bytes and 2,148,483,647 bytes of audit records on the TOE. When connectivity with its configured syslog server is restored, the WLC will transmit the buffer contents. The exact size of the audit storage is configured using the “logging buffered” command. If the local logging limit is reached, the oldest messages overwritten to accommodate the new message.</p>
<p>The WLC protects the local logging buffer from unauthorized access, modification or deletion. No account is able to modify data that has been written to the local logging buffer. Only the Administrator is able to clear the local logging buffer. Audit messages are stored locally on the Controller and are viewable via CLI or GUI.</p>
</td></tr>
<tr><td>FAU_STG_EXT.4
FAU_STG_EXT.5</td><td>WLC, AP</td><td>The AP maintains the audit data in a transmission buffer and continues to do so until the AP has transferred its contents to the WLC where it is stored locally.</td></tr>
</table>

TOE SFR	Component Implemented	Rationale
FCO_CPC_EXT.1	WLC, AP	At the WLC, before an AP can join and communicate with a WLC, the Administrator must enable an AP authorization list maintained on the WLC. The AP authorization list defines the APs that are permitted to join by identification of its unique serial number. The AP authorization list is available under Configuration -> Security -> AAA Advanced in the Controller GUI. Only the Administrator can access the AP authorization list. At the AP, the AP will compare the contents of the "AC Name" field received from the CAPWAP Discovery Response packet and compare it to the contents of the Common Name field in the WLC's certificate. The WLC and AP components will implement a registration channel that meets secure channel requirements in FPT_ITT.1 and proceed to join if the following is met: ■ If the WLC determines the serial number in the AP authorization list matches the subject Distinguished Name in the X.509 certificate presented by the AP. ■ If the AP determines the contents of the "AC Name" field in the CAPWAP Discovery Response packet matches the contents of the Common Name field in the WLC's certificate. If the WLC determines the contents of the subject Distinguished Name does not match a serial number entry in the authorization list, or if the AP determines the contents of the "AC Name" field does not match the contents of the CN field of the WLC certificates, the secure registration channel will not form and the AP will not be able to join the WLC. Once registration has completed the channel is used for internal communications. All aspects of the registration and internal communication channel are met by FPT_ITT.1. Refer to FCS_DTLSS_EXT.1 for additional information. The Administrator may remove an AP from the authorization list, thereby disabling the AP from joining the WLC.

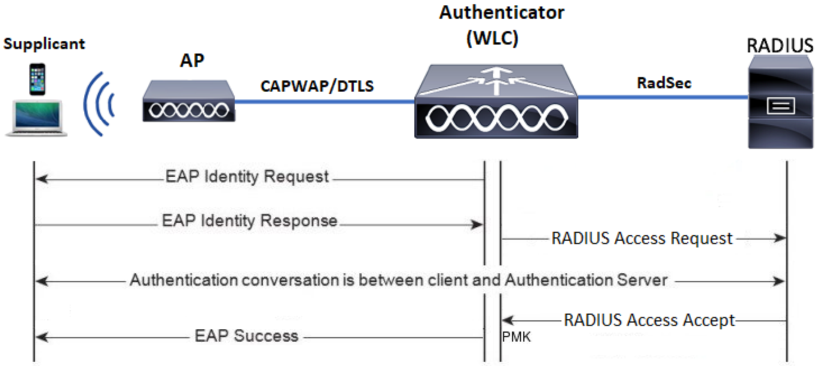
<table>
<tr>
<td>FCS_CKM.1/KeyGen
FCS_CKM.2/KeyEst</td>
<td>WLC, AP</td>
<td>
<p>The following table describes the key generation algorithms the TOE implements to generate asymmetric keys used for <b>device authentication</b>:</p>
<table>
<tr><th>Scheme</th><th>Standard</th><th>Key Size/ NIST Curve</th><th>SFR</th><th>Service</th></tr>
<tr><td>RSA</td><td>FIPS PUB 186-4</td><td>2048
3072</td><td>FCS_SSHS_EXT.1</td><td>SSH Remote Administration</td></tr>
<tr><td></td><td></td><td></td><td>FCS_TLSC_EXT.1 /RADsec
FCS_TLSC_EXT.2</td><td>RADsec</td></tr>
<tr><td></td><td></td><td></td><td>FCS_TLSC_EXT.1/EST
FCS_TLSC_EXT.2</td><td>EST Server</td></tr>
<tr><td></td><td></td><td></td><td>FCS_TLSS_EXT.1</td><td>HTTPS Remote Administration</td></tr>
<tr><td></td><td></td><td></td><td>FCS_DTLSS_EXT.1</td><td>DTLS Server</td></tr>
<tr><td></td><td></td><td></td><td>FCS_IPSEC_EXT.1</td><td>Transmit generated audit data to an external IT entity</td></tr>
<tr><td>ECC</td><td>FIPS PUB 186-4</td><td>P-256
P-384</td><td>FCS_TLSS_EXT.1</td><td>HTTPS Remote Administration</td></tr>
<tr><td></td><td></td><td></td><td>FCS_IPSEC_EXT.1</td><td>Transmit generated audit data to an external IT entity</td></tr>
<tr><td></td><td></td><td></td><td>FCS_TLSC_EXT.1/EST
FCS_TLSC_EXT.2</td><td>EST Server</td></tr>
<tr><td>ECC</td><td>FIPS PUB 186-4</td><td>P-384</td><td>FCS_DTLSS_EXT.1</td><td>DTLS Server</td></tr>
<tr><td></td><td></td><td></td><td>FCS_DTLSC_EXT.1</td><td>DTLS Client</td></tr>
</table>
<p>With the exception to SSH, the keys are used to generate certificate signing requests (CSRs) in which the public key is associated with an X.509 certificate.</p>
<p>The following table shows the key generation algorithms the TOE implements to generate asymmetric keys used for <b>key establishment</b>:</p>
<table>
<tr><th>Scheme</th><th>Standard</th><th>Key Size/ NIST Curve</th><th>SFR</th><th>Service</th></tr>
<tr><td>RSA</td><td>FIPS PUB 186-4</td><td>2048</td><td>FCS_TLSC_EXT.2</td><td>RADsec</td></tr>
<tr><td>ECC</td><td>FIPS PUB 186-4</td><td>P-256
P-384
P-521</td><td>FCS_TLSS_EXT.1</td><td>HTTPS Remote Administration</td></tr>
<tr><td></td><td></td><td></td><td>FCS_IPSEC_EXT.1</td><td>Transmit generated audit</td></tr>
</table>
</td>
</tr>
</table>

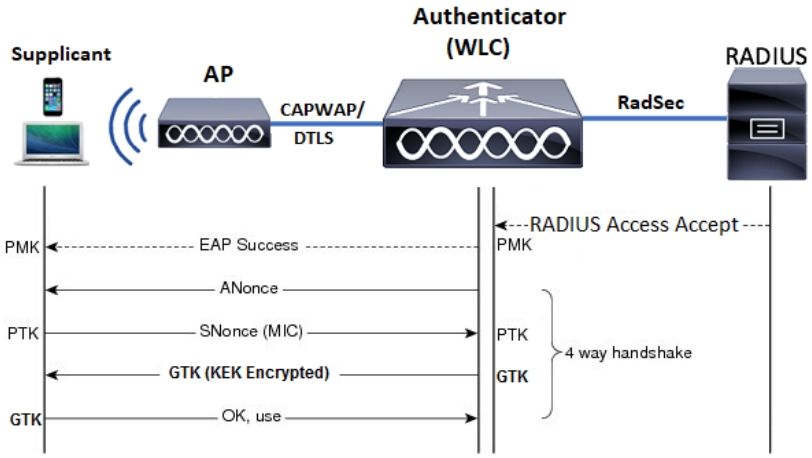
				data to an external IT entity
			FCS_SSHS_EXT.1	SSH Remote Administration
			FCS_TLSC_EXT.1/EST FCS_TLSC_EXT.2	EST Server
ECC	FIPS PUB 186-4	P-384	FCS_DTLSS_EXT.1	DTLS Server
			FCS_DTLSC_EXT.1	DTLS Client
FFC	FIPS PUB 186-4	2048	FCS_DTLSS_EXT.1	DTLS Server
			FCS_DTLSC_EXT.1	DTLS Client
			FCS_TLSC_EXT.1/EST FCS_TLSC_EXT.2	EST Server

The following table shows the methods the TOE implements for **key establishment**:

Scheme	Standard	SFR	Service
RSAES-PKCS1-v1_5	Section 7.2 of RFC 3447	FCS_TLSC_EXT.2	RADsec
		FCS_TLSS_EXT.1	HTTPS Remote Administration
EC-DH	NIST SP 800-56A Revision 2	FCS_TLSS_EXT.1	HTTPS Remote Administration
		FCS_IPSEC_EXT.1	Transmit generated audit data to an external IT entity
		FCS_SSHS_EXT.1	SSH Remote Administration
		FCS_TLSC_EXT.1/EST FCS_TLSC_EXT.2	EST Server

<table>
<tr><th>TOE SFR</th><th>Component Implemented</th><th>Rationale</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td rowspan="2"></td><td rowspan="2"></td><td>FCS_DTLSS_EXT.1</td><td>DTLS Server</td></tr>
<tr><td>FCS_DTLSC_EXT.1</td><td>DTLS Client</td></tr>
<tr><td rowspan="3">FFC</td><td rowspan="3">NIST SP 800-56A Revision 2</td><td>FCS_DTLSS_EXT.1</td><td>DTLS Server</td></tr>
<tr><td>FCS_DTLSC_EXT.1</td><td>DTLS Client</td></tr>
<tr><td>FCS_TLSC_EXT.1/EST
FCS_TLSC_EXT.2</td><td>EST Server</td></tr>
</table>
</td></tr>
</table>

FCS_CKM.1/WPA2 FCS_CKM.2/PMK FCS_CKM.2/GTK FCS_CKM.2/PTK FIA_8021X_EXT.1	WLC, AP	Prior to allowing network access to wireless clients, the TOE facilitates authentication of Supplicants and derivation of 802.11 encryption keys by performing the role of ‘Authenticator’ in an 802.1X authentication exchange. The TSF strictly follows port-based network control as defined in Clause 7.1 and EAP as defined in Clause 8 and Clause 11 of [IEEE 802.1X-2010]. After the wireless client and AP complete the initial 802.11 Association process, the WLC begins by sending an EAPOL identity request to the Supplicant. The Supplicant answers with an EAP identity response, which the TOE relays to the Authentication Server as an RADIUS Access Request message. See the figure below. **Figure 3. EAP Message Exchange**  Supplicant AP Authenticator (WLC) RADIUS CAPWAP/DTLS RadSec EAP Identity Request EAP Identity Response RADIUS Access Request Authentication conversation is between client and Authentication Server RADIUS Access Accept PMK EAP Success ‘EAP-TLS’ is needed for testing authentication in the WLAN AS EP. EAP is an authentication framework and key distribution protocol and TLS requires the Supplicant and RADIUS authentication server mutually authenticate with X.509 certificates. If the Supplicant is successfully authenticated using EAP-TLS, the RADIUS server returns Access-Accept packet and generates the Pairwise Master Key (PMK). The RADIUS authentication server distributes the PMK to both the Authenticator and Supplicant. The TOE also creates the Group Master Key (GMK). The TOE provides RADsec to protect the PMK received from the RADIUS authentication server. The PMK is received by the TOE (Authenticator) via the **MS-MPPE-Recv-Key** EAP attribute. The Authenticator and Supplicant perform a four-way handshake to derive the PTK and if necessary, the GTK temporal keys from the master keys. The TSF implements PRF-384 and PRF-704 key derivation algorithms as specified in [IEEE 802.11-2012] and [IEEE 802.11ac-2013] respectively, to derive the number of bits required to obtain Pairwise Transient Key (PTK) and Group Temporal Key (GTK) keys. The Authenticator securely distributes the GTK to the Supplicant using a KEK and distributes both the PTK and GTK to the AP over the internal trusted channel protected by DTLS. The GTK is also protected with an AES Key Wrap. The GTK is used to protect multicast/broadcast traffic and is shared among all Supplicants and the AP. The Pairwise Transient Key (PTK) is used to protect unicast traffic with a single Supplicant. Figure 4 below represents the four-way handshake exchanges. **Figure 4. Four-Way Handshake**

		 Supplicant AP CAPWAP/ DTLS Authenticator (WLC) RadSec RADIUS RADIUS Access Accept PMK EAP Success PMK ANonce PTK SNonce (MIC) PTK GTK (KEK Encrypted) GTK 4 way handshake GTK OK, use 1. The Authenticator sends an EAPOL-Key frame containing an Authenticator nonce (ANonce), a random number generated from the TOE's DRBG The Supplicant derives a PTK from the ANonce and Supplicant nonce (SNonce), which is a random number generated by the Supplicant. 2. The Supplicant sends an EAPOL-Key frame containing a SNonce and an message integrity check (MIC). The Authenticator validates the MIC in the EAPOL-Key frame. The Authenticator derives a PTK using a pseudo-random function (PRF), and ANonce generated from the TOE's DRBG. The PTK includes a Key Encryption Key (KEK) generated using an AES key wrap algorithm. The KEK provides confidentiality of the GTK when distributed to the Supplicant. 3. The Authenticator derives the GTK from its GMK. The Authenticator sends an EAPOL-Key frame containing the KEK protected GTK with the MIC to the Supplicant for installation. The Supplicant is able to decrypt the GTK as it has derived its own copy of the PTK from its successful authentication with the RADIUS authentication server. 4. The Supplicant sends an EAPOL-Key frame to confirm that the temporal keys were installed and encrypted transmissions are ready to begin. If the 4-way handshake was successful, the Authenticator will distribute its temporal keys to the AP and open access to the logical port allowing 802.11 wireless data frames from the wireless client to pass as 802.3 Ethernet frames on the network. By default, the Authenticator will update the GMK every 3600 seconds (1 hour). When Authenticator updates the GMK the TOE performs the following two-step process to securely distribute the updated GTK to the Supplicant: 1. The Authenticator sends the updated GTK protected with the KEK to the Supplicant for installation. 2. The Supplicant sends an acknowledgement message indicating the TOE can begin using the new GTK. By default, the Authenticator will limit the PMK lifetime to 1800 seconds (30 minutes). The WLC will send a de-authentication frame to the client thus forcing the Supplicant to re-authenticate with a new key.

<table>
<tr><th>TOE SFR</th><th>Component Implemented</th><th>Rationale</th></tr>
<tr><td></td><td></td><td>Certification testing performed by the Wi-Fi Alliance demonstrates the TOE implements the IEEE 802.11-2012 standard correctly. Refer to Table 24 for identification of the relevant Wi-Fi Alliance certificates.</td></tr>
<tr><td>FCS_CKM.4</td><td>WLC, AP</td><td>The TOE destroys private keys, session keys, and Critical Security Parameters (CSP) used to generate keys as specified in table 22.</td></tr>
<tr><td>FCS_COP.1/
DataEncryption</td><td>WLC, AP</td><td>The TOE provides symmetric encryption and decryption capabilities using AES as specified in ISO 18033-3 supporting the following modes:
- CBC as specified in ISO 10116;
- GCM mode as specified in ISO 1977;
- CCMP mode as specified in NIST SP800-38C and IEEE 802.11-2012;
- GCMP mode as specified in NIST SP800-38D and IEEE 802.11ac-2013.
The TOE uses the AES encryption algorithm in the following protocols:
- SSH – CBC mode with key sizes of 128 bits and 256 bits;
- HTTPS (TLS Server) - GCM and CBC modes with a key size of 128 and 256 bits;
- TLS Client (RADsec) – CBC mode with a key size of 128 bits;
- DTLS Server (CAPWAP) – CBC mode with a key size of 256 bits;
- IPsec - GCM mode with key sizes of 128 bits;
- WPA2/Enterprise: CCMP and GCMP modes and key sizes as listed in the table below:<table><tr><th>AP</th><th>Modes</th><th>Key Sizes</th></tr><tr><td>4800, 3800, 2800, IW6300, ESW6300, 1562, 9130</td><td>GCMP, CCMP</td><td>128, 256</td></tr><tr><td>9105, 9120, 9115</td><td>GCMP, CCMP</td><td>128</td></tr></table>Refer to Table 23 for identification of the relevant CAVP certificates.</td></tr>
<tr><td>FCS_COP.1/SigGen</td><td>WLC, AP</td><td>The TOE provides cryptographic signature services using Elliptic Curve Digital Signature Algorithm with a key size of 256 and 384 bits and RSA Digital Signature Algorithm with key size of 2048 and greater, as specified in FIPS PUB 186-4, “Digital Signature Standard.” Refer to Table 21 for identification of the relevant CAVP certificates.</td></tr>
</table>

TOE SFR	Component Implemented	Rationale
FCS_COP.1/Hash	WLC, AP	The TOE provides cryptographic hashing services using SHA-1, SHA-256, SHA-384, and SHA-512 as specified in FIPS Pub 180-3 "Secure Hash Standard." Refer to Table 23 for identification of the relevant CAVP certificates. Hash functions are used in the TOE as follows: ■ SSH – SHA-256 and SHA-512 ■ HTTPS (TLS Server) – SHA-1, SHA-256, and SHA-384 ■ TLS Client (RADsec) – SHA-1 ■ DTLS Server (CAPWAP) – SHA-2 ■ IKE/IPSEC – SHA-1, SHA-256, SHA-384, and SHA-512 ■ Image Verification and Software Integrity - SHA-512
FCS_COP.1/ KeyedHash	WLC, AP	The TOE provides keyed-hashing message authentication services using HMAC-SHA-1 and HMAC-SHA-256 that operates on 512-bit blocks and HMAC-SHA-384 and HMAC-SHA-512 operating on 1024-bit blocks of data, with key sizes and message digest sizes of 160-bits, 256 bits, 384 bits, and 512 bits respectively as specified in ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2".
FCS_RBG_EXT.1	WLC, AP	The TSF implements a random bit generator (RBG) based on the AES-256 block cipher, in accordance with ISO/IEC 18031:2011. This DRBG is seeded with a hardware entropy source that provides 256 bits of entropy to the DRBG.

FCS_IPSEC_EXT.1	WLC	The TSF implements IPsec to provide authentication and encryption services to prevent unauthorized viewing or modification of syslog data as it travels over the external network. The TSF's implementation of the IPsec standard (in accordance with the RFCs noted in the SFR) uses the Encapsulating Security Payload (ESP) protocol to provide authentication, encryption and anti-replay services supporting the following algorithms: ▪ AES-GCM-128 and AES-GCM-256 The TOE provides IPsec protection supporting one of two modes: 1) With a syslog server operating as an IPsec peer of the TOE (transport mode); or 2) With a syslog server is not directly co-located with the TOE but is adjacent to an IPsec peer within a trusted facility, and the syslog records are tunneled over the public network (tunnel mode). The administrator defines the traffic that needs to be protected between two IPsec peers by configuring access lists and applying these access lists to interfaces using crypto map sets. A crypto map set can contain multiple entries, each with a different access list. The crypto map entries are searched in a sequence--the router attempts to match the packet to the access list specified in that entry. When a packet matches a permit entry in a particular access list, and the corresponding crypto map entry is tagged connections are established, if necessary. If the crypto map entry is tagged as ipsec-isakmp, IPsec is triggered. If there is no SA that the IPsec can use to protect this traffic to the peer, IPsec uses IKE to negotiate with the re-mote peer to set up the necessary IPsec SAs on behalf of the data flow. The negotiation uses information specified in the crypto map entry as well as the data flow information from the specific access list entry. Once established, the set of SAs (outbound to the peer) is then applied to the triggering packet and to subsequent applicable packets as those packets exit the Controller. "Applicable" packets are packets that match the same access list criteria that the original packet matched. For example, all applicable packets could be encrypted be-fore being forwarded to the remote peer. The corresponding inbound SAs are used when processing the incoming traffic from that peer. Access lists associated with IPsec crypto map entries also represent the traffic that the Controller needs protected by IPsec. Inbound traffic is processed against crypto map entries. if an unprotected packet matches a permit entry in a particular access list associated with an IPsec crypto map entry, that packet is dropped because it was not sent as an IPsec-protected packet. The traffic matching the permit ACLs would then flow through the IPsec tunnel and be classified as "PROTECTED". Traffic that does not match a permit ACL in the crypto map, but that is not disallowed by other ACLs on the interface is allowed to BYPASS the tunnel. Traffic that does not match a permit ACL and is also blocked by other non-crypto ACLs on the interface would be DISCARDED. Rules applied to an access control list can be applied to either inbound or outbound traffic. IPsec Internet Key Exchange, also called ISAKMP, is the negotiation protocol that lets two peers agree on how to build an IPsec Security Association (SA). The strength of the symmetric algorithm negotiated to protect the IKEv2 IKE_SA connection is greater than or equal to the strength of the symmetric algorithm negotiated to protect the IKEv2 CHILD_SA connection. The IKE protocols implement Peer Authentication using ECDSA or RSA X.509v3 certificates or pre-shared keys. IKE separates negotiation into two phases: phase 1 and phase 2. Phase 1 creates the first tunnel, which protects later ISAKMP negotiation messages. The key negotiated in phase 1 enables IKE peers to communicate securely in phase 2. During Phase 2 IKE establishes the IPsec SA. IKE maintains a trusted channel, referred to as a Security

		Association (SA), between IPsec peers that is also used to manage IPsec connections, including: ■ The negotiation of mutually acceptable IPsec options between peers (including peer authentication parameters, either signature based or pre-shared key based), ■ The establishment of additional Security Associations to protect packets flows using Encapsulating Security Payload (ESP), and ■ The agreement of secure bulk data encryption AES keys for use with ESP. The resulting potential strength of the symmetric key will be 128 or 256 bits of security depending on the algorithms negotiated between the two IPsec peers. As part of this negotiation, the TOE verifies that the negotiated phase 2 symmetric algorithm key strength is at most as large as the negotiated phase 1 key strength as configured on the TOE and peer via an explicit check. Each IKE negotiation begins by agreement of both peers on a common (shared) IKE policy. This policy states which security parameters will be used to protect subsequent IKE negotiations and mandates how the peers are authenticated. The Security Administrator can configure multiple, prioritized policies on each peer, each with a different combination of parameter values. However, at least one of these policies must contain exactly the same encryption, hash, authentication, and Diffie-Hellman parameter values as one of the policies on the remote peer. For each policy created, the Security Administrator assign's a unique priority (1 through 10,000, with 1 being the highest priority). When the IKE negotiation begins, IKE searches for an IKE policy that is the same on both peers. The peer that initiates the negotiation will send all its policies to the remote peer, and the remote peer will try to find a match. The remote peer looks for a match by comparing its own highest priority policy against the policies received from the other peer. The remote peer checks each of its policies in order of its priority (highest priority first) until a match is found. After the two peers agree upon a policy, the security parameters of the policy are identified by an SA established at each peer, and these IKE SAs apply to all subsequent IKE traffic during the negotiation. When a packet is processed by the TOE and it determines it requires IPsec, it uses active SA settings or creates new SAs for initial connections with the IPsec peer. The TOE supports IKEv2 session establishment. The TOE supports configuration of session lifetimes for both Phase 1 SAs and Phase 2 SAs using the following the command “lifetime.” The time values for Phase 1 SAs can be limited up to 24 hours and for Phase 2 SAs up to 8 hours. The Phase 2 SA lifetimes can also be configured by an Administrator based on number of bytes. The TOE supports Diffie-Hellman Groups 19 and 20. The length of the nonce is equal to that of the hash PRF used in the session establishment (for SHA-256 hash based PRF the nonce is 256-bits and for SHA-384 Hash based PRF the nonce is 384-bits) The TSF generates the secret value 'x' used in the IKEv2 Diffie-Hellman key exchange ('x' in g^x mod p) using the NIST approved DRBG specified in FCS_RBG_EXT.1 and having possible lengths of 256 or 384 bits. When a random number is needed for a nonce, the probability that a specific nonce value will be repeated during the life a specific IPsec SA is less than 1 in 2^{128}. The nonce is likewise generated using the AES-CTR DRBG.

TOE SFR	Component Implemented	Rationale
		The TOE supports authentication of IPsec peers using pre-shared keys, and ECDSA or RSA X.509 certificates. Pre-shared keys must be entered my the Security Administrator and must be of length 22 characters or greater. During IKE establishment, IPsec peers authenticate each other by creating and exchanging a hash value that includes the pre-shared key. The TOE will compare the received hash value to its computed hash and determine if it matches. If it does, pre-shared key authentication is successful; otherwise pre-shared key authentication fails. For peer authentication using RSA or ECDSA certificates, the TOE validates the presented identifier provided supporting the following fields and types: SAN: IP address, SAN: Fully Qualified Domain Name (FQDN), CN: IP address, and CN: Fully Qualified Domain Name (FQDN). Simultaneous use of the same identifier type in both the CN and SAN fields is not supported. Certificate maps provide the ability for a certificate to be matched with a given set of criteria. The Administrator is instructed in the CC Configuration Guide to specify one or more certificate fields together with their matching criteria and the value to match. In the evaluated configuration, the field name must specify the SAN (alt-subject-name) field. Match criteria should be "eq" for equal. SAN example: alt-subject-name eq <peer.cisco.com> The TOE will reject the IKE connection in any of these situations: 1) If the data ID Payload for any of those ID Types does not match the peer's certificate exactly; 2) If an ID Payload is not provided by the peer; 3) If multiple ID Types are provided in the ID Payload. When using pre-shared a key the TOE will reference the match identity setting as configured its own admin-defined settings to match the peer's IP address to the corresponding reference identifier.

TOE SFR	Component Implemented	Rationale
FCS_SSHS_EXT.1	WLC	The TSF implements SSHv2 conformant to RFCs 4251, 4252, 4253, 4254 4344, 5656, 6668, 8308 section 3, and 8332 to provide a secure command line interface for remote administration. The TOE supports public-key authentication with rsa-sha2-256 and rsa-sha2-512 public key algorithm and password-based authentication methods. SSHv2 connections will be dropped if the TOE receives a packet larger than 32,767 bytes. Large packets are detected by the SSHv2 implementation and dropped internal to the SSH process. The TSF's SSH transport implementation supports the following encryption algorithms: ■ aes128-cbc ■ aes256-cbc All connection attempts from remote SSH clients requesting any other encryption algorithm is denied. The TSF's SSH transport implementation supports the following MAC algorithms: ■ hmac-sha2-256 ■ hmac-sha2-512 All connection attempts from remote SSH clients requesting any other MAC algorithm is denied. The TSF's SSH transport implementation supports the following public-key algorithms for both Client Authentication and Hostkey authentication: ■ rsa-sha2-256 ■ rsa-sha2-512 When the SSH client presents a public key, the TSF verifies it matches the one configured for the Administrator account. If the presented public key does not match the one configured for the Administrator account, access is denied. The TSF's SSH key exchange implementation supports ecdh-sha2-nistp256, ecdh-sha2-nistp384, and ecdh-sha2-nistp521. The TSF's SSH implementation will perform a rekey after no longer than one hour or more than one gigabyte of data has been transmitted with the same session key. Both thresholds are checked. Rekeying is performed upon reaching whichever threshold is met first. The Administrator can configure lower rekey values if desired. The minimum time value is 10 minutes. The minimum volume value is 100 kilobytes.

FCS_DTLSS_EXT.1	WLC	The TSF implements DTLS 1.2 conformant to RFC 6347 supporting the following ciphersuites: ■ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 ■ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 ■ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 ■ TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246 ■ TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268 ■ TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268 Upon receiving the Client Hello message the WLC sends a Hello Verify Request message and performs a stateless cookie exchange to ensure the DTLS Client is not being spoofed. During internal channel communication between the AP and WLC, if there is a Message Authentication Code (MAC) verification failure, the WLC will silently discard the record and continue with the connection. The WLC will increment its DTLS packet error counter. DTLS Server key establishment is implemented as follows: ■ If DHE_RSA_* ciphersuites are configured, the WLC generates the Diffie-Hellman 2048 bit ephemeral key agreement parameters, prime ‘p’ and generator ‘g’ which has at a minimum a 112-bit level of security. The prime ‘p’ and generator ‘g’ parameters are transmitted to the client in the Server Key Exchange message on each connection attempt. ■ If TLS_ECDHE_* ciphersuites are configured, the secp384r1 NIST elliptic curve will be used by default. On each connection attempt, the Server Key Exchange message includes: 1) the NIST named curve which specifies predefined EC domain parameters; and 2) an ECDH public key corresponding to those parameters. The WLC enforces replay detection using sequence numbers. Valid record sequence numbers are maintained in a sliding window. For each record received, the TOE verifies if it is in the window boundary. Messages that are received where the same record was previously received or too old to fit in the sliding window are silently discarded. The TSF implements support for session resumption based on session IDs according to RFC 5246 (TLS1.2) using multiple contexts. The contexts are coordinated as follows: After the WLC successfully authenticates the AP, an internal trusted channel is established. This control channel protects the management traffic between a WLC and AP. When Enable Data DTLS is configured, as instructed in the Common Criteria Configuration Guide, a second channel is established using TLS session resumption. This data channel protects user data sent from the wireless client destined to the VLAN on the wired interface. The session resumption functions as follows: If the WLC determines there is a session ID match with the AP and the control channel session state is still valid, the WLC will proceed with an abbreviated handshake and send a Server Hello message with the matched Session ID. Both AP and WLC will then exchange ChangeCipherSpec and Finished messages. If the WLC determines there is not a Session ID match with the AP, the WLC requires a full TLS handshake to establish the data channel.

TOE SFR	Component Implemented	Rationale
		The DN is compared to the expected identifier as follows: The CC Configuration Guide requires the Security Administrator to maintain an AP authorization list on the WLC. The AP authorization list defines the APs that are permitted to join by identification of its unique serial number. If the serial number matches the subject Distinguished Name in the certificate presented by the AP, the components will proceed to implement an internal channel protected with DTLS. If it does not match an entry in the authorization list, the DTLS internal channel will not be established and the and the AP will not be able to join.
FCS_DTLSC_EXT.1	AP	The TSF implements DTLS 1.2 conformant to RFC 6347 supporting the following ciphersuites: ■ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 ■ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 ■ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 ■ TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246 ■ TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268 ■ TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268 When establishing a DTLS connection, the WLC TOE Component supports a reference identifier of type id-at-commonName per RFC 5280 Appendix A. The AP will establish its reference identifier through a "Gatekeeper" discovery process. Specifically, the AP will obtain the reference identifier from the "AC Name" field received from the CAPWAP Discovery Response packet and will seek a match to the contents of the CN field. If the AP TOE Component determines there is a mismatch in the presented identifier, the AP will not establish the DTLS trusted channel connection. The TOE does not support the use of wildcards within certificates and does not support certificate pinning. Use of an IP Address reference identifier in the CN field is not supported in the evaluated configuration. For DTLS 1.2 connections to the WLC TOE Component, the TSF presents secp256r1, secp384r1, and secp521r1 and no other curves in the Supported Group extension of the Client Hello. This behavior is implemented by default and is not configurable.

FCS_HTTPS_EXT.1 FCS_TLSS_EXT.1	WLC	The TSF implements HTTPS conformant to RFC 2818 to provide a secure interactive Web interface for remote administrative functions. The TLS Server implementation is conformant to RFC 5246 and supports TLS 1.2 with the following ciphersuites: ■ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 ■ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289 ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 ■ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 ■ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 ■ TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246 ■ TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246 ■ TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288 ■ TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288 ■ TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268 ■ TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268 Only TLS 1.2 is supported. All connection attempts from remote clients requesting SSL2.0, SSL3.0, TLS1.0, or TLS 1.1 are denied. For TLS Server key establishment, if TLS_ECDHE_* ciphersuites are configured, the Security Administrator has the ability to also configure one of the following named curves and inclusive key exchange parameter: ■ secp256r1 NIST curve with 256-bit ECDHE ephemeral key agreement parameter for server key exchange which has at a minimum a 128-bit level of security. ■ secp384r1 NIST curve with 384-bit ECDHE ephemeral key agreement parameter for server key exchange which has at a minimum a 192-bit level of security. If a named curve is not configured, the secp256r1 NIST elliptic curve will be used by default. On each connection attempt, the Server Key Exchange message includes: 1) the NIST named curve which specifies predefined EC domain parameters; and 2) an ECDH public key corresponding to those parameters. If TLS_RSA_WITH_AES_* ciphersuites are configured by the Security Administrator and selected by the TLS Server for use with HTTPS, there is no server key exchange message sent during the handshake phase. The TOE supports session resumption based on session tickets according to RFC 5077. The tickets adhere to the structural format provided in section 4 of RFC 5077. For FCS_TLSS_EXT.1, the TOE supports session resumption as a single context only. An encrypted session ticket containing the current session key information is sent by the TOE at the end of the TLS handshake. A web-client supporting session tickets will cache the ticket and may resume the earlier session by sending the encrypted session ticket in the handshake message. The TOE will decrypt the ticket, obtain the session key, and resume the session. Session tickets are encrypted using 128-bit AES in CBC mode, which is consistent with FCS_COP.1/DataEncryption.

TOE SFR	Component Implemented	Rationale
FCS_RADSEC_EXT.1 FCS_TLSC_EXT.1/ RADsec	WLC	The TSF implements RFC 6614 to provide secure TLS communication between itself and an external RADIUS server (RADsec). The TLS client implementation is conformant to RFC 5246 and supports TLS 1.2 with the following ciphersuites: ■ TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268 When establishing a TLS connection, the TOE supports reference identifiers of type DNS-ID and IP address and will seek a match to the DNS domain name or IP address respectively in the subjectAltName extension. If the TOE determines there is a mismatch in the presented identifier, it will not establish the TLS trusted channel connection. The TOE does not support the use of wildcards within certificates and does not support certificate pinning. For TLS 1.2 connections to the RADsec server, the TSF does not present the Supported Group Extension in the Client Hello. This behavior is implemented by default and is not configurable.
FCS_TLSC_EXT.1/EST	WLC	The TSF implements TLS 1.2 conformant to RFC 5246 to provide secure TLS communication between itself and an EST server supporting the following ciphersuites: ■ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 ■ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 ■ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 ■ TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288 ■ TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246 ■ TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288 ■ TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246 ■ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289 ■ TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288 ■ TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246 ■ TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288 ■ TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246 When establishing a TLS connection, the TOE supports reference identifiers of type DNS-ID and IP address and will seek a match to the DNS domain name or IP address respectively in the subjectAltName extension. If the TOE determines there is a mismatch in the presented identifier, it will not establish the TLS trusted channel connection. The TOE does not support the use of wildcards within certificates and does not support certificate pinning. For TLS 1.2 connections to the EST server, the TSF presents secp256r1, secp384r1, and secp521r1 and no other curves in the Supported Group extension of the Client Hello. This behavior is implemented by default and is not configurable.

TOE SFR	Component Implemented	Rationale
FCS_TLSC_EXT.2	WLC	The TOE supports TLS mutual authentication and will present a client certificate to the RADsec server and EST Server during connection establishment.
FIA_PMG_EXT.1	WLC	The WLC supports the local definition of users with corresponding passwords. The passwords can be composed of any combination of upper and lower case letters, numbers, and special characters that include: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)” and other special characters listed in table 18. Minimum password length is settable by the Authorized Administrator, and can be configured for minimum password lengths of 8 to 16 characters and maximum of 127 characters.
FIA_AFL.1	WLC	To block password-based brute force attacks, the TOE uses an internal AAA function to detect and track failed login attempts. When an account attempting to log into an administrative interface reaches the set maximum number of failed authentication attempts, the account will not be granted access until the time period has elapsed or until the Administrator manually unblocks the account. The TOE provides the Administrator the ability to specify the maximum number of unsuccessful authentication attempts before an offending account will be blocked. The TOE also provides the ability to specify the time period to block offending accounts. To avoid a potential situation where password failures made by Administrators leads to no Administrator access until the defined blocking time period has elapsed, the CC Configuration Guide instructs the Administrator to configure the Controller for SSH public key access, which is not subjected to password-based brute force attacks. During the block out period, the TOE provides the ability for the Administrator account to login remotely using SSH public key authentication.

TOE SFR	Component Implemented	Rationale
FIA_UIA_EXT.1 FIA_UAU_EXT.2	WLC	The WLC component requires all users to be successfully identified and authenticated before allowing any TSF mediated actions to be performed. The requirement applies to users of the Controllers who connect locally to the CLI via serial console or over SSH and HTTPS remote administrative interfaces. Administrative access to the TOE is facilitated through a local password-based authentication and SSH public key authentication mechanisms on the Controller through which all Administrator actions are mediated. Once a potential (unauthenticated) administrative user attempts to access the TOE through an interactive administrative interface (CLI or GUI), the TOE prompts the user for a user name and password or SSH public key authentication. No access is allowed to the administrative functionality of the TOE until the administrator is successfully identified and authenticated. After the end-user provides a username and authentication credentials the TOE grants administrative access (if credentials are valid, and the account has not been locked) or indicates that the login attempt was unsuccessful. At the CLI a successful login is indicated by a hash sign ("#") next to the device hostname. At the HTTPS Web GUI, a successful login is indicated by providing the Administrator with the default landing page, which is the Wireless Dashboard. Prior to authentication at each interactive administrative interfaces (CLI and GUI), the TOE may be configured by the Administrator to display a customized login banner, which describes restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the Controller. There are no local or remote management administrative interfaces directly available on the Access Points. Additionally, there are no unauthenticated services provided or supported. All administration of the APs are performed via the WLC. If an attempt is made to directly connect to the local serial port of the AP, it will respond with the following message: "Console disabled while in FIPS mode".
FIA_UAU.6	WLC	When an Administrator changes their own password, the TOE requires the administrator to re-enter the old/current password prior to changing the password.
FIA_UAU.7	WLC	When a user enters their password at the local CLI console, the TOE does not provide feedback in the password field and the TOE does not echo any characters back as the characters are entered.
FIA_PSK_EXT.1	WLC	The TOE supports use of pre-shared keys for authentication of IPsec peers between the WLC component and a remote syslog server. Pre-shared keys can be entered as ASCII characters and must be 22 characters long. Pre-shared keys can also be entered as HEX ("bit-based") values.

TOE SFR	Component Implemented	Rationale
FIA_X509_EXT.1/Rev	WLC	The TOE uses X.509v3 certificates to support authentication for IPsec and TLS connections. The TSF determines the validity of certificates by ensuring that the certificate and the certificate path are valid in accordance with RFC 5280. The certificate path is validated by ensuring that all the CA certificates have the basicConstraints extension and the CA flag is set to TRUE and the certificate path must terminate with a trusted CA certificate. The TOE ensures the extendedKeyUsage field includes: ■ The Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) for server certificates used in TLS. CRL revocation checking is supported by the TOE. Revocation checking is performed on the leaf and intermediate certificate(s) when authenticating a certificate chain provided by the remote peer. There are no functional differences if a full certificate chain or only a leaf certificate is presented.
FIA_X509_EXT.1/ITT	WLC	The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication of internal TOE entities. X.509v3 certificate validation is performed when the AP attempts to join the WLC. The AP will only be able to join the WLC and form a distributed TOE if the WLC determines the X.509v3 certificate of the AP is valid and the subject Distinguished Name field, which contains the AP's hardware serial number, matches an entry in the AP authorization list defined and maintained by the Security Administrator. The WLC will also verify the extendedKeyUsage field of the AP certificate contains the Client Authentication purpose.
FIA_X509_EXT.2	WLC, AP	The TOE determines which certificate to use based upon the trustpoint configured. The instructions for configuring trustpoints is provided in CC Configuration Guide. In the event that a network connection cannot be established to verify the revocation status of certificate for an external peer the connection will be rejected with the exception of certificate enrollment over TLS. For certificate enrollment over TLS, the TOE will accept the connection if a network connection cannot be established to verify the revocation status of the EST Server certificate. For internal TOE communication in accordance with FPT_ITT.1, certificate revocation checking is not performed.
FIA_X509_EXT.3	WLC, AP	A Certificate Request Message can be generated as specified by RFC 2986 and provide the following information in the request – CN, O, OU, and Country. The TOE can validate the chain of certificates from the Root CA when the CA Certificate Response is received.
FMT_MOF.1/ ManualUpdate	WLC, AP	The WLC and AP TOE components ensure only the authorized Administrator at the WLC may update the TOE software.

TOE SFR	Component Implemented	Rationale
FMT_MOF.1/ Services FMT_MOF.1/ Functions FMT_MTD.1/ CryptoKeys	WLC	The WLC provides all the capabilities necessary to centrally manage all TOE components. There is no remote trusted path administrative interface available directly on the Access Points. In addition, the TOE prohibits direct Access Point administration on the local console. Only the authorized Administrator on the WLC may: ■ Initiate manual updates of the TOE software; ■ Start and Stop Services; ■ Modify the security function behavior including: ○ Transmission of audit data to an external syslog server; ○ Enable or disable logging to the local audit log, or to the local console, or to remote syslog servers, and to display the configuration and status of audit functions. Some accounts may not have abilities to perform all functions. For example, user accounts may be configured with less than level 15 privilege. These accounts would not have the ability to enable, disable or modify security functional management behavior.
FMT_MTD.1/ CoreData	WLC, AP	The WLC and AP TOE components ensure all Admin functions including those functions that manage TSF data are mediated by the TOE which ensures there is no capability to manage TSF data at any administrative interface until an administrator is successfully identified and authenticated. In addition, the TOE ensures management of truststores (trustpoints) containing X.509 certificates is restricted to the authorized Administrator. User accounts with less than level 15 privilege do not have the ability to add or remove a truststore.

TOE SFR	Component Implemented	Rationale
FMT_SMF.1 FMT_MTD.1/ CryptoKeys	WLC	The Administrator can connect to the WLC to perform management functions via a directly connected console cable. The Administrator can also connect (from wired networks) remotely to the WLC over TLS/HTTPS or SSH to perform management functions. The WLC provides all the capabilities necessary to centrally manage the TOE including, but not limited to: ■ Local and remote administration of the TOE and the services provided by the TOE; ■ Configure an advisory notice and consent warning message to be displayed at login prior to gaining access to administrative functions; ■ Define the length of time that an administrative session can remain inactive before the session is terminated, and can configure serial console, SSH, and HTTPS with separate timeout limits; ■ Initiate updates of the TOE software; ■ Change the number of consecutive incorrect password attempts and the block out time duration; ■ Configure the cryptographic functionality; ■ Set the time and date; ■ Enable or disable logging to the local audit log, or to the local console, or to remote syslog servers, and to display the configuration; ■ Maintain an AP authorization list to allow the Administrator to configure the interaction between the WLC and APs and which APs are allowed to join. Refer to FCO_CPC_EXT.1 for further details.
FMT_SMR.1	WLC	Wireless clients do not have any administrative access to the TOE, and none of the administrative interfaces of the TOE are accessible from wireless clients. The TOE does not maintain admin roles for wireless clients/users, and the TOE maintains clear distinction between authenticated wireless clients and authenticated Administrators.
FMT_SMR.2	WLC	The TOE provides a local password-based authentication and SSH public key authentication mechanisms and requires all users to be successfully identified and authenticated before allowing any TSF mediated actions to be performed. The process for authentication is the same for the Administrator whether administration is occurring via a directly connected console cable or remotely via TLS/HTTPS or SSH. The Administrator is dependent upon having a level 15 privilege. A user without a level 15 privilege would not have the ability to enable, disable or modify security functional management behavior.
FPT_SKP_EXT.1	WLC, AP	The TOE is designed specifically to not disclose any keys stored in the TOE. The TOE stores all private keys in a secure directory that cannot be viewed or accessed, even by the Administrator. The TOE stores symmetric keys only in volatile memory. Pre-shared keys may be specified in the configuration file by the Administrator using a bit-based (hex) format. Only the Administrator may view the configuration file.

TOE SFR	Component Implemented	Rationale
FPT_APW_EXT.1	WLC	The TOE is designed specifically to not disclose any passwords stored in the TOE. All passwords are stored using a SHA-2 hash. 'Show' commands display only the hashed password. The CC Configuration Guide instructs the Administrator to use the `algorithm-type sha256 | scrypt` sub-command when passwords are created or updated. The SHA256 sub-command is password type 8 while scrypt is password type 9. Both password types uses SHA-2.
FPT_FLS.1	WLC, AP	If a critical failure occurs that results in the TOE ceasing operation, the TOE securely disables its interfaces to prevent the unintentional flow of any information and then will reload. If the failure persists the TOE will continue to reload. This functionally prevents any failure from causing an unauthorized information flow. There are no failures that circumvent this protection.
FPT_STM_EXT.1	WLC, AP	The TSF implements a clock function to provide a source of date and time. The clock function is reliant on the system clock provided by the underlying hardware. All controller models have a real-time clock (RTC) with battery to maintain time across reboots and power loss. APs synchronize their time with the WLC upon successfully joining. The TOE relies upon date and time information for the following security functions: ■ To deny establishment of connections from wireless clients based on a configured time restriction (FTA_TSE.1); ■ To monitor local and remote interactive administrative sessions for inactivity (FTA_SSL_EXT.1, FTA_SSL.3); ■ Validating X.509 certificates to determine if a certificate has expired (FIA_X509_EXT.1/Rev, FIA_X509_EXT.1/ITT); ■ To determine when SSH session keys have expired and to initiate a rekey (FCS_SSHS_EXT.1); ■ To determine when IKEv2 SA lifetimes have expired and to initiate a rekey (FCS_IPSEC_EXT.1); ■ To determine when IPsec Child SA lifetimes have expired and to initiate a rekey (FCS_IPSEC_EXT.1); ■ To provide accurate timestamps in audit records (FAU_GEN.1.2).

FPT_TST_EXT.1	WLC, AP	All TOE components (WLC and AP) run a suite of self-tests during initial start-up to verify correct operation of cryptographic modules. If any component reports failure for the POST, the system crashes and appropriate information is displayed on the local console. All ports are blocked from moving to forwarding state during the POST. If all components of all modules pass the POST, the system is placed in FIPS PASS state and ports are allowed to forward data traffic. If any of the tests fail, a message is displayed to the local console. During the system boot process (power on or reboot), all the Power on Startup Test (POST) components for all the cryptographic modules perform the POST for the corresponding component (hardware or software). These tests are sufficient to verify correct operation of cryptographic modules. These tests include: ■ AES Known Answer Test - For the encrypt test, a known key is used to encrypt a known plain text value resulting in an encrypted value. This encrypted value is compared to a known encrypted value to ensure that the encrypt operation is working correctly. The decrypt test is just the opposite. In this test a known key is used to decrypt a known encrypted value. The resulting plaintext value is compared to a known plaintext value to ensure that the decrypt operation is working correctly. ■ DRBG Known Answer Test - For this test, known seed values are provided to the DRBG implementation. The DRBG uses these values to generate random bits. These random bits are compared to known random bits to ensure that the DRBG is operating correctly. ■ SHA-1/256/512 Known Answer Test – For each of the values listed, the SHA implementation is fed known data and key. These values are used to generate a hash. This hash is compared to a known value to verify they match and the hash operations are operating correctly. ■ HMAC (HMAC-SHA-1/256/512) KATs - For each of the hash values listed, the HMAC implementation is fed known plaintext data and a known key. These values are used to generate a MAC. This MAC is compared to a known MAC to verify that the HMAC and hash operations are operating correctly. ■ Software Integrity Test - The Software Integrity Test is run automatically whenever the module is loaded and confirms the image has maintained its integrity. ■ ECDSA Signature Test – This test takes a known plaintext value and Private/Public key pair and used the public key to encrypt the data. This value is compared to a known encrypted value to verify that encrypt operation is working properly. The encrypted data is then decrypted using the private key. This value is compared to the original plaintext value to ensure the decrypt operation is working properly. At the request of the authorized administrator, the self-tests for the WLC component can be executed at any point after the image has been successfully loaded by executing the command: `test crypto self-test` All TOE components (WLC and AP) will automatically verify the integrity of the stored image when loaded for execution. The WLC uses a Cisco public key to validate the digital signature to obtain an embedded SHA512 hash that was generated prior to the image being distributed from Cisco. The WLC then computes its own hash of the image using the same

TOE SFR	Component Implemented	Rationale

		SHA512 algorithm. The WLC verifies the computed hash against the embedded hash. If they match the image is authenticated and has not been modified or tampered. If they do not match the image will not boot or execute.
		All hardware WLC appliances will display at bootup a message that the image was successfully validated:
		`“RSA Signed RELEASE Image Signature Verification Successful.”`
		After boot, the authorized administrator can also manually verify the digital signature by executing on the WLC:
		`verify bootflash:<image or package name>`
		The AP will perform a digital signature verification check on its stored image. When successfully validated the AP will display at bootup:
		`"Image signing verification success, continue to run…"`
		If integrity of the stored image is not successfully verified the image will not boot or execute.

TOE SFR	Component Implemented	Rationale

FPT_TUD_EXT.1	WLC, AP	To query the currently active software version, the Administrator will need to navigate to the Dashboard page and locate the version listed under the Controller model in the top left corner. Alternatively, the same information can be obtained by entering the following command at the CLI:
		`show version | include Cisco IOS XE Software`
		For the APs, the Security Administrator can query the currently active AP software version by navigating to Monitoring -> Wireless -> AP Statistics. Clicking on an AP Name will display general AP information including the software version. Alternatively, the Administrator can enter the following command at the CLI:
		`show ap image`
		The Administrator can download updates (new software images) appropriate for controller hardware. Software images are made available via Cisco.com.
		The WLC will authenticate the image using a digital signature verification check to ensure it has not been modified since distribution. The WLC uses the following process:
		Prior to being made publicly available, the software image is hashed using a SHA512 algorithm and then digitally signed. The digital signature is embedded to the image (hence the image is signed). The WLC uses a Cisco public key to validate the digital signature to obtain the SHA512 hash.
		The WLC then computes its own hash of the image using the same SHA512 algorithm. The WLC verifies the computed hash against the embedded hash. If they match the image has not been modified or tampered since distributed from Cisco meaning the software is authenticate. If they do not match the image will not install.
		AP software images are embedded in the WLC image and are not downloaded separately from Cisco.com. To keep software versions synchronized, after the WLC image has successfully transferred the CC Configuration Guide instructs the Administrator to download the AP image from the WLC image using a process termed AP preloading. The AP image is transferred over the DTLS protected internal channel and the AP will perform a digital signature verification check on the image it receives from the WLC.
		All images will not be active until the Administrator reboots the WLC as instructed in the CC Configuration Guide. When the WLC reboots the Access Points will automatically reboot.
		Prior to reboot, the Administrator can query the currently installed but not yet active WLC software version by entering the following command at the CLI:
		`show install inactive`
		For the APs Administrator can query the currently installed but not yet active AP image version by entering the following command at the CLI before pre-downloading the AP image:
		`show ap image`

FPT_ITT.1	WLC	The TOE includes two distinct types of components that use a secure network protocol for internal communication. When TSF data is transferred between APs and WLCs the data is protected from modification and disclosure using DTLS.

<table>
<tr><th>TOE SFR</th><th>Component Implemented</th><th>Rationale</th></tr>
<tr><td>FTA_SSL_EXT.1
FTA_SSL.3</td><td>WLC</td><td>The Administrator can configure maximum inactivity times individually for both local and remote administrative sessions. If either the local or remote administrative sessions are inactive for a configured period of time, the session will be terminated and will require re-authentication.

To configure the maximum inactivity time, the TOE provides the "exec-timeout" command for the CLI. For the HTTPS WebGUI, the TOE provides the ip http session-idle-timeout command. These settings are not immediately activated for the current session. When the user exits and logs back in, the inactivity timer will be activated for the new session.</td></tr>
<tr><td>FTA_SSL.4</td><td>WLC</td><td>The Administrator can terminate their own administrative sessions. The Administrator can logout of the Web GUI by clicking logout icon in the top-right corner of the page. The Administrator can logout of the CLI by entering the logout or exit command.</td></tr>
<tr><td>FTA_TAB.1</td><td>WLC</td><td>The Administrator can configure an access banner that describes restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the Controller. The banner will display on the local console port, SSH, and HTTPS interfaces prior to allowing any administrative access.</td></tr>
<tr><td>FTA_TSE.1</td><td>WLC</td><td>The Administrator can deny establishment of wireless client sessions based on SSID, time, day attributes. The SSID is the name for a wireless network defined by the Security Administrator. To deny based on time or day attributes, the Administrator from the WLC defines "calendar profile" and tags that to the "wireless profile policy". The wireless clients where the Administrator has applied the "wireless profile policy" are denied access to WLAN during the configured day and/or time.</td></tr>
<tr><td>FTP_ITC.1</td><td>WLC, AP</td><td>Components of the TOE uses secure protocols to provide trusted communications between itself and authorized IT entities as specified in the table below:
<table>
<tr><th>TOE Component</th><th>Acting as Client or Server</th><th>IT Entity</th><th>Secure Communication Mechanism/ Protocol</th><th>Non-TSF Endpoint Identification</th></tr>
<tr><td>WLC</td><td>Client</td><td>Syslog Server</td><td>IPsec</td><td>X.509 Certificate</td></tr>
<tr><td>WLC</td><td>Client</td><td>RADIUS Server</td><td>RADsec</td><td>X.509 Certificate</td></tr>
<tr><td>WLC</td><td>Client</td><td>RADIUS Server</td><td>IEEE 802.1X</td><td>X.509 Certificate</td></tr>
<tr><td>WLC</td><td>Client</td><td>EST Server</td><td>TLS</td><td>X.509 Certificate</td></tr>
<tr><td>AP</td><td>Server</td><td>Wireless Client</td><td>IEEE 802.11-2012 (WPA2)</td><td>IEEE 802.1X EAP-TLS</td></tr>
</table></td></tr>
<tr><td>FTP_TRP.1/Admin</td><td>WLC</td><td>All remote administrative communications take place over a secure encrypted SSHv2 (CLI) session or HTTPS (web-based GUI) session. Both SSHv2 and HTTPS sessions are protected using AES encryption. The remote users are able to initiate both HTTPS and SSHv2 communications with the TOE and is required to successfully authenticate and be authorized for the role of authorized Administrator before any remote administrative actions may be performed.</td></tr>
</table>

Key Zeroization

The table below describes the key zeroization referenced by FCS_CKM.4 provided by the TOE

Table 22. Key Zeroization

Key	Description	Storage Location	Zeroization Method
Diffie-Hellman Shared Secret	The shared secret used in Diffie-Hellman (DH) exchange. Created per the Diffie-Hellman Exchange.	SDRAM	Overwritten automatically with 0x00 when the IPsec trusted channel is no longer in use.
Diffie Hellman private key	The private key used in Diffie-Hellman (DH) Exchange	SDRAM	Overwritten automatically with 0x00 when the IPsec trusted channel is no longer in use.
Skey_id	IKE SA key from which Phase2/Child IPsec keys are derived.	SDRAM	Overwritten automatically with 0x00 when the IPsec trusted channel is no longer in use.
IKE session encrypt key	Used for IKE payload protection	SDRAM	Overwritten automatically with 0x00 when the IPsec trusted channel is no longer in use.
IKE session authentication key	Used for IKE payload integrity verification	SDRAM	Overwritten automatically with 0x00 when the IPsec trusted channel is no longer in use.
IKE Preshared key	This shared secret was manually entered for IKE pre-shared key based authentication used to authenticate the peer	SDRAM	Overwritten automatically with 0x00 when the IPsec trusted channel is no longer in use.
		NVRAM	Overwritten with a new value of the key. # pre-shared-key <key value>
IPsec encryption key	Used to secure IPsec traffic	SDRAM	Overwritten automatically with 0x00 when the IPsec trusted channel is no longer in use.
IPsec authentication key	Used to authenticate the IPsec peer	SDRAM	Overwritten automatically with 0x00 when the IPsec trusted channel is no longer in use.
SSH Session Key	Used to encrypt SSH traffic	SDRAM	Overwritten automatically with 0x00 when the SSH trusted channel is no longer in use.
SSH Private Key	Used in establishing a secure SSH session	NVRAM	Overwritten with 0x00 by using the following command: #crypto key zeroize <label>

Key	Description	Storage Location	Zeroization Method
HTTPS TLS Pre-Master secret	Shared secret created using asymmetric cryptography from which new HTTPS session keys can be created.	SDRAM	Overwritten automatically with 0x00 when the HTTPS session is no longer in use.
HTTPS TLS Encryption Key	HTTPS TLS Encryption Key	SDRAM	Overwritten automatically with 0x00 when the HTTPS session is no longer in use.
HTTPS TLS Integrity Key	Used for HTTPS integrity protection	SDRAM	Overwritten automatically with 0x00 when the HTTPS session is no longer in use.
HTTPS Private Key	Used in establishing a secure HTTPS session	NVRAM	Overwritten with 0x00 by using the following command: #crypto key zeroize <label>
RADIUS Preshared key	This shared secret was manually entered for RADIUS pre-shared key based authentication used to authenticate the RADIUS Server.	SDRAM	Overwritten automatically with 0x00 when RADIUS is no longer in use.
		NVRAM	Overwritten with a new value of the key. (config-radius-server)# key <key value>
TLS Pre-Master secret	Shared secret created using asymmetric cryptography from which new TLS session keys can be created.	SDRAM	Overwritten automatically with 0x00 when the TLS session is no longer in use.
TLS Encryption Key	TLS Encryption Key	SDRAM	Overwritten automatically with 0x00 when the TLS session is no longer in use.
TLS Integrity Key	Used for TLS integrity protection	SDRAM	Overwritten automatically with 0x00 when the TLS session is no longer in use.
TLS Private Key	Used in establishing a secure TLS session	NVRAM	Overwritten with 0x00 by using the following command: #crypto key zeroize <label>
DTLS Pre-Master Secret	Used to derive the DTLS Encryption/Decryption Key and DTLS Integrity Key.	SDRAM	Overwritten automatically with 0x00 when the DTLS session is no longer in use.
DTLS Encryption/Decryption Key (CAPWAP session keys)	Session Keys used to encrypt/decrypt CAPWAP control messages.	SDRAM	Overwritten automatically with 0x00 when the DTLS session is no longer in use.

Key	Description	Storage Location	Zeroization Method
DTLS Integrity Key	This key is used for integrity checks on CAPWAP control messages.	SDRAM	Overwritten automatically with 0x00 when the DTLS session is no longer in use.

DTLS Private Key	Used in establishing a secure DTLS session	NVRAM	`Overwritten with 0x00 by using the following command:`
			`#crypto key zeroize <label>`

802.11i Key Confirmation Key (KCK)	The KCK is used by IEEE 802.11i to provide data origin authenticity in the 4-Way Handshake and Group Key Handshake messages.	SDRAM	Overwritten with a new value of the key. Zeroized on Power Cycle
802.11i Key Encryption Key (KEK)	The KEK is used by the EAPOL-Key frames to provide confidentiality in the 4-Way Handshake and Group Key Handshake messages.	SDRAM	Overwritten with a new value of the key. Zeroized on Power Cycle
802.11i Pairwise Transient Key (PTK)	The PTK is the 802.11i session key for unicast communications. This key is generated in the module by calling FIPS approved DRBG and then is transported into the Access Point (AP) protected by DTLS Encryption/Decryption Key. The Access Point (AP) uses this key with AES-CCM function to implement 802.11i unicast communications service.	SDRAM	Overwritten with a new value of the key. Zeroized on Power Cycle
802.11i Group Temporal Key (GTK)	The GTK is the 802.11i session key for broadcast communications. This key is generated in the module by calling FIPS approved DRBG and then is transported into the Access Point (AP) protected by DTLS Encryption/Decryption Key. The Access Point (AP) uses this key with AES-CCM function to implement 802.11i broadcast communications service.	SDRAM	Overwritten with a new value of the key. Zeroized on Power Cycle

CAVP Certificates

The table below lists the CAVP certificates for the TOE

Table 23. CAVP Certificates

TOE Component	SFR	Selection	Algorithm	Implementation	Certificate Number
IW6300 ESW6300 AP 1562 AP 2802 AP 3802 AP 4800	FCS_CKM.1/KeyGen – Cryptographic Key Generation	P-256 P-384	ECDSA	CiscoSSL FOM	A2452
	FCS_COP.1/SigGen – Cryptographic Operation (Signature Generation and Verification)				
IW6300 ESW6300 AP 1562 AP 2802 AP 3802 AP 4800	FCS_CKM.1/KeyGen – Cryptographic Key Generation	2048 3072	RSA	CiscoSSL FOM	A2452
	FCS_COP.1/SigGen – Cryptographic Operation (Signature Generation and Verification)				
IW6300 ESW6300 AP 1562 AP 2802 AP 3802 AP 4800	FCS_CKM.1/WPA2 – Cryptographic Key Generation (Symmetric Keys for WPA2 Connections)	PRF-384 - IEEE 802.11-2012 PRF-704 - IEEE 802.11ac-2013	HMAC	CiscoSSL FOM	A2452
IW6300 ESW6300 AP 1562 AP 2802 AP 3802 AP4800	FCS_CKM.2/KeyEst – Cryptographic Key Establishment	P-256 P-384 P-521	KAS-ECC	CiscoSSL FOM	A2452
IW6300 ESW6300 AP 1562 AP 2802 AP 3802 AP4800	FCS_CKM.2/KeyEst – Cryptographic Key Establishment		KAS-FFC	CiscoSSL FOM	A2452
IW6300 ESW6300 AP 1562 AP 2802 AP 3802 AP4800	FCS_CKM.2/GTK – Cryptographic Key Distribution (GTK)	AES-KW	AES	CiscoSSL FOM	A2452
		HMAC-SHA1	HMAC	CiscoSSL FOM	A2452
IW6300 ESW6300 AP 1562 AP 2802 AP 3802 AP 4800	FCS_COP.1/DataEncryption – AES Data Encryption/Decryption	AES-CBC-128 AES-CBC-256 AES-GCM-128 AES-GCM-256	AES	CiscoSSL FOM	A2452

TOE Component	SFR	Selection	Algorithm	Implementation	Certificate Number
IW6300 ESW6300 AP 1562 AP 2802 AP 3802 AP 4800	FCS_COP.1/DataEncryption – AES Data Encryption/Decryption	AES-CCMP-128 AES-CCMP-256 AES-GCMP-128 AES-GCMP-256	AES	Marvell Radio Chipset - 88W8964C	AES 4114
IW6300 ESW6300 AP 1562 AP 2802 AP 3802 AP 4800	FCS_COP.1/Hash – Cryptographic Operation (Hash Algorithm)	SHA-256 SHA-384	SHS	CiscoSSL FOM	A2452
IW6300 ESW6300 AP 1562 AP 2802 AP 3802 AP 4800	FCS_COP.1/KeyedHash – Cryptographic Operation (Keyed Hash Algorithm)	HMAC-SHA-256 HMAC-SHA-384	HMAC	CiscoSSL FOM	A2452
IW6300 ESW6300 AP 1562 AP 2802 AP 3802 AP 4800	FCS_RBG_EXT.1– Random Bit Generation	CTR_DRBG (AES)	DRBG	CiscoSSL FOM	A2452
Catalyst 9130	FCS_CKM.1/KeyGen – Cryptographic Key Generation	P-256 P-384	ECDSA	CiscoSSL FOM	A877
Catalyst 9130	FCS_COP.1/SigGen – Cryptographic Operation (Signature Generation and Verification)				
Catalyst 9130	FCS_COP.1/SigGen – Cryptographic Operation (Signature Generation and Verification)	2048 3072	RSA	CiscoSSL FOM	A877
Catalyst 9130	FCS_CKM.1/WPA2 – Cryptographic Key Generation (Symmetric Keys for WPA2 Connections)	PRF-384 - IEEE 802.11-2012 PRF-704 - IEEE 802.11ac-2013	HMAC	CiscoSSL FOM	A877
Catalyst 9130	FCS_CKM.2/KeyEst – Cryptographic Key Establishment	P-256 P-384 P-521	KAS-ECC	CiscoSSL FOM	A877

TOE Component	SFR	Selection	Algorithm	Implementation	Certificate Number
Catalyst 9130	FCS_CKM.2/KeyEst – Cryptographic Key Establishment		KAS-FFC	CiscoSSL FOM	A877
Catalyst 9130	FCS_CKM.2/GTK – Cryptographic Key Distribution (GTK)	AES-KW	AES	CiscoSSL FOM	A877
		HMAC-SHA1	HMAC	CiscoSSL FOM	A877
Catalyst 9130	FCS_COP.1/DataEncryption – AES Data Encryption/Decryption	AES-CBC-128 AES-CBC-256 AES-GCM-128 AES-GCM-256	AES	CiscoSSL FOM	A877
Catalyst 9130	FCS_COP.1/DataEncryption – AES Data Encryption/Decryption	AES-CCMP-128 AES-CCMP-256 AES-GCMP-128 AES-GCMP-256	AES	Qualcomm Radio Chipset	AES 5663
Catalyst 9130	FCS_COP.1/Hash – Cryptographic Operation (Hash Algorithm)	SHA-256 SHA-384	SHS	CiscoSSL FOM	A877
Catalyst 9130	FCS_COP.1/KeyedHash – Cryptographic Operation (Keyed Hash Algorithm)	HMAC-SHA-256 HMAC-SHA-384	HMAC	CiscoSSL FOM	A877
Catalyst 9130	FCS_RBG_EXT.1– Random Bit Generation	CTR_DRBG (AES)	DRBG	CiscoSSL FOM	A877
Catalyst 9115 Catalyst 9120	FCS_CKM.1/KeyGen – Cryptographic Key Generation	P-256 P-384	ECDSA	CiscoSSL FOM	A877
Catalyst 9115 Catalyst 9120	FCS_COP.1/SigGen – Cryptographic Operation (Signature Generation and Verification)				
Catalyst 9115 Catalyst 9120	FCS_COP.1/SigGen – Cryptographic Operation (Signature Generation and Verification)	2048 3072	RSA	CiscoSSL FOM	A877
Catalyst 9115 Catalyst 9120	FCS_CKM.1/WPA2 – Cryptographic Key Generation (Symmetric Keys for WPA2 Connections)	PRF-384 - IEEE 802.11-2012 PRF-704 - IEEE 802.11ac-2013	HMAC	CiscoSSL FOM	A877

TOE Component	SFR	Selection	Algorithm	Implementation	Certificate Number
Catalyst 9115 Catalyst 9120	FCS_CKM.2/KeyEst – Cryptographic Key Establishment	P-256 P-384 P-521	KAS-ECC	CiscoSSL FOM	A877
Catalyst 9115 Catalyst 9120	FCS_CKM.2/KeyEst – Cryptographic Key Establishment		KAS-FFC	CiscoSSL FOM	A877
Catalyst 9115 Catalyst 9120	FCS_CKM.2/GTK – Cryptographic Key Distribution (GTK)	AES-KW	AES	CiscoSSL FOM	A877
		HMAC-SHA1	HMAC	CiscoSSL FOM	A877
Catalyst 9115 Catalyst 9120	FCS_COP.1/DataEncryption – AES Data Encryption/Decryption	AES-CBC-128 AES-CBC-256 AES-GCM-128 AES-GCM-256	AES	CiscoSSL FOM	A877
Catalyst 9115 Catalyst 9120	FCS_COP.1/DataEncryption – AES Data Encryption/Decryption	AES-CCMP-128 AES-CCMP-256 AES-GCMP-128 AES-GCMP-256	AES	Broadcom Radio Chipset	C1273
Catalyst 9115 Catalyst 9120	FCS_COP.1/Hash – Cryptographic Operation (Hash Algorithm)	SHA-256 SHA-384	SHS	CiscoSSL FOM	A877
Catalyst 9115 Catalyst 9120	FCS_COP.1/KeyedHash – Cryptographic Operation (Keyed Hash Algorithm)	HMAC-SHA-256 HMAC-SHA-384	HMAC	CiscoSSL FOM	A877
Catalyst 9115 Catalyst 9120	FCS_RBG_EXT.1– Random Bit Generation	CTR_DRBG (AES)	DRBG	CiscoSSL FOM	A877
Catalyst 9105	FCS_CKM.1/KeyGen – Cryptographic Key Generation	P-256 P-384	ECDSA	CiscoSSL FOM	A877
Catalyst 9105	FCS_COP.1/SigGen – Cryptographic Operation (Signature Generation and Verification)				
Catalyst 9105	FCS_COP.1/SigGen – Cryptographic Operation (Signature Generation and Verification)	2048 3072	RSA	CiscoSSL FOM	A877

TOE Component	SFR	Selection	Algorithm	Implementation	Certificate Number
Catalyst 9105	FCS_CKM.1/WPA2 – Cryptographic Key Generation (Symmetric Keys for WPA2 Connections)	PRF-384 - IEEE 802.11-2012 PRF-704 - IEEE 802.11ac-2013	HMAC	CiscoSSL FOM	A877
Catalyst 9105	FCS_CKM.2/KeyEst – Cryptographic Key Establishment	P-256 P-384 P-521	KAS-ECC KAS-FFC	CiscoSSL FOM	A877
Catalyst 9105	FCS_CKM.2/KeyEst – Cryptographic Key Establishment		KAS-ECC KAS-FFC	CiscoSSL FOM	A877
Catalyst 9105	FCS_CKM.2/GTK – Cryptographic Key Distribution (GTK)	AES-KW	AES	CiscoSSL FOM	A877
		HMAC-SHA1	HMAC	CiscoSSL FOM	A877
Catalyst 9105	FCS_COP.1/DataEncryption – AES Data Encryption/Decryption	AES-CBC-128 AES-CBC-256 AES-GCM-128 AES-GCM-256	AES	CiscoSSL FOM	A877
Catalyst 9105	FCS_COP.1/DataEncryption – AES Data Encryption/Decryption	AES-CCMP-128 AES-CCMP-256 AES-GCMP-128 AES-GCMP-256	AES	Broadcom Radio Chipset	C1275
Catalyst 9105	FCS_COP.1/Hash – Cryptographic Operation (Hash Algorithm)	SHA-256 SHA-384	SHS	CiscoSSL FOM	A877
Catalyst 9105	FCS_COP.1/KeyedHash – Cryptographic Operation (Keyed Hash Algorithm)	HMAC-SHA-256 HMAC-SHA-384	HMAC	CiscoSSL FOM	A877
Catalyst 9105	FCS_RBG_EXT.1– Random Bit Generation	CTR_DRBG (AES)	DRBG	CiscoSSL FOM	A877
Catalyst 9800-80 Catalyst 9800-40 Catalyst 9800-L Catalyst 9800-CL	FCS_CKM.1/KeyGen – Crypto-graphic Key Generation	P-256 P-384	ECDSA	CiscoSSL FOM IC2M	A2452 A1462
	FCS_COP.1/SigGen – Cryptographic Operation (Signature Generation and Verification)				

TOE Component	SFR	Selection	Algorithm	Implementation	Certificate Number
Catalyst 9800-80 Catalyst 9800-40 Catalyst 9800-L Catalyst 9800-CL	FCS_CKM.1/KeyGen – Cryptographic Key Generation	2048 3072	RSA	CiscoSSL FOM IC2M	A2452 A1462
	FCS_COP.1/SigGen – Cryptographic Operation (Signature Generation and Verification)				
Catalyst 9800-80 Catalyst 9800-40 Catalyst 9800-L Catalyst 9800-CL	FCS_CKM.1/WPA2 – Cryptographic Key Generation (Symmetric Keys for WPA2 Connections)	PRF-384 - IEEE 802.11-2012 PRF-704 - IEEE 802.11ac-2013	HMAC	CiscoSSL FOM IC2M	A2452 A1462
Catalyst 9800-80 Catalyst 9800-40 Catalyst 9800-L Catalyst 9800-CL	FCS_CKM.2/KeyEst – Cryptographic Key Establishment	P-256 P-384 P-521	KAS-ECC	CiscoSSL FOM IC2M	A2452 A1462
Catalyst 9800-80 Catalyst 9800-40 Catalyst 9800-L Catalyst 9800-CL	FCS_CKM.2/KeyEst – Cryptographic Key Establishment		KAS-FFC	CiscoSSL FOM IC2M	A2452 A1462
Catalyst 9800-80 Catalyst 9800-40 Catalyst 9800-L Catalyst 9800-CL	FCS_CKM.2/GTK – Cryptographic Key Distribution (GTK)	AES-KW	AES	CiscoSSL FOM IC2M	A2452 A1462
Catalyst 9800-80 Catalyst 9800-40 Catalyst 9800-L Catalyst 9800-CL		HMAC-SHA1	HMAC	CiscoSSL FOM IC2M	A2452 A1462
Catalyst 9800-80 Catalyst 9800-40 Catalyst 9800-L Catalyst 9800-CL	FCS_COP.1/DataEncryption – AES Data Encryption/Decryption	AES-CBC-128 AES-CBC-256 AES-GCM-128 AES-GCM-256	AES	CiscoSSL FOM IC2M	A2452 A1462
Catalyst 9800-80 Catalyst 9800-40 Catalyst 9800-L Catalyst 9800-CL	FCS_COP.1/Hash – Cryptographic Operation (Hash Algorithm	SHA-256 SHA-384 SHA-512	SHS	CiscoSSL FOM IC2M	A2452 A1462
Catalyst 9800-80 Catalyst 9800-40 Catalyst 9800-L Catalyst 9800-CL	FCS_COP.1/KeyedHash – Cryptographic Operation (Keyed Hash Algorithm)	HMAC-SHA-256 HMAC-SHA-384 HMAC-SHA-512	HMAC	CiscoSSL FOM IC2M	A2452 A1462
Catalyst 9800-80 Catalyst 9800-40 Catalyst 9800-L Catalyst 9800-CL	FCS_RBG_EXT.1 – Random Bit Generation	CTR_DRBG (AES)	DRBG	CiscoSSL FOM IC2M	A2452 A1462

Wi-Fi Alliance Certificates

The table below lists the Wi-Fi Alliance certificates for the TOE

Table 24. Wi-Fi Alliance Certificates

Product	Certification
Cisco Catalyst 9800-80 Wireless Controller and Cisco C9130AX AP	WFA98109
Cisco Catalyst 9800-80 Wireless Controller and Cisco C9120AX AP	WFA98120
Cisco Catalyst 9800-80 Wireless Controller and Cisco C9115AX AP	WFA98113
Cisco Catalyst 9800-80 Wireless Controller and Cisco C9105AX AP	WFA100774
Cisco Catalyst 9800-80 Wireless Controller and Cisco Aironet 1560 Series AP	WFA97683
Cisco Catalyst 9800-80 Wireless Controller and Cisco Aironet 4800 Series AP	WFA97651
Cisco Catalyst 9800-80 Wireless Controller and Cisco Aironet 3800 Series AP	WFA97641
Cisco Catalyst 9800-80 Wireless Controller and Cisco Aironet 2800 Series AP	WFA97646
Cisco Catalyst 9800-80 Wireless Controller and Cisco Catalyst Industrial Wireless 6300 Series AP	WFA98227
Cisco Catalyst 9800-80 Wireless Controller and Cisco 6300 Series Embedded Services AP	WFA98232
Cisco Catalyst 9800-40 Wireless Controller and Cisco C9130AX AP	WFA98108
Cisco Catalyst 9800-40 Wireless Controller and Cisco C9120AX AP	WFA98119
Cisco Catalyst 9800-40 Wireless Controller and Cisco C9115AX AP	WFA98112
Cisco Catalyst 9800-40 Wireless Controller and Cisco C9105AX AP	WFA100773
Cisco Catalyst 9800-40 Wireless Controller and Cisco Aironet 1560 Series AP	WFA97655
Cisco Catalyst 9800-40 Wireless Controller and Cisco Aironet 4800 Series AP	WFA97650
Cisco Catalyst 9800-40 Wireless Controller and Cisco Aironet 3800 Series AP	WFA97640
Cisco Catalyst 9800-40 Wireless Controller and Cisco Aironet 2800 Series AP	WFA97645
Cisco Catalyst 9800-40 Wireless Controller and Cisco Catalyst Industrial Wireless 6300 Series AP	WFA98226
Cisco Catalyst 9800-40 Wireless Controller and Cisco 6300 Series Embedded Services AP	WFA98231
Cisco Catalyst 9800-L Wireless Controller and Cisco C9130AX AP	WFA97958
Cisco Catalyst 9800-L Wireless Controller and Cisco C9120AX AP	WFA98117
Cisco Catalyst 9800-L Wireless Controller and Cisco C9115AX AP	WFA97959
Cisco Catalyst 9800-L Wireless Controller and Cisco C9105AX AP	WFA100294
Cisco Catalyst 9800-L Wireless Controller and Cisco Aironet 1560 Series AP	WFA97654
Cisco Catalyst 9800-L Wireless Controller and Cisco Aironet 4800 Series AP	WFA97649
Cisco Catalyst 9800-L Wireless Controller and Cisco Aironet 3800 Series AP	WFA97429
Cisco Catalyst 9800-L Wireless Controller and Cisco Aironet 2800 Series AP	WFA97644
Cisco Catalyst 9800-L Wireless Controller and Cisco Catalyst Industrial Wireless 6300 Series AP	WFA98225

Product	Certification
Cisco Catalyst 9800-L Wireless Controller and Cisco 6300 Series Embedded Services AP	WFA98230
Cisco Catalyst 9800 Cloud Wireless Controller and Cisco C9130AX AP	WFA98110
Cisco Catalyst 9800 Cloud Wireless Controller and Cisco C9120AX AP	WFA98121
Cisco Catalyst 9800 Cloud Wireless Controller and Cisco C9115AX AP	WFA98114
Cisco Catalyst 9800 Cloud Wireless Controller and Cisco C9105AX AP	WFA100775
Cisco Catalyst 9800 Cloud Wireless Controller and Cisco Aironet 1560 Series AP	WFA97684
Cisco Catalyst 9800 Cloud Wireless Controller and Cisco Aironet 4800 Series AP	WFA97652
Cisco Catalyst 9800 Cloud Wireless Controller and Cisco Aironet 3800 Series AP	WFA97642
Cisco Catalyst 9800 Cloud Wireless Controller and Cisco Aironet 2800 Series AP	WFA97647
Cisco Catalyst 9800-CL Wireless Controller and Cisco Catalyst Industrial Wireless 6300 Series AP	WFA98228
Cisco Catalyst 9800-CL Wireless Controller and Cisco 6300 Series Embedded Services AP	WFA98233

Auditing

Auditing allows Security Administrators to discover intentional and unintentional issues with the TOE's configuration and/or operation. Auditing of administrative activities provides information that may be used to hasten corrective action should the system be configured incorrectly. Security audit data can also provide an indication of failure of critical portions of the TOE (e.g. a communication channel failure or anomalous activity (e.g. establishment of an administrative session at a suspicious time, repeated failures to establish sessions or authenticate to the TOE) of a suspicious nature.

The TOE generates an audit record whenever an audited event occurs. The types of events that cause audit records to be generated include, cryptography related events, identification and authentication related events, and administrative events (the specific events and the contents of each audit record are listed in the table below). Each of the events is specified in enough detail to identify the user for which the event is associated, when the event occurred, where the event occurred, the outcome of the event, and the type of event that occurred.

The table below provides an auditable event to TOE component mapping.

Table 25. TOE Component Audit Event Mapping

SFR	Component	Auditable Event
FAU_GEN.1.1a	WLC	Startup and Shutdown of Audit Function
FAU_GEN.1.1.c	WLC	Administrative login and logout
FAU_GEN.1.1.c	WLC	Changes to TSF data related to configuration changes:
		■ Password Reset
		■ Importing certificates into the TOE's trust store
		■ Designating X509.v3 certificates as trust anchors

		■ Adding a TOE Access Banner
		■ Setting the Time
FAU_GEN.1.1.c	WLC	Generating/import of, changing, or deleting of cryptographic keys.
FAU_GEN.1.1.c	WLC	Resetting passwords
FAU_GEN.1.1.c	WLC	Starting and stopping services
FCO_CPC_EXT.1	WLC	Enabling communications between a pair of components. Disabling communications between a pair of components.
FCS_IPSEC_EXT.1	WLC	Protocol failures. Establishment/Termination of an IPsec SA.
FCS_DTLSS_EXT.1	WLC	Failure to establish a DTLS session; Reason for failure Detected replay attacks; Identity (e.g., source IP address) of the source of the replay attack.
FCS_DTLSC_EXT.1	AP	Failure to establish a DTLS session; Reason for failure
FCS_SSHS_EXT.1	WLC	Failure to establish an SSH session; Reason for failure
FCS_HTTPS_EXT.1 FCS_TLSS_EXT.1	WLC	Failure to establish a HTTPS Session; Reason for failure Failure to establish a TLS Session; Reason for failure
FCS_TLSC_EXT.1/RADsec	WLC	Failure to establish a TLS Session; Reason for failure
FCS_TLSC_EXT.1/EST	WLC	Failure to establish a TLS Session; Reason for failure
FIA_AFL.1	WLC	Unsuccessful login attempts limit is met or exceeded. The reaching of the threshold for the unsuccessful authentication attempts and the actions taken (e.g, disabling of an account) and the subsequent, if appropriate, restoration to the normal state (e.g., re-enabling of a terminal).
FIA_UIA_EXT.1 FIA_UAU_EXT.2	WLC	All use of the authentication mechanism.
FIA_UAU.6	WLC	Attempts to re-authenticate; Origin of the attempt
FIA_8021X_EXT.1	WLC	Attempts to access to the 802.1X controlled port prior to successful completion of the authentication exchange.
FIA_X509_EXT.1/Rev	WLC	Unsuccessful attempt to validate a certificate
		Any addition, replacement or removal of trust anchors in the TOE's trust store

FIA_X509_EXT.1/ITT	WLC	Unsuccessful attempt to validate a certificate
		Any addition, replacement or removal of trust anchors in the TOE's trust store
FMT_MOF.1/ ManualUpdate	WLC, AP	Any attempt to initiate a manual update
FMT_SMF.1	WLC	All management activities of TSF data.
FPT_FLS.1	WLC, AP	Failure of the TSF and the type of failure that occurred.
FPT_ITT.1	WLC	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.
FPT_STM_EXT.1	WLC, AP	Discontinuous changes to time - either Administrator actuated or changed via an automated process.
FPT_TST_EXT.1	WLC, AP	Execution of this set of TSF-self-tests. Detected integrity violations.
FPT_TUD_EXT.1	WLC, AP	Initiation of update. result of the update attempt (success or failure)
FTA_SSL_EXT.1	WLC	The termination of a local session by the session locking mechanism.
FTA_SSL.3	WLC	The termination of a remote session by the session locking mechanism.
FTA_SSL.4	WLC	The termination of an interactive session.
FTA_TSE.1	WLC	Denial of a session establishment due to the session establishment mechanism.
FTP_ITC.1	WLC, AP	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions (including IEEE 802.11).
FTP_TRP.1/Admin	WLC	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.

Extended Components Definition

Extended Components – WLAN_EP

The [WLAN_EP] does not provide an extended components definition. The following is drawn from extended SFRs defined [WLAN_EP].

FCS_RADSEC_EXT.1 – RADsec

FCS_RADSEC_EXT.1.1 – The TSF shall implement RADIUS over TLS as specified in RFC 6614 to communicate securely with a RADIUS server.

FCS_RADSEC_EXT.1.2 – The TSF shall perform peer authentication using [selection: X.509v3 certificates, pre-shared keys].

Application Note: If X.509v3 certificates is selected, then FCS_TLSC_EXT.2 from Appendix B of the Network Device collaborative Protection Profile must be included in the ST.

If pre-shared keys is selected, then FCS_RADSEC_EXT.2 must be included in the ST.

FIA_8021X_EXT.1 – Extended: 802.1X Port Access Entity (Authenticator) Authentication

FIA_8021X_EXT.1.1 The TSF shall conform to IEEE Standard 802.1X for a Port Access Entity (PAE) in the “Authenticator” role.

FIA_8021X_EXT.1.2 The TSF shall support communications to a RADIUS authentication server conforming to RFCs 2865 and 3579.

FIA_8021X_EXT.1.3 The TSF shall ensure that no access to its 802.1X controlled port is given to the wireless client prior to successful completion of this authentication exchange.

Application Note: This requirement covers the TOE's role as the authenticator in an 802.1X authentication exchange. If the exchange is completed successfully, the TOE will obtain the PMK from the RADIUS server and perform the 4-way handshake with the wireless client (supplicant) to begin 802.11 communications.

As indicated previously, there are at least three communication paths present during the exchange; two with the TOE as an endpoint and one with TOE acting as a transfer point only. The TOE establishes an EAP over LAN (EAPOL) connection with the wireless client as specified in 802.1X-2007. The TOE also establishes (or has established) a RADIUS protocol connection (which is tunneled inside of an IPsec connection) with the RADIUS server. The wireless client and RADIUS server establish an EAP-TLS session (RFC 5216); in this transaction the TOE merely takes the EAP-TLS packets from its EAPOL/RADIUS endpoint and transfers them to the other endpoint. Because the specific authentication method (TLS in this case) is opaque to the TOE, there are no requirements with respect to RFC 5126 in this EP. However, the base RADIUS protocol (2865) has an update (3579) that will need to be addressed in the implementation and assurance activities. Additionally, RFC 5080 contains implementation issues that will need to be addressed by developers, but which levy no new requirements.

The point of performing 802.1X authentication is to provide access to the network (assuming the authentication was successful and that all 802.11 negotiations are performed successfully); in the terminology of 802.1X, this means the wireless client has access to the "controlled port" maintained by the TOE.

FIA_PSK_EXT.1 – Extended: Pre-Shared Key Composition

FIA_PSK_EXT.1.1 The TSF shall be able to use pre-shared keys for [**selection: RADIUS over TLS, IPSEC**] and [selection: IEEE 802.11 WPA2-PSK, [assignment: other protocols that use pre-shared keys], no other protocols].

FIA_PSK_EXT.1.2 The TSF shall be able to accept text-based pre-shared keys that:

- are 22 characters and [selection: [assignment: *other supported lengths*], no other lengths];
- composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”).

FIA_PSK_EXT.1.3 The TSF shall be able to [selection: accept, generate using the random bit generator specified in FCS_RBG_EXT.1] bit-based pre-shared keys.

Application Note: This requirement shall be included if IPsec or another protocol that uses pre-shared Keys is claimed, and pre-shared key authentication is selected. In the second selection, if other protocols can use pre-shared keys, they should be listed in the assignment as well; otherwise "no other protocols" should be chosen. The intent of this requirement is that all protocols will support both text-based and bit-based pre-shared keys. If other lengths are supported they should be listed in the assignment; this assignment can also specify a range of values (e.g., "lengths from 5 to 55 characters") as well. For FIA_PSK_EXT.1.3, the ST author specifies whether the TSF merely accepts bit-based pre-shared keys, or is capable of generating them. If it generates them, the requirement specifies that they must be generated using the RBG provided by the TOE.

Extended Components – NDcPP

Security Audit (FAU)

Security Audit Data Generation (FAU_GEN_EXT)

Family Behaviour

This component defines the requirements for components in a distributed TOE to generate security audit data.

Component levelling

FAU_GEN_EXT.1 Security audit data shall be generated by all components in a distributed TOE

Management: FAU_GEN_EXT.1

The following actions could be considered for the management functions in FMT:

a) The TSF shall have the ability to configure the cryptographic functionality.

Audit: FAU_GEN_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

b) No audit necessary.

FAU_ GEN_EXT.1 Security Audit Data Generation for Distributed TOE Components

FAU_GEN_EXT.1 – Security Audit Generation

Hierarchical to:	No other components.
Dependencies:	None.

FAU_GEN_EXT.1.1. The TSF shall be able to generate audit records for each TOE component. The audit records generated by the TSF of each TOE component shall include the subset of security relevant audit events which can occur on the TOE component.

Protected Audit Event Storage (FAU_STG_EXT)

Family Behaviour

This component defines the requirements for the TSF to be able to securely transmit audit data between the TOE and an external IT entity.

Component levelling

FAU_STG_EXT Protected Audit Event Storage
1
2
3
4
5

FAU_STG_EXT.1 Protected audit event storage requires the TSF to use a trusted channel implementing a secure protocol.

FAU_STG_EXT.2 Counting lost audit data requires the TSF to provide information about audit records affected when the audit log becomes full.

FAU_STG_EXT.3 Action in case of possible audit data loss requires the TSF to generate a warning before the audit trail exceeds the local storage capacity.

FAU_STG_EXT.4 Protected Local audit event storage for distributed TOEs requires the TSF to use a trusted channel to protect audit transfer to another TOE component.

FAU_STG_EXT.5 Protected Remote audit event storage for distributed TOEs requires the TSF to use a trusted channel to protect audit transfer to another TOE component.

Management: FAU_STG_EXT.1, FAU_STG_EXT.2, FAU_STG_EXT.3, FAU_STG_EXT.4, FAU_STG_EXT.5

The following actions could be considered for the management functions in FMT:

a) The TSF shall have the ability to configure the cryptographic functionality.

Audit: FAU_STG_EXT.1, FAU_STG_EXT.2, FAU_STG_EXT.3, FAU_STG_EXT.4, FAU_STG_EXT.5

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) No audit necessary.

FAU_ STG_EXT.1 Protected Audit Event Storage

FAU_STG_EXT.1 – Protected Audit Event Storage

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation
FTP_ITC.1 Inter-TSF Trusted Channel

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to an external IT entity using a trusted channel according to FTP_ITC.1.

FAU_STG_EXT.1.2 The TSF shall be able to store generated audit data on the TOE itself. In addition [selection:

- *The TOE shall consist of a single standalone component that stores audit data locally,*

- *The TOE shall be a distributed TOE that stores audit data on the following TOE components: [assignment: identification of TOE components],*
- *The TOE shall be a distributed TOE with storage of audit data provided externally for the following TOE components: [assignment: list of TOE components that do not store audit data locally and the other TOE components to which they transmit their generated audit data].*

FAU_STG_EXT.1.3 The TSF shall [selection: *drop new audit data, overwrite previous audit records according to the following rule: [assignment: rule for overwriting previous audit records], [assignment: other action]*] when the local storage space for audit data is full.

FAU_ STG_EXT.2 Counting Lost Audit Data

FAU_STG_EXT.2 – Counting Lost Audit Data

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation
FAU_STG_EXT.1 External Audit Trail Storage

FAU_STG_EXT.2.1 The TSF shall provide information about the number of [selection: *dropped, overwritten, [assignment: other information]*] audit records in the case where the local storage has been filled and the TSF takes one of the actions defined in FAU_STG_EXT.1.3.

FAU_ STG_EXT.3 Action in Case of Possible Audit Data Loss

FAU_STG_EXT.3 – Action in Case of Possible Audit Data Loss

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation
FAU_STG_EXT.1 External Audit Trail Storage

FAU_STG_EXT.3.1/LocSpace The TSF shall *generate a warning to inform the Administrator before the audit trail exceeds the local audit trail storage capacity.*

FAU_ STG_EXT.4 Protected Local Audit Event Storage for Distributed TOEs

FAU_STG_EXT.4 – Protected Local Audit Event Storage

Hierarchical to: No other components.

Dependencies: FAU_GEN_EXT.1 Security Audit data generation for Distributed TOE Components
[FPT_ITT.1 Intra-TSF Trusted Channel or
FTP_ITC.1 Inter-TSF Trusted Channel]

FAU_STG_EXT.4.1 The TSF of each TOE component which stores security audit data locally shall perform the following actions when the local storage space for audit data is full: [*assignment: table of components and for each component its action chosen according to the following: [selection: drop new audit data, overwrite previous audit records according to the following rule: [assignment: rule for overwriting previous audit records], [assignment: other action]*]].

FAU_ STG_EXT.5 Protected Remote Audit Event Storage for Distributed TOEs

FAU_STG_EXT.5 – Protected Audit Event Storage

Hierarchical to: No other components.

Dependencies: FAU_GEN_EXT.1 Security Audit data generation for Distributed TOE Components
[FPT_ITT.1 Intra-TSF Trusted Channel or
FTP_ITC.1 Inter-TSF Trusted Channel]

FAU_STG_EXT.5.1 Each TOE component which does not store security audit data locally shall be able to buffer security audit data locally until it has been transferred to another TOE component that stores or forwards it. All transfer of audit records between TOE components shall use a protected channel according to [selection: *FPT_ITT.1, FTP_ITC.1*].

Cryptographic Support (FCS)

Random Bit Generation (FCS_RBG_EXT)

FCS_RBG_EXT.1 Random Bit Generation

Family Behaviour

Components in this family address the requirements for random bit/number generation. This is a new family defined for the FCS class.

Component levelling

FCS_RBG_EXT.1 Random Bit Generation requires random bit generation to be performed in accordance with selected standards and seeded by an entropy source.

Management: FCS_RBG_EXT.1

The following actions could be considered for the management functions in FMT:

a) There are no management activities foreseen

Audit: FCS_RBG_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: failure of the randomization process

FCS_RBG_EXT.1 – Random Bit Generation

Hierarchical to:	No other components
Dependencies:	No other components

FCS_RBG_EXT.1.1 The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using [selection: *Hash_DRBG (any), HMAC_DRBG (any), CTR_DRBG (AES)*].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [selection: *[assignment: number of software-based sources] software-based noise source, [assignment: number of platform-based sources] platform-based noise source*] with a minimum of [selection: *128 bits, 192 bits, 256 bits*] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 “Security Strength Table for Hash Functions”, of the keys and hashes that it will generate.

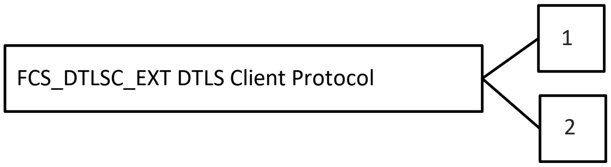
Cryptographic Protocols (FCS_DTLSC_EXT, FCS_DTLSS_EXT, FCS_HTTPS_EXT, FCS_IPSEC_EXT, FCS_NTP_EXT, FCS_SSHC_EXT, FCS_SSHS_EXT, FCS_TLSC_EXT, FCS_TLSS_EXT)

FCS_DTLSC_EXT DTLS Client Protocol

Family Behaviour

The component in this family addresses the ability for a client to use DTLS to protect data between the client and a server using the DTLS protocol.

Component levelling



FCS_DTLSC_EXT.1 DTLS Client requires that the client side of DTLS be implemented as specified.

FCS_DTLSC_EXT.2 DTLS Client requires that the client side of the DTLS implementation include mutual authentication.

Management: FCS_DTLSC_EXT.1, FCS_DTLSC_EXT.2

The following actions could be considered for the management functions in FMT:

a) There are no management activities foreseen.

Audit: FCS_DTLSC_EXT.1, FCS_DTLSC_EXT.2

The following actions should be considered for audit if FAU_GEN Security audit data generation is included in the PP/ST:

a) Failure of DTLS session establishment
b) DTLS session establishment
c) DTLS session termination

FCS_DTLSC_EXT.1 – DTLS Client Protocol

Hierarchical to: No other components

Dependencies: FCS_CKM. 1DataEncryption1 Cryptographic Key Generation
FCS_CKM.2 Cryptographic Key Establishment
FCS_COP.1/DataEncryption Cryptographic operation (AES Data encryption/decryption)
FCS_COP.1/SigGen1SigGen Cryptographic operation (Signature Generation and Verification)
FCS_COP.1/Hash Cryptographic operation (Hash Algorithm)
FCS_COP.1/KeyedHash Cryptographic operation (Keyed Hash Algorithm)
FCS_RBG_EXT.1 Random Bit Generation
FIA_X509_EXT.1 X.509 Certificate Validation
FIA_X509_EXT.2 X.509 Certificate Authentication

FCS_DTLSC_EXT.1.1 The TSF shall implement [selection: *DTLS 1.2 (RFC 6347), DTLS 1.0 (RFC 4347)*] supporting the following ciphersuites:

- *[assignment: List of optional ciphersuites and reference to RFC in which each is defined].*

FCS_DTLSC_EXT.1.2 The TSF shall verify that the presented identifier matches [selection: *the reference identifier per RFC 6125 section 6, IPv4 address in CN or SAN, IPv6 address in the CN or SAN, IPv4 address in SAN, IPv6 address in the SAN, the identifier per RFC 5280 Appendix A using* *[selection: id-at-commonName, id-at-countryName, id-at-dnQualifier, id-at-generationQualifier, id-at-givenName, id-at-initials, id-at-localityName, id-at-name, id-at-organizationalUnitName, id-at-organizationName, id-at-pseudonym, id-at-serialNumber, id-at-stateOrProvinceName, id-at-surname, id-at-title] and no other attribute types*].

FCS_DTLSC_EXT.1.3 When establishing a trusted channel, by default the TSF shall not establish a trusted channel if the server certificate is invalid. The TSF shall also [selection:

- *Not implement any administrator override mechanism*

- *require administrator authorization to establish the connection if the TSF fails to [selection: match the reference identifier, validate certificate path, validate expiration date, determine the revocation status] of the presented server certificate*

].

FCS_DTLSC_EXT.1.4 The TSF shall [selection: *not present the Supported Elliptic Curves/Supported Groups Extension, present the Supported Elliptic Curves/Supported Groups Extension with the following curves/groups:* [selection: *secp256r1, secp384r1, secp521r1, ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192] and no other curves/groups*] in the Client Hello.

FCS_DTLSC_EXT.2 – DTLS Client Support for Mutual Authentication

Hierarchical to:	No other components
Dependencies:	FCS_CKM. 1DataEncryption1 Cryptographic Key Generation FCS_CKM.2 Cryptographic Key Establishment FCS_COP.1/DataEncryption Cryptographic operation (AES Data encryption/decryption) FCS_COP.1/SigGen1SigGen Cryptographic operation (Signature Generation and Verification) FCS_COP.1/Hash Cryptographic operation (Hash Algorithm) FCS_COP.1/KeyedHash Cryptographic operation (Keyed Hash Algorithm) FCS_RBG_EXT.1 Random Bit Generation FCS_DTLSC_EXT.1 DTLS Client Protocol FIA_X509_EXT.1 X.509 Certificate Validation FIA_X509_EXT.2 X.509 Certificate Authentication

FCS_DTLSC_EXT.2.1 The TSF shall support mutual authentication using X.509v3 certificates.

FCS_DTLSC_EXT.2.2 The TSF shall [selection: *terminate the DTLS session, silently discard the record*] if a message received contains an invalid MAC.

FCS_DTLSC_EXT.2.3 The TSF shall detect and silently discard replayed messages for:

- DTLS records previously received;
- DTLS records too old to fit in the sliding window.

FCS_DTLSS_EXT DTLS Server Protocol

Family Behaviour

The component in this family addresses the ability for a server to use DTLS to protect data between a client and the server using the DTLS protocol.

Component levelling

FCS_DTLSS_EXT.1 DTLS Server requires that the server side of TLS be implemented as specified.

FCS_DTLSS_EXT.2: DTLS Server requires that mutual authentication be included in the DTLS implementation.

Management: FCS_DTLSS_EXT.1, FCS_DTLSS_EXT.2

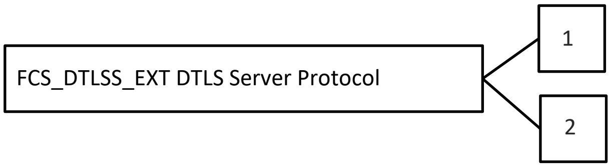
The following actions could be considered for the management functions in FMT:

a) There are no management activities foreseen.

Audit: FCS_DTLSS_EXT.1, FCS_DTLSS_EXT.2

The following actions should be considered for audit if FAU_GEN Security audit data generation is included in the PP/ST:

a) Failure of DTLS session establishment.
b) DTLS session establishment



c) DTLS session termination

FCS_DTLSS_EXT.1 – DTLS Server Protocol

Hierarchical to:	No other components
Dependencies:	FCS_CKM. 1DataEncryption1 Cryptographic Key Generation FCS_CKM.2 Cryptographic Key Establishment FCS_COP.1/DataEncryption Cryptographic operation (AES Data encryption/decryption) FCS_COP.1/SigGen1SigGen Cryptographic operation (Signature Generation and Verification) FCS_COP.1/Hash Cryptographic operation (Hash Algorithm) FCS_COP.1/KeyedHash Cryptographic operation (Keyed Hash Algorithm) FCS_RBG_EXT.1 Random Bit Generation FIA_X509_EXT.1 X.509 Certificate Validation FIA_X509_EXT.2 X.509 Certificate Authentication

FCS_DTLSS_EXT.1.1 The TSF shall implement [selection: *DTLS 1.2 (RFC 6347), DTLS 1.0 (RFC 4347)*] supporting the following ciphersuites:

- *[assignment: List of optional ciphersuites and reference to RFC in which each is defined]*

FCS_DTLSS_EXT.1.2 The TSF shall deny connections from clients requesting *[assignment: list of protocol versions]*.

FCS_DTLSS_EXT.1.3 The TSF shall not proceed with a connection handshake attempt if the DTLS Client fails validation.

FCS_DTLSS_EXT.1.4 The TSF shall perform key establishment for TLS using [selection: *RSA with key size* [selection*: 2048 bits, 3072 bits, 4096 bits], Diffie-Hellman parameters with size* [selection*: 2048 bits, 3072 bits, 4096 bits, 6144 bits, 8192 bits], Diffie-Hellman groups* [selection*: ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, no other groups], ECDHE curves* [selection*: secp256r1, secp384r1, secp521r1] and no other curves*].

FCS_DTLSS_EXT.1.5 The TSF shall [selection: *terminate the DTLS session, silently discard the record*] if a message received contains an invalid MAC.

FCS_DTLSS_EXT.1.6 The TSF shall detect and silently discard replayed messages for:

- DTLS records previously received.
- DTLS Records too old to fit in the sliding window.

FCS_DTLSS_EXT.1.7 The TSF shall support [selection: *no session resumption or session tickets, session resumption based on session IDs according to RFC 4346 (TLS1.1) or RFC 5246 (TLS1.2), session resumption based on session tickets according to RFC 5077*].

FCS_DTLSS_EXT.2 – DTLS Server Support for Mutual Authentication

Hierarchical to:	No other components
Dependencies:	FCS_CKM. 1DataEncryption1 Cryptographic Key Generation FCS_CKM.2 Cryptographic Key Establishment FCS_COP.1/DataEncryption Cryptographic operation (AES Data encryption/decryption) FCS_COP.1/SigGen1SigGen Cryptographic operation (Signature Generation and Verification) FCS_COP.1/Hash Cryptographic operation (Hash Algorithm) FCS_COP.1/KeyedHash Cryptographic operation (Keyed Hash Algorithm) FCS_RBG_EXT.1 Random Bit Generation FCS_DTLSS_EXT.1 DTLS Server Protocol FIA_X509_EXT.1 X.509 Certificate Validation

FCS_DTLSS_EXT.2.1 The TSF shall support mutual authentication of DTLS clients using X.509v3 certificates.

FCS_DTLSS_EXT.2.2 When establishing a trusted channel, by default the TSF shall not establish a trusted channel if the client certificate is invalid. The TSF shall also [selection:

- *Not implement any administrator override mechanism*
- *require administrator authorization to establish the connection if the TSF fails to* [selection: *match the reference identifier, validate certificate path, validate expiration date, determine the revocation status] of the presented client certificate*

].

FCS_DTLSS_EXT.2.3 The TSF shall not establish a trusted channel if the distinguished name (DN) or Subject Alternative Name (SAN) contained in a certificate does not match the expected identifier for the client.

FCS_HTTPS_EXT.1 HTTPS Protocol

Family Behaviour

Components in this family define the requirements for protecting remote management sessions between the TOE and a Security Administrator. This family describes how HTTPS will be implemented. This is a new family defined for the FCS Class.

Component levelling

FCS_HTTPS_EXT HTTPS Protocol
1

FCS_HTTPS_EXT.1 HTTPS requires that HTTPS be implemented according to RFC 2818 and supports TLS.

Management: FCS_HTTPS_EXT.1

The following actions could be considered for the management functions in FMT:

a) There are no management activities foreseen.

Audit: FCS_HTTPS_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) There are no auditable events foreseen.

FCS_HTTPS_EXT.1 – HTTPS Protocol

FCS_HTTPS_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2 The TSF shall implement the HTTPS protocol using TLS.

FCS_HTTPS_EXT.1.3 If a peer certificate is presented, the TSF shall [selection: *not establish the connection, request authorization to establish the connection, [assignment: other action]*] if the peer certificate is deemed invalid**.**

FCS_IPSEC_EXT.1 IPsec Protocol

Family Behaviour

Components in this family address the requirements for protecting communications using IPsec.

Component levelling

FCS_IPSEC_EXT.1 IPsec requires that IPsec be implemented as specified.

Management: FCS_IPSEC_EXT.1

The following actions could be considered for the management functions in FMT:

a) Maintenance of SA lifetime configuration

Audit: FCS_IPSEC_EXT.1

The following actions should be considered for audit if FAU_GEN Security audit data generation is included in the PP/ST:

a) Decisions to DISCARD, BYPASS, PROTECT network packets processed by the TOE.
b) Failure to establish an IPsec SA
c) IPsec SA establishment
d) IPsec SA termination
e) Negotiation “down” from an IKEv2 to IKEv1 exchange.

FCS_IPSEC_EXT.1 – Internet Protocol Security (IPsec) Communications

Hierarchical to:	No other components
Dependencies:	FCS_CKM. 1DataEncryption1 Cryptographic Key Generation FCS_CKM.2 Cryptographic Key Establishment FCS_COP.1/DataEncryption Cryptographic operation (AES Data encryption/decryption) FCS_COP.1/SigGen1SigGen Cryptographic operation (Signature Generation and Verification)

FCS_COP.1/Hash Cryptographic operation (Hash Algorithm)
FCS_COP.1/KeyedHash Cryptographic operation (Keyed Hash Algorithm)
FCS_RBG_EXT.1 Random Bit Generation

FCS_IPSEC_EXT.1.1 The TSF shall implement the IPsec architecture as specified in RFC 4301.

FCS_IPSEC_EXT.1.2 The TSF shall have a nominal, final entry in the SPD that matches anything that is otherwise unmatched and discards it.

FCS_IPSEC_EXT.1.3 The TSF shall implement [selection: *tunnel mode, transport mode*].

FCS_IPSEC_EXT.1.4 The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using the cryptographic algorithms [selection: *AES-CBC-128 (RFC 3602), AES-CBC-192 (RFC 3602), AES-CBC-256 (RFC 3602), AES-GCM-128 (RFC 4106), AES-GCM-192 (RFC 4106), AES-GCM-256 (RFC 4106),*] together with a Secure Hash Algorithm (SHA)-based HMAC [selection: *HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512, no HMAC algorithm*].

FCS_IPSEC_EXT.1.5 The TSF shall implement the protocol: [selection:

- *IKEv1, using Main Mode for Phase 1 exchanges, as defined in RFCs 2407, 2408, 2409, RFC 4109,* [selection: *no other RFCs for extended sequence numbers, RFC 4304 for extended sequence numbers*]*, and* [selection: *no other RFCs for hash functions, RFC 4868 for hash functions*]*;*

- *IKEv2 as defined in RFCs 5996 [selection: with no support for NAT traversal, with mandatory support for NAT traversal as specified in RFC 5996, section 2.23)*]*, and* [selection: *no other RFCs for hash functions, RFC 4868 for hash functions*]].

FCS_IPSEC_EXT.1.6 The TSF shall ensure the encrypted payload in the [selection: *IKEv1, IKEv2*] protocol uses the cryptographic algorithms [selection: *AES-CBC-128, AES_CBC-192 AES-CBC-256 (specified in RFC 3602), AES-GCM-128, AES-GCM-192, AES-GCM-256 (specified in RFC 5282)*].

FCS_IPSEC_EXT.1.7 The TSF shall ensure that [selection:

- *IKEv1 Phase 1 SA lifetimes can be configured by a Security Administrator based on* [selection:
  - *number of bytes;*
  - *length of time, where the time values can be configured within [assignment: integer range including 24*] *hours;*

  ]*;*
- *IKEv2 SA lifetimes can be configured by a Security Administrator based on* [selection:
  - *number of bytes;*
  - *length of time, where the time values can be configured within [assignment: integer range including 24*] *hours*

  ]

].

FCS_IPSEC_EXT.1.8 The TSF shall ensure that [selection:

- *IKEv1 Phase 2 SA lifetimes can be configured by a Security Administrator based on* [selection:
  - *number of bytes;*
  - *length of time, where the time values can be configured within [assignment: integer range including 8] hours;*

  ]*;*
- *IKEv2 Child SA lifetimes can be configured by a Security Administrator based on* [selection:
  - *number of bytes;*
  - *length of time, where the time values can be configured within [assignment: integer range including 8] hours;*

  ]

].

FCS_IPSEC_EXT.1.9 The TSF shall generate the secret value x used in the IKE Diffie-Hellman key exchange (“x” in g^x mod p) using the random bit generator specified in FCS_RBG_EXT.1, and having a length of at least *[assignment: (one or more) number(s) of bits that is at least twice the security strength of the negotiated Diffie-Hellman group*] bits.

FCS_IPSEC_EXT.1.10 The TSF shall generate nonces used in [selection: *IKEv1, IKEv2*] exchanges of length [selection:

- *according to the security strength associated with the negotiated Diffie-Hellman group;*
- *at least 128 bits in size and at least half the output size of the negotiated pseudorandom function (PRF) hash*
  ].

FCS_IPSEC_EXT.1.11 The TSF shall ensure that IKE protocols implement DH Group(s) [selection:

- [selection*: 14 (2048-bit MODP), 15 (3072-bit MODP), 16 (4096-bit MODP), 17 (6144-bit MODP), 18 (8192-bit MODP)] according to RFC 3526,*
- [selection*: 19 (256-bit Random ECP), 20 (384-bit Random ECP), 21 (521-bit Random ECP), 24 (2048-bit MODP with 256-bit POS)] according to RFC 5114.*

].

FCS_IPSEC_EXT.1.12 The TSF shall be able to ensure by default that the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [selection: *IKEv1 Phase 1, IKEv2 IKE_SA*] connection is greater than or equal to the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [selection: *IKEv1 Phase 2, IKEv2 CHILD_SA*] connection.

FCS_IPSEC_EXT.1.13 The TSF shall ensure that all IKE protocols perform peer authentication using [selection: *RSA, ECDSA*] that use X.509v3 certificates that conform to RFC 4945 and [selection: *Pre-shared Keys, no other method*].

FCS_IPSEC_EXT.1.14 The TSF shall only establish a trusted channel if the presented identifier in the received certificate matches the configured reference identifier, where the presented and reference identifiers are of the following fields and types: [selection: *SAN: IP address, SAN: Fully Qualified Domain Name (FQDN), SAN: user FQDN, CN: IP address, CN: Fully Qualified Domain Name (FQDN), CN: user FQDN, Distinguished Name (DN)]* and [selection: *no other reference identifier type, [assignment: other supported reference identifier types*]].

FCS_NTP_EXT.1 NTP Protocol

Family Behaviour

The component in this family addresses the ability for a TOE to protect NTP time synchronization traffic.

Component levelling

FCS_NTP_EXT.1 Requires NTP to be implemented as specified.

Management: FCS_NTP_EXT.1

The following actions could be considered for the management functions in FMT:

a) Ability to configure NTP

Audit: FCS_NTP_EXT.1

The following actions should be considered for audit if FAU_GEN Security audit data generation is included in the PP/ST:

a) No audit requirements are specified.

FCS_NTP_EXT.1 – NTP Protocol

Hierarchical to: No other components

Dependencies:

FCS_COP.1 Cryptographic operation
[FCS_DTLSC_EXT.1 DTLSC Client Protocol or
FCS_IPSEC_EXT.1 IPsec Protocol]

FCS_NTP_EXT.1.1 The TSF shall use only the following NTP version(s) [selection: *NTP v3 (RFC 1305), NTP v4 (RFC 5905)*].

FCS_NTP_EXT.1.2 The TSF shall update its system time using [selection:

- Authentication using [selection: *SHA1, SHA256, SHA384, SHA512, AES-CBC-128, AES-CBC-256*] as the message digest algorithm(s);
- [selection: *IPsec, DTLS*] to provide trusted communication between itself and an NTP time source.
  ].

FCS_NTP_EXT.1.3 The TSF shall not update NTP timestamp from broadcast and/or multicast addresses.

FCS_NTP_EXT.1.4 The TSF shall support configuration of at least three (3) NTP time sources in the Operational Environment.

FCS_SSHC_EXT.1 SSH Client

Family Behaviour

The component in this family addresses the ability for a client to use SSH to protect data between the client and a server using the SSH protocol.

Component levelling

FCS_SSHC_EXT.1 SSH Client requires that the client side of SSH be implemented as specified.

Management: FCS_SSHC_EXT.1

The following actions could be considered for the management functions in FMT:

a) There are no management activities foreseen.

Audit: FCS_SSHC_EXT.1

The following actions should be considered for audit if FAU_GEN Security audit data generation is included in the PP/ST:

a) Failure of SSH session establishment
b) SSH session establishment
c) SSH session termination

FCS_SSHC_EXT.1 – SSH Client Protocol

Hierarchical to: No other components

Dependencies: FCS_CKM.1Cryptographic Key Generation
FCS_CKM.2 Cryptographic Key Establishment
FCS_COP.1/DataEncryption Cryptographic operation (AES Data encryption/decryption)
FCS_COP.1/SigGen Cryptographic operation (Signature Generation and Verification)
FCS_COP.1/Hash Cryptographic operation (Hash Algorithm)
FCS_COP.1/KeyedHash Cryptographic operation (Keyed Hash Algorithm)
FCS_RBG_EXT.1 Random Bit Generation

FCS_SSHC_EXT.1.1 The TSF shall implement the SSH protocol in accordance with: RFCs *4251, 4252, 4253, 4254,* [selection: *4256, 4344, 5647, 5656, 6187, 6668, 8268, 8308 section 3.1, 8332*].

FCS_SSHC_EXT.1.2 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, [selection: *password-based, no other method*].

FCS_SSHC_EXT.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than *[assignment: number of bytes]* bytes in an SSH transport connection are dropped.

FCS_SSHC_EXT.1.4 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: [assignment: *list of encryption algorithms*].

FCS_SSHC_EXT.1.5 The TSF shall ensure that the SSH public-key based authentication implementation uses [selection: *ssh-rsa, rsa-sha2-256, rsa-sha2-512, ecdsa-sha2-nistp256, x509v3-ssh-rsa, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384, x509v3-ecdsa-sha2-nistp521, x509v3-rsa2048-sha256*] as its public key algorithm(s) and rejects all other public key algorithms

FCS_SSHC_EXT.1.6 The TSF shall ensure that the SSH transport implementation uses *[assignment: list of data integrity MAC algorithms]* as its data integrity MAC algorithm(s) and rejects all other MAC algorithm(s).

FCS_SSHC_EXT.1.7 The TSF shall ensure that *[assignment: list of key exchange methods]* are the only allowed key exchange methods used for the SSH protocol.

FCS_SSHC_EXT.1.8 The TSF shall ensure that within SSH connections, the same session keys are used for a threshold of no longer than one hour, and each encryption key is used to protect no more than one gigabyte of data. After any of the thresholds are reached, a rekey needs to be performed.

FCS_SSHC_EXT.1.9 The TSF shall ensure that the SSH client authenticates the identity of the SSH server using a local database associating each host name with its corresponding public key and [selection: *a list of trusted certification authorities, no other methods*] as described in RFC 4251 section 4.1.

FCS_SSHS_EXT.1 SSH Server Protocol

Family Behaviour

The component in this family addresses the ability for a server to offer SSH to protect data between a client and the server using the SSH protocol.

Component levelling

FCS_SSHS_EXT.1 SSH Server requires that the server side of SSH be implemented as specified.

Management: FCS_SSHS_EXT.1

The following actions could be considered for the management functions in FMT:

a) There are no management activities foreseen.

Audit: FCS_SSHS_EXT.1

The following actions should be considered for audit if FAU_GEN Security audit data generation is included in the PP/ST:

a) Failure of SSH session establishment
b) SSH session establishment
c) SSH session termination

FCS_SSHS_EXT.1 – SSH Server Protocol

Hierarchical to: No other components

Dependencies: FCS_CKM.1Cryptographic Key Generation
FCS_CKM.2 Cryptographic Key Establishment
FCS_COP.1/DataEncryption Cryptographic operation (AES Data encryption/decryption)
FCS_COP.1/SigGen Cryptographic operation (Signature Generation and Verification)
FCS_COP.1/Hash Cryptographic operation (Hash Algorithm)
FCS_COP.1/KeyedHash Cryptographic operation (Keyed Hash Algorithm)
FCS_RBG_EXT.1 Random Bit Generation

FCS_SSHS_EXT.1.1 The TSF shall implement the SSH protocol in accordance with: RFCs 4251, 4252, 4253, 4254, [selection: *4256, 4344, 5647, 5656, 6187, 6668, 8268, 8308* section 3.1, 8332].

FCS_SSHS_EXT.1.2 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, [selection: *password-based, no other method*].

FCS_SSHS_EXT.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than *[assignment: number of bytes]* bytes in an SSH transport connection are dropped.

FCS_SSHS_EXT.1.4 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: *[assignment: encryption algorithms]*.

FCS_SSHS_EXT.1.5 The TSF shall ensure that the SSH public-key based authentication implementation uses [selection: *ssh-rsa, rsa-sha2-256, rsa-sha2-512, ecdsa-sha2-nistp256, x509v3-ssh-rsa, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384, x509v3-ecdsa-sha2-nistp521, x509v3-rsa2048-sha256*] as its public key algorithm(s) and rejects all other public key algorithms.

FCS_SSHS_EXT.1.6 The TSF shall ensure that the SSH transport implementation uses *[assignment: list of MAC algorithms]* as its MAC algorithm(s) and rejects all other MAC algorithm(s).

FCS_SSHS_EXT.1.7 The TSF shall ensure that *[assignment: list of key exchange methods]* are the only allowed key exchange methods used for the SSH protocol.

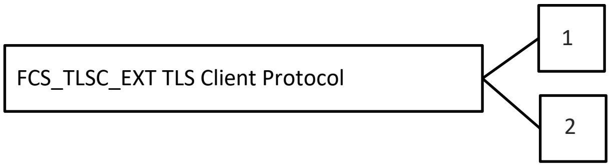
FCS_SSHS_EXT.1.8 The TSF shall ensure that within SSH connections, the same session keys are used for a threshold of no longer than one hour, and each encryption key is used to protect no more than one gigabyte of data. After any of the thresholds are reached, a rekey needs to be performed.

FCS_TLSC_EXT TLS Client Protocol

Family Behaviour

The component in this family addresses the ability for a client to use TLS to protect data between the client and a server using the TLS protocol.

Component levelling



FCS_TLSC_EXT.1 TLS Client requires that the client side of TLS be implemented as specified.

FCS_TLSC_EXT.2 TLS Client requires that the client side of the TLS implementation include mutual authentication.

Management: FCS_TLSC_EXT.1, FCS_TLSC_EXT.2

The following actions could be considered for the management functions in FMT:

a) There are no management activities foreseen.

Audit: FCS_TLSC_EXT.1, FCS_TLSC_EXT.2

The following actions should be considered for audit if FAU_GEN Security audit data generation is included in the PP/ST:

a) Failure of TLS session establishment
b) TLS session establishment
c) TLS session termination

FCS_TLSC_EXT.1 – TLS Client Protocol without Mutual Authentication

Hierarchical to:	No other components
Dependencies:	FCS_CKM. 1 Cryptographic Key Generation FCS_CKM.2 Cryptographic Key Establishment FCS_COP.1/DataEncryption Cryptographic operation (AES Data encryption/decryption) FCS_COP.1/SigGen Cryptographic operation (Signature Generation and Verification) FCS_COP.1/Hash Cryptographic operation (Hash Algorithm) FCS_COP.1/KeyedHash Cryptographic operation (Keyed Hash Algorithm) FCS_RBG_EXT.1 Random Bit Generation FIA_X509_EXT.1 X.509 Certificate Validation FIA_X509_EXT.2 X.509 Certificate Authentication

FCS_TLSC_EXT.1.1 The TSF shall implement [selection: *TLS 1.2 (RFC 5246), TLS 1.1 (RFC 4346)*] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites:

- *[assignment: list of optional ciphersuites and reference to RFC in which each is defined]* and no other ciphersuites.

FCS_TLSC_EXT.1.2 The TSF shall verify that the presented identifier matches [selection: *the reference identifier per RFC 6125 section 6, IPv4 address in CN or SAN, IPv6 address in the CN or SAN, IPv4 address in SAN, IPv6 address in the SAN, the identifier per RFC 5280 Appendix A using [selection: id-at-commonName, id-at-countryName, id-at-dnQualifier, id-at-generationQualifier, id-at-givenName, id-at-initials, id-at-localityName, id-at-name, id-at-organizationalUnitName, id-at-organizationName, id-at-pseudonym, id-at-serialNumber, id-at-stateOrProvinceName, id-at-surname, id-at-title] and no other attribute types*].

FCS_TLSC_EXT.1.3 When establishing a trusted channel, by default the TSF shall not establish a trusted channel if the server certificate is invalid. The TSF shall also [selection:

- *Not implement any administrator override mechanism*

- *require administrator authorization to establish the connection if the TSF fails to [selection: match the reference identifier, validate certificate path, validate expiration date, determine the revocation status] of the presented server certificate*

].

FCS_TLSC_EXT.1.4 The TSF shall [selection: *not present the Supported Elliptic Curves/Supported Groups Extension, present the Supported Elliptic Curves/Supported Groups Extension with the following curves/groups:* [selection*: secp256r1, secp384r1, secp521r1, ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192] and no other curves/groups*] in the Client Hello.

FCS_TLSC_EXT.2 – TLS Client Support for Mutual Authentication

Hierarchical to:	No other components
Dependencies:	FCS_CKM. 1 Cryptographic Key Generation FCS_CKM.2 Cryptographic Key Establishment FCS_COP.1/DataEncryption Cryptographic operation (AES Data encryption/decryption) FCS_COP.1/SigGen Cryptographic operation (Signature Generation and Verification) FCS_COP.1/Hash Cryptographic operation (Hash Algorithm) FCS_COP.1/KeyedHash Cryptographic operation (Keyed Hash Algorithm) FCS_RBG_EXT.1 Random Bit Generation FIA_X509_EXT.1 X.509 Certificate Validation FIA_X509_EXT.2 X.509 Certificate Authentication

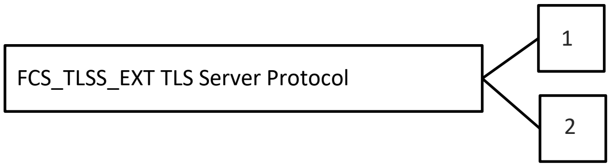
FCS_TLSC_EXT.2.1 The TSF shall support TLS communication with mutual authentication using X.509v3 certificates.

FCS_TLSS_EXT TLS Server Protocol

Family Behaviour

The component in this family addresses the ability for a server to use TLS to protect data between a client and the server using the TLS protocol.

Component levelling



FCS_TLSS_EXT.1 TLS Server requires that the server side of TLS be implemented as specified.

FCS_TLSS_EXT.2: TLS Server requires the mutual authentication be included in the TLS implementation.

Management: FCS_TLSS_EXT.1, FCS_TLSS_EXT.2

The following actions could be considered for the management functions in FMT:

a) There are no management activities foreseen.

Audit: FCS_TLSS_EXT.1, FCS_TLSS_EXT.2

The following actions should be considered for audit if FAU_GEN Security audit data generation is included in the PP/ST:

a) Failure of TLS session establishment
b) TLS session establishment
c) TLS session termination

FCS_TLSS_EXT.1 – TLS Server Protocol without Mutual Authentication

Hierarchical to:	No other components
Dependencies:	FCS_CKM. 1 Cryptographic Key Generation FCS_CKM.2 Cryptographic Key Establishment FCS_COP.1/DataEncryption Cryptographic operation (AES Data encryption/decryption) FCS_COP.1/SigGen Cryptographic operation (Signature Generation and Verification) FCS_COP.1/Hash Cryptographic operation (Hash Algorithm) FCS_COP.1/KeyedHash Cryptographic operation (Keyed Hash Algorithm) FCS_RBG_EXT.1 Random Bit Generation FIA_X509_EXT.1 X.509 Certificate Validation FIA_X509_EXT.2 X.509 Certificate Authentication

FCS_TLSS_EXT.1.1 The TSF shall implement [selection: *TLS 1.2 (RFC 5246), TLS 1.1 (RFC 4346)*] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites:

- *[assignment: list of optional ciphersuites and reference to RFC in which each is defined]* and no other ciphersuites.

FCS_TLSS_EXT.1.2 The TSF shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0 and [selection: *TLS 1.1, TLS 1.2, none*].

FCS_TLSS_EXT.1.3 The TSF shall perform key establishment for TLS using [selection: *RSA with key size* [selection*: 2048 bits, 3072 bits, 4096 bits], Diffie-Hellman parameters with size* [selection*: 2048 bits, 3072 bits, 4096 bits, 6144 bits, 8192 bits], Diffie-Hellman groups* [selection: *ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, no other groups], ECDHE curves* [selection: *secp256r1, secp384r1, secp521r1] and no other curves*]].

FCS_TLSS_EXT.1.4 The TSF shall support [selection: *no session resumption or session tickets, session resumption based on session IDs according to* RFC 4346 *(TLS1.1) or* RFC 5246 *(TLS1.2), session resumption based on session tickets according to* RFC 5077].

FCS_TLSS_EXT.2 – TLS Server Support for Mutual Authentication

Hierarchical to:	No other components
Dependencies:	FCS_CKM. 1 Cryptographic Key Generation FCS_CKM.2 Cryptographic Key Establishment FCS_COP.1/DataEncryption Cryptographic operation (AES Data encryption/decryption) FCS_COP.1/SigGen Cryptographic operation (Signature Generation and Verification) FCS_COP.1/Hash Cryptographic operation (Hash Algorithm) FCS_COP.1/KeyedHash Cryptographic operation (Keyed Hash Algorithm) FCS_RBG_EXT.1 Random Bit Generation FCS_TLSS_EXT.1 TLS Server Protocol without mutual authentication FIA_X509_EXT.1 X.509 Certificate Validation FIA_X509_EXT.2 X.509 Certificate Authentication

FCS_TLSS_EXT.2.1 The TSF shall support TLS communication with mutual authentication of TLS clients using X.509v3 certificates.

FCS_TLSS_EXT.2.2 When establishing a trusted channel, by default the TSF shall not establish a trusted channel if the client certificate is invalid. The TSF shall also [selection:

- *Not implement any administrator override mechanism*

- *require administrator authorization to establish the connection if the TSF fails to* [selection: *match the reference identifier, validate certificate path, validate expiration date, determine the revocation status] of the presented client certificate*

].

FCS_TLSS_EXT.2.3 The TSF shall not establish a trusted channel if the identifier contained in a certificate does not match an expected identifier for the client. If the identifier is a Fully Qualified Domain Name (FQDN), then the TSF shall match the identifiers according to RFC 6125, otherwise the TSF shall parse the identifier from the certificate and match the identifier against the expected identifier of the client as described in the TSS.

Identification and Authentication (FIA)

Password Management (FIA_PMG_EXT)

Family Behaviour

The TOE defines the attributes of passwords used by administrative users to ensure that strong passwords and passphrases can be chosen and maintained.

Component levelling

FIA_PMG_EXT.1 Password management requires the TSF to support passwords with varying composition requirements, minimum lengths, maximum lifetime, and similarity constraints.

Management: FIA_PMG_EXT.1

No management functions.

Audit: FIA_PMG_EXT.1

No specific audit requirements.

FIA_PMG_EXT.1 Password Management

FIA_PMG_EXT.1 – Password Management

Hierarchical to:	No other components
Dependencies:	No other components

FIA_PMG_EXT.1.1 The TSF shall provide the following password management capabilities for administrative passwords:

a) Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [selection: *“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, [assignment: other characters]*];

b) Minimum password length shall be configurable to between [*assignment: minimum number of characters supported by the TOE*] and [*assignment: number of characters greater than or equal to 15*] characters.

User Identification and Authentication (FIA_UIA_EXT)

Family Behaviour

The TSF allows certain specified actions before the non-TOE entity goes through the identification and authentication process.

Component levelling

FIA_UIA_EXT User Identification and Authentication
1

FIA_UIA_EXT.1 User Identification and Authentication requires Administrators (including remote Administrators) to be identified and authenticated by the TOE, providing assurance for that end of the communication path. It also ensures that every user is identified and authenticated before the TOE performs any mediated functions

Management: FIA_UIA_EXT.1

The following actions could be considered for the management functions in FMT:

a) Ability to configure the list of TOE services available before an entity is identified and authenticated

Audit: FIA_UIA_EXT.N

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) All use of the identification and authentication mechanism
b) Provided user identity, origin of the attempt (e.g. IP address)

FIA_UIA_EXT.1 – User Identification and Authentication

Hierarchical to:	No other components
Dependencies:	FTA_TAB.1 Default TOE Access Banners

FIA_UIA_EXT.1.1 The TSF shall allow the following actions prior to requiring the non-TOE entity to initiate the identification and authentication process:

- Display the warning banner in accordance with FTA_TAB.1;

- [selection: *no other actions, automated generation of cryptographic keys, [assignment: list of services, actions performed by the TSF in response to non-TOE requests]*].

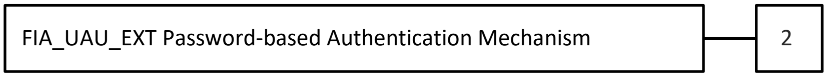
FIA_UIA_EXT.1.2 The TSF shall require each administrative user to be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that administrative user.

User Identification and Authentication (FIA_UAU_EXT)

Family Behaviour

Provides for a locally based administrative user authentication mechanism

Component levelling



FIA_UAU_EXT.2 The password-based authentication mechanism provides administrative users a locally based authentication mechanism.

Management: FIA_UAU_EXT.2

The following actions could be considered for the management functions in FMT:

a) None

Audit: FIA_UAU_EXT.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: All use of the authentication mechanism

FIA_UAU_EXT.2 Password-based Authentication Mechanism

FIA_UAU_EXT.2 – Password-based Authentication Mechanism

Hierarchical to:	No other components
Dependencies:	No other components

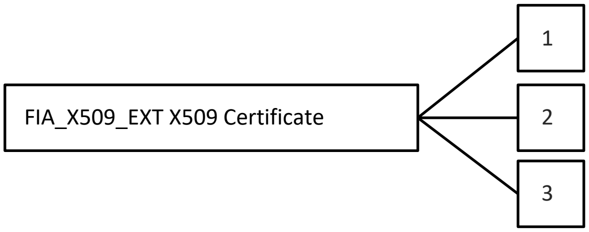
FIA_UAU_EXT.2.1 The TSF shall provide a local [selection: *password-based, SSH public key-based, certificate-based, [assignment: other authentication mechanism(s)]*] authentication mechanism to perform local administrative user authentication.

Authentication using X.509 certificates (FIA_X509_EXT)

Family Behaviour

This family defines the behaviour, management, and use of X.509 certificates for functions to be performed by the TSF. Components in this family require validation of certificates according to a specified set of rules, use of certificates for authentication for protocols and integrity verification, and the generation of certificate requests.

Component levelling



FIA_X509_EXT.1 X509 Certificate Validation, requires the TSF to check and validate certificates in accordance with the RFCs and rules specified in the component.

FIA_X509_EXT.2 X509 Certificate Authentication, requires the TSF to use certificates to authenticate peers in protocols that support certificates, as well as for integrity verification and potentially other functions that require certificates.

FIA_X509_EXT.3 X509 Certificate Requests, requires the TSF to be able to generate Certificate Request Messages and validate responses.

Management: FIA_X509_EXT.1, FIA_X509_EXT.2, FIA_X509_EXT.3

The following actions could be considered for the management functions in FMT:

a) Remove imported X.509v3 certificates
b) Approve import and removal of X.509v3 certificates
c) Initiate certificate requests

Audit: FIA_X509_EXT.1, FIA_X509_EXT.2, FIA_X509_EXT.3

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: No specific audit requirements are specified.

FIA_X509_EXT.1 X.509 Certificate Validation

FIA_X509_EXT.1 – X.509 Certificate Validation

Hierarchical to:	No other components
Dependencies:	FIA_X509_EXT.2 X.509 Certificate Authentication

FIA_X509_EXT.1.1 The TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certification path validation.
- The certification path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [selection: *the Online Certificate Status Protocol (OCSP) as specified in RFC 6960, a Certificate Revocation List (CRL) as specified in RFC 5280 Section 6.3, Certificate Revocation List (CRL) as specified in RFC 5759 Section 5, no revocation method*]
- The TSF shall validate the extendedKeyUsage field according to the following rules: *[assignment: rules that govern contents of the extendedKeyUsage field that need to be verified]*.

FIA_X509_EXT.1.2 The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

FIA_X509_EXT.2 X.509 Certificate Authentication

FIA_X509_EXT.2 – X.509 Certificate Authentication

Hierarchical to:	No other components
Dependencies:	FIA_X509_EXT.1 X.509 Certificate Validation

FIA_X509_EXT.2.1 The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [selection*: DTLS, HTTPS, IPsec, TLS, SSH, [assignment: other protocols], no protocols*], and [selection: *code signing for system software updates [assignment: other uses], no additional uses*].

FIA_X509_EXT.2.2 When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall [selection: *allow the Administrator to choose whether to accept the certificate in these cases, accept the certificate, not accept the certificate*].

FIA_X509_EXT.3 X.509 Certificate Request

FIA_X509_EXT.3 – X.509 Certificate Request

FIA_X509_EXT.3.1 The TSF shall generate a Certificate Request as specified by RFC 2986 and be able to provide the following information in the request: public key and [selection: *device-specific information, Common Name, Organization, Organizational Unit, Country, [assignment: other information]*].

FIA_X509_EXT.3.2 The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.

Protection of the TSF (FPT)

Protection of the TSF (FPT_SKP_EXT)

Family Behaviour

Components in this family address the requirements for managing and protecting TSF data, such as cryptographic keys. This is a new family modelled after the FPT_PTD Class.

Component levelling

FPT_SKP_EXT Protection of TSF Data
1

FPT_SKP_EXT.1 Protection of TSF Data (for reading all symmetric keys), requires preventing symmetric keys from being read by any user or subject. It is the only component of this family.

Management: FPT_SKP_EXT.1

The following actions could be considered for the management functions in FMT:

a) There are no management activities foreseen.

Audit: FPT_SKP_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) There are no auditable events foreseen.

FPT_SKP_EXT.1 Protection of TSF Data (for reading of all symmetric keys)

FPT_SKP_EXT.1 – Protection of TSF Data (for reading of all symmetric keys)

Hierarchical to:	No other components
Dependencies:	No other components

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

Protection of Administrator Passwords (FPT_APW_EXT)

FPT_APW_EXT.1 Protection of Administrator Passwords

Family Behaviour

Components in this family ensure that the TSF will protect plaintext credential data such as passwords from unauthorized disclosure.

Component levelling

FPT_APW_EXT.1 Protection of Administrator passwords requires that the TSF prevent plaintext credential data from being read by any user or subject.

Management: FPT_APW_EXT.1

The following actions could be considered for the management functions in FMT:

a) No management functions.

Audit: FPT_APW_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) No audit necessary.

FPT_APW_EXT.1 – Protection of Administrator Passwords

Hierarchical to:	No other components
Dependencies:	No other components

FPT_APW_EXT.1.1 The TSF shall store administrative passwords in non-plaintext form.

FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext administrative passwords.

TSF Self-Test (FPT_TST_EXT)

FPT_TST_EXT.1 TSF Testing

Family Behaviour

Components in this family address the requirements for self-testing the TSF for selected correct operation.

Component levelling

FPT_TST_EXT TSF Self Test
1

FPT_TST_EXT.1 TSF Self-Test requires a suite of self-tests to be run during initial start-up in order to demonstrate correct operation of the TSF.

Management: FPT_TST_EXT.1

The following actions could be considered for the management functions in FMT:

a) No management functions.

Audit: FPT_TST_EXT.1

The following actions should be considered for audit if FAU_GEN Security audit data generation is included in the PP/ST:

a) Indication that TSF self-test was completed
b) Failure of self-test

FPT_TST_EXT.1 – TSF Testing

Hierarchical to:	No other components
Dependencies:	No other components

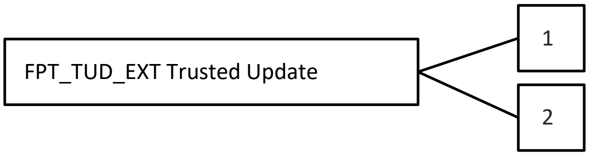
FPT_TST_EXT.1.1 The TSF shall run a suite of the following self-tests [selection: *during initial start-up (on power on), periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self-tests should occur]*] to demonstrate the correct operation of the TSF: *[assignment: list of self-tests run by the TSF*].

Trusted Update (FPT_TUD_EXT)

Family Behaviour

Components in this family address the requirements for updating the TOE firmware and/or software.

Component levelling



FPT_TUD_EXT.1 Trusted Update requires management tools be provided to update the TOE firmware and software, including the ability to verify the updates prior to installation.

FPT_TUD_EXT.2 Trusted update based on certificates applies when using certificates as part of trusted update and requires that the update does not install if a certificate is invalid.

Management: FPT_TUD_EXT.1, FPT_TUD_EXT.2

The following actions could be considered for the management functions in FMT:

a) Ability to update the TOE and to verify the updates
b) Ability to update the TOE and to verify the updates using the digital signature capability (FCS_COP.1/SigGen) and [selection: *no other functions, [assignment: other cryptographic functions (or other functions) used to support the update capability]*]
c) Ability to update the TOE, and to verify the updates using [selection: *digital signature, published hash, no other mechanism*] capability prior to installing those updates

Audit: FPT_TUD_EXT.1, FPT_TUD_EXT.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Initiation of the update process.
b) Any failure to verify the integrity of the update

FPT_TUD_EXT.1 – Trusted Update

Hierarchical to: No other components

Dependencies: FCS_COP.1/SigGen Cryptographic operation (for Cryptographic Signature and Verification), or
FCS_COP.1/Hash Cryptographic operation (for cryptographic hashing)

FPT_TUD_EXT.1.1 The TSF shall provide [assignment: *Administrators*] the ability to query the currently executing version of the TOE firmware/software and [selection: *the most recently installed version of the TOE firmware/software; no other TOE firmware/software version*].

FPT_TUD_EXT.1.2 The TSF shall provide [assignment: *Administrators*] the ability to manually initiate updates to TOE firmware/software and [selection: *support automatic checking for updates, support automatic updates, no other update mechanism*].

FPT_TUD_EXT.1.3 The TSF shall provide means to authenticate firmware/software updates to the TOE using a [selection: *X.509 certificate, digital signature, published hash*] prior to installing those updates.

FPT_TUD_EXT.2 Trusted Update Based on Certificates

FPT_TUD_EXT.2 – Trusted Update Based on Certificates

Hierarchical to: No other components

Dependencies: FPT_TUD_EXT.1

FPT_TUD_EXT.2.1 The TSF shall check the validity of the code signing certificate before installing each update.

FPT_TUD_EXT.2.2 If revocation information is not available for a certificate in the trust chain that is not a trusted certificate designated as a trust anchor, the TSF shall [selection: *not install the update, allow the Administrator to choose whether to accept the certificate in these cases*].

FPT_TUD_EXT.2.3 If the certificate is deemed invalid because the certificate has expired, the TSF shall [selection: *allow the Administrator to choose whether to install the update in these cases, not accept the certificate*].

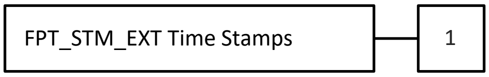
FPT_TUD_EXT.2.4 If the certificate is deemed invalid for reasons other than expiration or revocation information being unavailable, the TSF shall not install the update.

Time stamps (FPT_STM_EXT)

Family Behaviour

Components in this family extend FPT_STM requirements by describing the source of time used in timestamps.

Component levelling


FPT_STM_EXT Time Stamps
1

FPT_STM_EXT.1 Reliable Time Stamps is hierarchic to FPT_STM.1: it requires that the TSF provide reliable time stamps for TSF and identifies the source of the time used in those timestamps.

Management: FPT_STM_EXT.1

The following actions could be considered for the management functions in FMT:

a) Management of the time
b) Administrator setting of the time.

Audit: FTA_SSL_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Discontinuous changes to the time.

FPT_STM_EXT.1 Reliable Time Stamps

FPT_STM_EXT.1 – Reliable Time Stamps

Hierarchical to: No other components

Dependencies: No other components

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

FPT_STM_EXT.1.2 The TSF shall [selection: *allow the Security Administrator to set the time, synchronise time with an NTP server*].

TOE Access (FTA)

TSF-initiated Session Locking (FTA_SSL_EXT)

Family Behaviour

Components in this family address the requirements for TSF-initiated and user-initiated locking, unlocking, and termination of interactive sessions.

The extended FTA_SSL_EXT family is based on the FTA_SSL family.

Component levelling

FTA_SSL_EXT TSF-initiated session locking
1

FTA_SSL_EXT.1 TSF-initiated session locking, requires system initiated locking of an interactive session after a specified period of inactivity. It is the only component of this family.

Management: FTA_SSL_EXT.1

The following actions could be considered for the management functions in FMT:

a) Specification of the time of user inactivity after which lock-out occurs for an individual user.

Audit: FTA_SSL_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

b) Any attempts at unlocking an interactive session.

FTA_SSL_EXT.1 TSF-initiated Session Locking

FTA_SSL_EXT.1 – TSF-initiated Session Locking

Hierarchical to:	No other components
Dependencies:	FIA_UAU.1 Timing of authentication

FCO_CPC_EXT Communication Partner Control
1

FTA_SSL_EXT.1.1 The TSF shall, for local interactive sessions, [selection:

- *lock the session - disable any activity of the Administrator's data access/display devices other than unlocking the session, and requiring that the Administrator re-authenticate to the TSF prior to unlocking the session;*

- *terminate the session*]

after a Security Administrator-specified time period of inactivity.

Communication (FCO)

Communication Partner Control (FCO_CPC_EXT)

Family Behaviour

This family is used to define high-level constraints on the ways that partner IT entities communicate. For example, there may be constraints on when communication channels can be used, how they are established, and links to SFRs expressing lower-level security properties of the channels.

Component levelling

FCO_CPC_EXT.1 Component Registration Channel Definition, requires the TSF to support a registration channel for joining together components of a distributed TOE, and to ensure that the availability of this channel is under the control of an Administrator. It also requires statement of the type of channel used (allowing specification of further lower-level security requirements by reference to other SFRs).

Management: FCO_CPC_EXT.1

No separate management functions are required. Note that elements of the SFR already specify certain constraints on communication in order to ensure that the process of forming a distributed TOE is a controlled activity.

Audit: FCO_CPC_EXT.1

The following actions should be auditable if FCO_CPC_EXT.1 is included in the PP/ST:

a) Enabling communications between a pair of components as in FCO_CPC_EXT.1.1 (including identities of the endpoints).
b) Disabling communications between a pair of components as in FCO_CPC_EXT.1.3 (including identity of the endpoint that is disabled).

If the required types of channel in FCO_CPC_EXT.1.2 are specified by using other SFRs then the use of the registration channel may be sufficiently covered by the audit requirements on those SFRs: otherwise a separate audit requirement to audit the use of the channel should be identified for FCO_CPC_EXT.1.

FCO_CPC_EXT.1 Component Registration Channel Definition

FCO_CPC_EXT.1 – Component Registration Channel Definition

Hierarchical to: No other components

Dependencies: No other components

FCO_CPC_EXT.1.1 The TSF shall require a Security Administrator to enable communications between any pair of TOE components before such communication can take place.

FCO_CPC_EXT.1.2 The TSF shall implement a registration process in which components establish and use a communications channel that uses [assignment: *list of different types of channel given in the form of a selection*] for at least [assignment: *type of data for which the channel must be used*].

FCO_CPC_EXT.1.3 The TSF shall enable a Security Administrator to disable communications between any pair of TOE components.

References

The documentation listed below was used to prepare this ST

Table 26. 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
[NDcPP]	collaborative Protection Profile for Network Devices, version 2.2e, March 23, 2020
[SD]	Supporting Document – Evaluation Activities for Network Device cPP, version 2.2, December-2019

Identifier	Description
[WLAN_EP]	Wireless Local Area Network (WLAN) Access Systems Extended Package, version 1.0, May 29, 2015
[IEEE 802.11-2012]	IEEE Standard for Information technology—Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications
[IEEE 802.11ac-2013]	Amendment 4: Enhancements for Very High Throughput for Operation in Bands below 6 GHz
[IEEE 802.1X-2010]	IEEE Standard for Local and metropolitan area networks—Port-Based Network Access Control
ISO 18033-3	Information technology -- Security techniques -- Encryption algorithms -- Part 3: Block ciphers
ISO 10116	Information technology -- Security techniques -- Modes of operation for an n-bit block cipher
ISO 19772	Information technology -- Security techniques -- Authenticated encryption
ISO/IEC 10118-3:2004	Information technology -- Security techniques -- Hash-functions -- Part 3: Dedicated hash-functions
ISO/IEC 9797-2:2011	Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 2: Mechanisms using a dedicated hash-function
ISO/IEC 18031:2011	Information technology -- Security techniques -- Random bit generation
NIST SP800-38C	Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality
NIST SP800-38D	Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC

Acronyms and Terms

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

Table 27. Acronyms and Terms

Acronym/Term	Definition
AAA	Administration, Authorization, and Accounting
ACL	Access Control Lists
AES	Advanced Encryption Standard
AES-CCM	AES Counter with CBC-MAC
AP	Access Point
BLE	Bluetooth Low Energy
CAPWAP	Control and Provisioning of Wireless Access Points
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
DHCP	Dynamic Host Configuration Protocol

EAL	Evaluation Assurance Level
EAP	Extensible Authentication Protocol
EAPoL	Extensible Authentication Protocol (EAP) over LAN
ESP	Encapsulating Security Payload
GE	Gigabit Ethernet port
GMK	Group Master Key
GTK	Group Temporal Key
HTTP	Hyper-Text Transport Protocol
HTTPS	Hyper-Text Transport Protocol Secure
ICMP	Internet Control Message Protocol
IT	Information Technology
KCK	Key Confirmation Key
KEK	Key Encryption Key
MIC	Message Integrity Check
MU-MIMO	Multi-User Multiple-Input Multiple-Output
NDcPP	collaborative Network Device Protection Profile
OFDMA	Orthogonal Frequency-Division Multiple Access
OS	Operating System
PMK	Pairwise Master Key
PoE	Power over Ethernet
PRF	Pseudo-random function
PP	Protection Profile
PTK	Pairwise Transient Key
RSN	Robust Security Network
SA	Security Association
SFP	Small–form-factor pluggable port
SHS	Secure Hash Standard
SSHv2	Secure Shell (version 2)
SSID	Service Set Identifier
ST	Security Target
Supplicant	The client software used for WLAN authentication

TCP	Transport Control Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
UDP	User datagram protocol
WAN	Wide Area Network

Obtaining Documentation and Submitting a Service Request

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

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

Contacting Cisco

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