# Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.12

# Security Target

**Version:** 1.2
**Date:** April 6, 2025

# Table of Contents

Document Introduction ..... 8
1. Security Target Introduction ..... 10
1.1. ST and TOE Reference ..... 10
1.2. TOE Overview ..... 12
1.3. TOE Product Type ..... 12
1.4. Required non-TOE Hardware/Software/Firmware ..... 12
1.5. TOE Description ..... 14
1.6. TOE Evaluated Configuration ..... 14
1.7. Physical Scope of the TOE ..... 16
1.8. Logical Scope of the TOE ..... 22
Security Audit ..... 22
Communication ..... 23
Cryptographic Support ..... 23
Identification and Authentication ..... 23
Security Management ..... 24
Protection of the TSF ..... 24
TOE Access ..... 24
Trusted Path/Channels ..... 25
1.9. Excluded Functionality ..... 25
2. Conformance Claims ..... 26
2.1. Common Criteria Conformance Claim ..... 26
2.2. PP Configuration Conformance Claim ..... 26
2.3. Protection Profile Conformance Claim Rationale ..... 29
2.3.1. TOE Appropriateness ..... 29
2.3.2. TOE Security Problem Definition Consistency ..... 29
2.3.3. Statement of Security Requirements Consistency ..... 29
3. Security Problem Definition ..... 30

3.1. Assumptions ..... 30
3.2. Threats ..... 33
3.3. Organizational Security Policies ..... 37
4. Security Objectives ..... 38
4.1. Security Objectives for the TOE ..... 38
4.2. Security Objectives for the Environment ..... 38
5. Security Requirements ..... 41
5.1. Conventions ..... 41
5.2. Class: Security Audit (FAU) ..... 46
5.2.1. FAU_GEN.1 – Audit Data Generation ..... 46
5.2.2. FAU_GEN.1/WLAN – WLAN Audit Data Generation ..... 50
5.2.3. FAU_GEN.2 – User Identity Association ..... 52
5.2.4. FAU_GEN_EXT.1 – Security Audit Generation ..... 52
5.2.5. FAU_STG.1 – Protected Audit Trail Storage ..... 52
5.2.6. FAU_STG_EXT.1 – Protected Audit Event Storage ..... 52
5.2.7. FAU_STG_EXT.4 – Protected Local Audit Event Storage for Distributed TOEs ..... 53
5.2.8. FAU_STG_EXT.5 – Protected Remote Audit Event Storage for Distributed TOEs ..... 53
5.3. Class: Communication Partner Control (FCO) ..... 53
5.3.1. FCO_CPC_EXT.1 – Component Registration Channel Definition ..... 53
5.4. Class: Cryptographic Support (FCS) ..... 53
5.4.1. FCS_CKM.1 – Cryptographic Key Generation (Refinement) ..... 53
5.4.2. FCS_CKM.2 – Cryptographic Key Establishment (Refinement) ..... 54
5.4.3. FCS_CKM.1/WPA – Cryptographic Key Generation (Symmetric Keys for WPA2 Connections) ..... 54
5.4.4. FCS_CKM.2/GTK – Cryptographic Key Distribution (GTK) ..... 54
5.4.5. FCS_CKM.2/PMK – Cryptographic Key Distribution (PMK) ..... 54
5.4.6. FCS_CKM.2/DISTRIB – Cryptographic Key Distribution (802.11 Keys) ..... 54
5.4.7. FCS_CKM.4 – Cryptographic Key Destruction ..... 55
5.4.8. FCS_COP.1/DataEncryption – Cryptographic Operation (AES Data Encryption/Decryption) ..... 55

5.4.9. FCS_COP.1/SigGen – Cryptographic Operation (Signature Generation and Verification) ..... 55
5.4.10. FCS_COP.1/Hash – Cryptographic Operation (Hash Algorithm) ..... 56
5.4.11. FCS_COP.1/KeyedHash – Cryptographic Operation (Keyed Hash Algorithm) ..... 56
5.4.12. FCS_RBG_EXT.1 – Random Bit Generation ..... 56
5.4.13. FCS_IPSEC_EXT.1 – IPsec Protocol ..... 56
5.4.14. FCS_SSHS_EXT.1 – SSH Server Protocol ..... 58
5.4.15. FCS_RADSEC_EXT.1 – RADsec ..... 58
5.4.16. FCS_TLSC_EXT.1/RADsec – TLS Client Protocol Without Mutual Authentication ..... 58
5.4.17. FCS_TLSC_EXT.1/EST – TLS Client Protocol Without Mutual Authentication ..... 59
5.4.18. FCS_TLSC_EXT.2 – TLS Client Support for Mutual Authentication ..... 59
5.4.19. FCS_DTLSS_EXT.1 – DTLS Server Protocol Without Mutual Authentication ..... 60
5.4.20. FCS_DTLSS_EXT.2 – DTLS Server Support for Mutual Authentication ..... 60
5.4.21. FCS_DTLSC_EXT.1 – DTLS Client Protocol Without Mutual Authentication ..... 60
5.4.22. FCS_DTLSC_EXT.2 – DTLS Client Support for Mutual Authentication ..... 61
5.4.23. FCS_HTTPS_EXT.1 – HTTPS Protocol ..... 61
5.4.24. FCS_TLSS_EXT.1 – TLS Server Protocol Without Mutual Authentication ..... 61
5.5. Class: Identification and Authentication (FIA) ..... 62
5.5.1. FIA_AFL.1 – Authentication Failure Management ..... 62
5.5.2. FIA_PMG_EXT.1 – Password Management ..... 62
5.5.3. FIA_PSK_EXT.1 – Extended: Pre-Shared Key Composition ..... 64
5.5.4. FIA_UIA_EXT.1 – User Identification and Authentication ..... 64
5.5.5. FIA_UAU_EXT.2 – Password-based Authentication Mechanism ..... 64
5.5.6. FIA_UAU.6 – Re-authenticating ..... 64
5.5.7. FIA_UAU.7 – Protected Authentication Feedback ..... 64
5.5.8. FIA_8021X_EXT.1 – Extended: 802.1X Port Access Entity (Authenticator) Authentication ..... 64
5.5.9. FIA_X509_EXT.1/Rev – X.509 Certificate Validation ..... 65
5.5.10. FIA_X509_EXT.1/ITT – X.509 Certificate Validation ..... 65
5.5.11. FIA_X509_EXT.2 – X.509 Certificate Authentication ..... 66

5.5.12. FIA_X509_EXT.3 – X.509 Certificate Requests ..... 66
5.6. Class: Security Management (FMT) ..... 66
5.6.1. FMT_MOF.1/ManualUpdate – Management of Security Functions Behavior ..... 66
5.6.2. FMT_MOF.1/Services – Management of Security Functions Behavior ..... 66
5.6.3. FMT_MOF.1/Functions – Management of Security Functions Behavior ..... 67
5.6.4. FMT_MTD.1/CoreData – Management of TSF Data ..... 67
5.6.5. FMT_MTD.1/CryptoKeys – Management of TSF Data ..... 67
5.6.6. FMT_SMF.1 – Specification of Management Functions ..... 67
5.6.7. FMT_SMF.1/AccessSystem – Specification of Management Functions (WLAN Access Systems) ..... 68
5.6.8. FMT_SMR_EXT.1 – No Administration from Client ..... 68
5.6.9. FMT_SMR.2 – Restrictions on Security Roles ..... 68
5.7. Class: Protection of the TSF (FPT) ..... 69
5.7.1. FPT_SKP_EXT.1 – Protection of TSF Data (for reading of all pre-shared, symmetric and private keys) ..... 69
5.7.2. FPT_APW_EXT.1 – Protection of Administrator Passwords ..... 69
5.7.3. FPT_FLS.1 – Failure with Preservation of Secure State ..... 69
5.7.4. FPT_STM_EXT.1 – Reliable Time Stamps ..... 69
5.7.5. FPT_TST_EXT.1 – TSF Testing ..... 69
5.7.6. FPT_TUD_EXT.1 – Trusted Update ..... 69
5.7.7. FPT_ITT.1 – Basic Internal TSF Data Transfer Protection ..... 70
5.8. Class: TOE Access (FTA) ..... 70
5.8.1. FTA_SSL_EXT.1 – TSF-initiated Session Locking ..... 70
5.8.2. FTA_SSL.3 – TSF-initiated Termination ..... 70
5.8.3. FTA_SSL.4 – User-initiated Termination ..... 70
5.8.4. FTA_TAB.1 – Default TOE Access Banners ..... 70
5.8.5. FTA_TSE.1 – TOE Session Establishment ..... 70
5.9. Class: Trusted Path/Channels (FTP) ..... 70
5.9.1. FTP_ITC.1 – Inter-TSF Trusted Channel ..... 70
5.9.2. FTP_ITC.1/Client Inter-TSF Trusted Channel (WLAN Client Communications) ..... 71

5.9.3. FTP_TRP.1/Admin – Trusted Path ..... 71
5.10. TOE SFR Dependencies Rationale ..... 71
5.11. Security Assurance Requirements Rationale ..... 71
5.12. Assurance Measures ..... 72
6. TOE Summary Specification ..... 73
6.1. Key Zeroization ..... 112
6.2. CAVP Certificates ..... 116
6.3. Wi-Fi Alliance Certificates ..... 120
6.4. Auditing ..... 121
7. References ..... 124
7.1. Acronyms and Terms ..... 126
7.2. Obtaining Documentation and Submitting a Service Request ..... 128
7.3. Contacting Cisco ..... 128

# Table of Tables

Table 1. ST and TOE Identification ..... 10
Table 2. IT Environment Components ..... 12
Table 3. Hardware Models and Specifications ..... 16
Table 4. TOE Software ..... 22
Table 5. Excluded Functionality and Rationale ..... 25
Table 6. PP Configuration Conformance ..... 26
Table 7. NIAP Technical Decisions ..... 26
Table 8. TOE Assumptions ..... 30
Table 9. Threats ..... 33
Table 10. Organizational Security Policies ..... 37
Table 11. Security Objectives for the TOE ..... 38
Table 12. Security Objectives for the Environment ..... 39
Table 13. Security Requirement Conventions ..... 41
Table 14. Security Functional Requirements ..... 41
Table 15. Auditable Events ..... 47
Table 16. WLAN Auditable Events ..... 51

Table 17. TOE Component Storing Audit Data Locally ..... 53
Table 18. Additional Password Special Characters ..... 63
Table 19. Assurance Measures ..... 72
Table 20. TSS Rationale ..... 73
Table 21. Key Zeroization ..... 113
Table 22. CAVP Certificates ..... 116
Table 23. Wi-Fi Alliance Certificates ..... 120
Table 24. TOE Component Audit Event Mapping ..... 121
Table 25. References ..... 125
Table 26. Acronyms and Terms ..... 126

# Table of Figures

Figure 1. TOE and Environment ..... 15
Figure 2. EAP Message Exchange ..... 79
Figure 3. Four-Way Handshake ..... 80

# 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 17.12. 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 18, 2023 | Initial Version |
| 0.2 | August 29, 2023 | Updates to address ORs |
| 0.3 | February 15, 2024 | Additional updates |
| 0.4 | March 19, 2024 | Updates to address CAVP ORs |
| 0.5 | April 5, 2024 | Additional Pre-Check-in updates |
| 0.6 | May 9, 2024 | Additional Pre-Check-in updates |
| 0.7 | May 29, 2024 | Updates in response to Issue Tracking 1 |
| 0.8 | September 30, 2024 | Update in response to OR6 |
| 0.9 | October 16, 2024 | Updates in response to ECR |
| 1.0 | January 29, 2025 | Updates from testing |
| 1.1 | March 5, 2025 | Updates for checkout package |
| 1.2 | April 6, 2025 | Updates to response to checkout ECR |

# 1. Security Target Introduction

This Security Target contains the following sections:

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

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

## 1.1. ST and TOE Reference

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

**Table 1. ST and TOE Identification**

| Name | Description |
|---|---|
| ST Title | Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.12 Security Target |
| ST Version | 1.2 |
| Publication Date | April 6, 2025 |
| Vendor and ST Author | Cisco Systems, Inc. |
| TOE Reference | Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.12.04 |

| | |
|---|---|
| TOE Hardware Models | Cisco 9800-80-K9 Wireless Controller:<br>■ C9800-80-K9<br>Cisco 9800-40-K9 Wireless Controller:<br>■ C9800-40-K9<br>Cisco 9800-L Wireless Controller:<br>■ C9800-L-F-K9<br>■ C9800-L-C-K9<br>Cisco Catalyst 9800-CL-K9 Wireless Controller for Private Cloud (vSphere):<br>■ C9800-CL-K9<br>Cisco Catalyst 9166I Series Access Points (x = regulatory domain):<br>■ CW9166I-x<br>■ CW9166D1-x<br>Cisco Catalyst 9164I Series Access Points (x = regulatory domain):<br>■ CW9164I-x<br>Cisco Catalyst 9162I Series Access Points (x = regulatory domain):<br>■ CW9162I-x<br>Cisco Catalyst 9136I Series Access Points (x = regulatory domain):<br>■ C9136I-x<br>Cisco Catalyst 9130AX Series Wi-Fi 6 Access Points (x = regulatory domain):<br>■ C9130AXI-x<br>■ C9130AXE-x<br>■ C9130AXE-STA-x |

| | |
|---|---|
| | Cisco Catalyst 9124AX Series Access Points (x = regulatory domain):<br>■ C9124AXI-x<br>■ C9124AXD-x<br>■ C9124AXE-x<br>Cisco Catalyst IW9167 Heavy Duty Access Point (x = regulatory domain):<br>■ IW9167EH-x-AP<br>■ IW9167IH-x-AP |
| TOE Software Version | IOS-XE 17.12.04 |
| Keywords | WLAN, Wireless, Access Point |

## 1.2. 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 administrators, the TOE provides central management and administration of the wireless infrastructure within an organization.

### 1.3. 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.

### 1.4. 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. IT Environment Components**

| Component | Usage/Purpose/Description | Required |
|---|---|---|

| | | |
|---|---|---|
| Wireless Client | Allows users to establish wireless communications with an organization's private network through the TOE | Yes |
| EST Server | The EST Server[1] authenticates EST Clients and determines if the EST Client is authorized to receive the certificate it has requested. | Yes |
| 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. | Yes |
| 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). | Yes |
| 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. | Yes |
| 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. | Yes |
| Syslog Server | This includes any syslog server to which the TOE would transmit syslog messages over a trusted channel. | Yes |
| 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. | No |
| DHCP Server | Use of a DHCP server allows the AP to automatically discover the IP address of the controller to which it joins. | No |

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

### 1.5. TOE Description

The Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.12 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, 5, and 6 GHz wireless radios and implements functions from the IEEE 802.11 standard to communicate over-the-air directly to wireless client radios. This 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.

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 802.11-2020 standard. AES-CCMP-128 bit encryption as specified in 802.11-2020 is more commonly known by its Wi-Fi Alliance certification name, WPA3-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 802.11ax-2021 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.

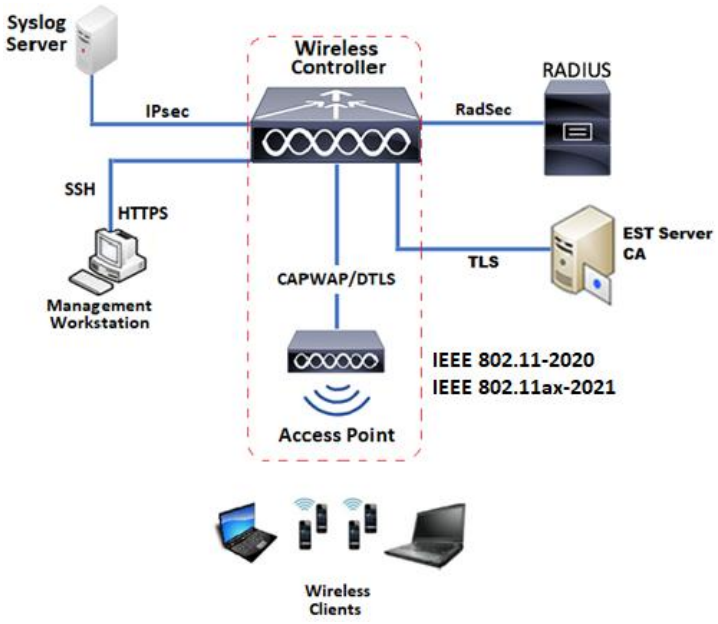
For connections to the Syslog audit server, the WLC authenticates those devices with X.509v3 certificates and protects communication channels with the IPsec protocol. For RADIUS, the WLC protects communication to the RADIUS authentication server with RADsec. Secure remote administration is protected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

## 1.6. TOE Evaluated Configuration

The Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.12 TOE is distributed. Deployment of the TOE in its evaluated configuration consists of one Wireless LAN Controller (WLC) model and at least one Access Point (AP). 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 vND evaluated configuration 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.

## 1.7. 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<br>■ Form factor: 2RU<br>■ Memory: 64GB, DDR4<br>■ Storage: 32 GB eUSB, 2x SSD<br>■ Control plane CPU: Intel Xeon Silver 4116T<br>■ Ports:<br>o 1x RJ-45 console port<br>o 1x USB 3.0 console port<br>o 2x USB 3.0 ports<br>o 1x RJ-45 management port<br>o 1x RJ-45 redundancy port<br>o 1x SFP Gigabit Ethernet redundancy port<br>o 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<br>■ Form factor: 1 RU<br>■ Memory: 32GB, DDR4<br>■ Storage: 32 GB eUSB<br>■ Control plane CPU: Intel Xeon Broadwell D-1548<br>■ Ports:<br>o 1x RJ-45 console port<br>o 1x USB 3.0 console port<br>o 2x USB 3.0 ports<br>o 1x RJ-45 management port<br>o 1x RJ-45 redundancy port |

| | | |
|---|---|---|
| | | ○ 1x SFP Gigabit Ethernet redundancy port<br>○ 4x 10 GE/1 GE SFP+ or SFP ports |
| Cisco Catalyst 9800-L Wireless Controller<br>  | C9800-L-F-K9<br>C9800-L-C-K9 | ■ Available in Fiber or Copper Uplink<br>■ Supports up to 5000 access points, 10,000 clients, and up to 10 Gbps throughput.<br>■ Form factor: 1 RU<br>■ Memory: 16GB, DDR4<br>■ Storage: 32 GB eUSB<br>■ CPU: Intel Xeon Broadwell D-1563N<br>■ Ports:<br>○ 1x RJ-45 management port<br>○ 1x RJ-45 redundancy port<br>○ 4x RJ-45 2.5 GE AP ports<br>○ 1x USB 3.0 console port<br>○ 1x USB 2.0 Micro-B port<br>○ 1x RJ-45 console port |
| Cisco Catalyst 9800-CL Wireless Controller for Private Cloud (vSphere)<br>  | 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:<br>  <br>■ UCSC-C220-M5<br>  <br>■ UCSC-C240-M5<br>  <br>■ UCSC-C480-M5 |

| | | |
|---|---|---|
| | | The specifications of VMware ESXi 6.x is dependent on the desired scale and sizing:<br>■ **Small**: Designed for distributed branches and small campuses supporting up to 1000 Access Points (APs) and 10,000 clients:<br>o Minimum Number of vCPUs: 4<br>o Minimum Memory (GB): 8GB<br>o Required Storage (GB): 8GB<br>o Minimum vNICs: 2<br>■ **Medium**: Designed for medium-sized campuses supporting up to 3000 APs and 32,000 clients:<br>o Minimum Number of vCPUs: 6<br>o Minimum Memory (GB): 16GB<br>o Required Storage (GB): 8GB<br>o Minimum vNICs: 2<br>■ **Large**: Designed for large enterprises and service providers supporting up to 6000 APs and 64,000 clients:<br>o Minimum Number of vCPUs: 10<br>o Minimum Memory (GB): 32GB<br>o Required Storage (GB): 8GB<br>o Minimum vNICs: 2<br><br>The specifications of the UCSC-C220-M5 and UCSC-C240-M5 are:<br>■ Form factor: 1 RU (C220-M5); 2 RU (C240-M5)<br>■ Memory: Up to 24 DDR4 DIMMs<br>■ Ports:<br>o 1x RJ-45 console port<br>o 2x USB 3.0 ports<br>o 1x RJ-45 management port<br>o 2x 10GTbase-T ports<br>o VGA connector<br>o 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]<br><br>The specifications of the UCSC-C480-M5 is:<br>■ Form factor: 4 RU<br>■ Memory: Up to 48 DDR4 DIMMs<br>■ Ports:<br>o 1x RJ-45 console port<br>o 3x USB 3.0 ports<br>o 1x RJ-45 management port<br>o 2x 10GTbase-T ports<br>o VGA connector<br>o Serial port (RS232)<br>■ CPU: Intel Xeon Skylake SP (Skylake microarchitecture)[2] |
| Cisco Catalyst 9166 Series Wi-Fi 6 and Wi-Fi 6E Access Points<br>  | CW9166I-x<br>CW9166D1-x | ■ Interfaces:<br>o 1x 100M/1000M/2.5G/5G Multigigabit Ethernet (RJ-45)<br>o Management console port (RJ-45)<br>o USB 2.0 at 4.5<br><br>■ Radios: Five radios: 2.4 GHz (4x4), 5 GHz (4x4), 6 GHz (4x4), IoT radio, and band steering radio<br><br>■ CPU: Qualcomm IPQ8076 ARMv8 |
| Cisco Catalyst 9164I Series Wi-Fi 6 and Wi-Fi 6E Access Points<br>  | CW9164I-x | ■ Interfaces:<br>o 1x 100M/1000M/2.5G/5G Multigigabit Ethernet (RJ-45)<br>o Management console port (RJ-45)<br>o USB 2.0 at 4.5W<br><br>■ Radios: Five radios: 2.4 GHz (2x2), 5 GHz (4x4), 6 GHz (4x4), IoT radio, and scanning radio<br><br>■ CPU: Qualcomm IPQ8076 ARMv8 |

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

| | | |
|---|---|---|
| Cisco Catalyst 9162I Series Wi-Fi 6 and Wi-Fi 6E Access Points<br>  | CW9162I-x | ■ Interfaces:<br>o 1x 100M/1000M/2.5G/5G Multigigabit Ethernet (RJ-45)<br>o Management console port (RJ-45)<br>o USB 2.0 at 4.5W<br>■ Radios: Five radios: 2.4 GHz (2x2), 5 GHz (2x2), 6 GHz (2x2), IoT radio, and scanning radio<br>■ CPU: Qualcomm IPQ6010 ARMv8 |
| Cisco Catalyst 9136I Series Access Points<br>  | C9136I-x | ■ Interfaces:<br>o 2x 100M/1000M/2.5G/5G Multigigabit Ethernet (RJ-45)<br>o Management console port (RJ-45)<br>o USB 2.0 at 9W<br>■ Radios: Six radios: 2.4 GHz (4x4), 5 GHz (8x8 and 4x4), 6 GHz (4x4), scanning radio, and BLE/IoT<br>■ CPU: Qualcomm IPQ8078 ARMv8 |
| Cisco Catalyst 9130AX Series Wi-Fi 6 Access Points<br>  | C9130AXI-x[3]<br>C9130AXE-x<br>C9130AXE-STA-x | ■ Interfaces:<br>o 1x100/1000/2500 Multigigabit Ethernet (RJ-45)<br>o RS-232 Console Interface through RJ-45<br>o Recovery push button (enables partial or full system configuration recovery)<br>o USB 2.0 Port<br>■ Radios: Up to five radios: 2.4 GHz (4x4), 5 GHz (8x8 and 4x4), Cisco RF ASIC, and BLE/IoT<br>■ CPU: Qualcomm IPQ8078 ARMv8 |

[3] x = regulatory domain

| | | |
|---|---|---|
| Cisco Catalyst 9124AX Series Access Points<br>  | C9124AXI-x<br>C9124AXD-x<br>C9124AXE-x | ■ Interfaces:<br>○ 1x 100/1000/2500 BASE-T (Ethernet) uplink interface<br>○ 1x Gigabit Ethernet SFP<br>○ Supports PoE output (802.3af compliant PSE) on the 1x 10/100/1000 BASE-T (Ethernet) downlink interface<br>○ Management console port (RJ-45<br>■ Radios: Up to three radios: 2.4 GHz (4x4:4), 5 GHz (4x4:4), and a built-in Bluetooth Low Energy (BLE) radio<br>■ CPU: Qualcomm IPQ8078 ARMv8 |
| Cisco Catalyst IW9167 Heavy Duty Access Point<br>  <br>  | IW9167EH-x-AP<br>IW9167IH-x-AP | ■ Interfaces:<br>1x 100M/1000M/2.5G/5G Multigigabit Ethernet (RJ-45)/M12 X-code autosensing PoE+ in (802.3at/bt), UPOE in<br>1x SFP (copper) 100M/1000M/10G Multigigabit Ethernet /M12 X-code<br>■ Radios: Three 4x4 radios: (1) 2.4 GHz, (2) 5 GHz<br>■ CPU: Qualcomm IPQ8076 ARMv8 |

The TOE hardware is shipped to customers via a commercial carrier.

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.17.12.04.SPA.bin |
| Cisco Catalyst 9800-40 | C9800-40-universalk9_wlc.17.12.04.SPA.bin |
| Cisco Catalyst 9800-80 | C9800-80-universalk9_wlc.17.12.04.SPA.bin |
| Cisco Catalyst 9800 Wireless Controller for Private Cloud - VMware ESXi | C9800-CL-universalk9.17.12.04.ova |

The AP software images v17.12.04 are embedded in each WLC v17.12.04 image and are not separately downloaded and installed.

The TOE includes the Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.12 CC Configuration Guide, v0.9, available for download in PDF format on the NIAP PCL alongside this ST.

## 1.8. 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

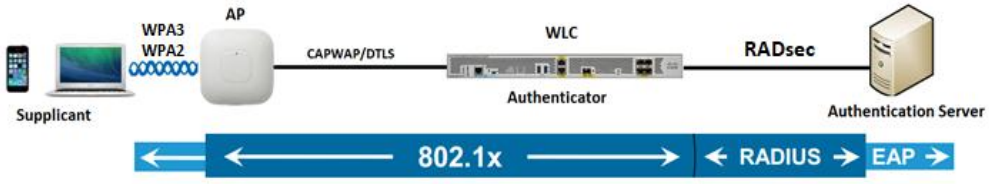
The TOE provides a secure internal channel, under control of the Security Administrator, for Access Points to register and join the WLC to form a distributed TOE.

### Cryptographic Support

The TOE provides cryptographic functions in order to implement HTTPS, TLS, DTLS, SSH, IPsec, WPA2, and IEEE 802.11ax-2021 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) Rel5a and CiscoSSL FOM 7.3 cryptographic modules. IC2M Rel5a applies to the WLC and CiscoSSL FOM 7.3 applies to the WLC and the AP. SSH and IPsec protocols are implemented using the IOS Common Cryptographic Module (IC2M) and TLS and DTLS protocols are implemented using the CiscoSSL FOM cryptographic modules. In addition, the IEEE 802.11 implementation has been validated by the Wi-Fi Alliance for WPA2 certification.

### Identification and Authentication

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




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 with a configurable minimum length 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 time period has elapsed or until the Administrator manually unblocks the account.

### 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 channels/paths between itself and remote endpoints and TOE administrators. Specifically, the TOE allows a trusted path to be established to itself from the remote authorized administrator over SSH and TLS/HTTPS. The TOE also initiates an outbound IPsec trusted channel to transmit audit messages to a remote syslog server. 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.

## 1.9. Excluded Functionality

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

**Table 5. 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 WPA2/3-Enterprise along with 802.1X with AES encryption will meet the requirements of the PP-Module for Wireless Local Area Network (WLAN) Access System, Version 1.0 (MOD_WLAN_AS_V1.0). |
| 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 PP-Module for Wireless Local Area Network (WLAN) Access System Version 1.0. The excluded functionality does not affect the TOE's conformance to the claimed Protection Profiles.

# 2. Conformance Claims

## 2.1. 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.

## 2.2. PP Configuration Conformance Claim

The TOE and ST are exact conformant with the PP-Configuration identified in the PP-Configuration column of Table 6.

**Table 6. PP Configuration Conformance**

| PP-Configuration | Component | Version | Date |
|---|---|---|---|
| PP-Configuration for Network Devices and Wireless Local Area Network Access Systems, 2022-04-21, Version 1.0, (CFG_ND_WLAN-AS_V1.0), which includes the components in the next column | Base-PP: collaborative Protection Profile for Network Devices (CPP_ND_V2.2E) | 2.2e | March 23, 2020 |
| | PP-Module: PP-Module for Wireless Local Area Network (WLAN) Access System, Version 1.0 (MOD_WLAN_AS_V1.0) | 1.0 | March 31, 2022 |

This ST applies the following NIAP Technical Decisions:

**Table 7. NIAP Technical Decisions**

| Number | Title | PP | Applicable | Exclusion Rational |
|---|---|---|---|---|
| TD0903 | Correction to Auditable Event for FTA_TSE.1 | [MOD_WLAN_AS] | Yes | |
| TD0832 | Aligning MOD_WLAN_AS 1.0 with NDcPP 3.0E | [MOD_WLAN_AS] | No | The ST does not claim conformance to NDcPP 3.0E |
| TD0807 | Corrections for WLAN AS CC Conformance | [MOD_WLAN_AS] | Yes | |
| TD0800 | Updated NIT Technical Decision for IPsec IKE/SA Lifetimes Tolerance | [NDcPP] | Yes | |

| Number | Title | PP | Applicable | Exclusion Rational |
|---|---|---|---|---|
| TD0792 | NIT Technical Decision: FIA_PMG_EXT.1 - TSS EA not in line with SFR | [NDcPP] | Yes | |
| TD0790 | NIT Technical Decision: Clarification Required for testing IPv6 | [NDcPP] | Yes | |
| TD0738 | NIT Technical Decision for Link to Allowed-With List | [NDcPP] | Yes | |
| TD0680 | OS 4.2.1 Conformance Claims section updated to allow for MOD_WLAN_CLI_v1.0 | [MOD_WLAN_AS] | Yes | |
| TD0679 | Handling Standalone WLANAS TOEs with Single Interfaces | [MOD_WLAN_AS] | Yes | |
| TD0670 | NIT Technical Decision for Mutual and Non-Mutual Auth TLSC Testing | [NDcPP] | Yes | |
| TD0651 | WLAN AS as Distributed and Non-distributed TOE | [MOD_WLAN_AS] | Yes | |
| TD0639 | NIT Technical Decision for Clarification for NTP MAC Keys | [NDcPP] | No | TOE does not claim FCS_NTP_EXT.1 |
| 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 | |
| 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 | |

| Number | Title | PP | Applicable | Exclusion Rational |
|---|---|---|---|---|
| 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 | |
| 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 | |

| Number | Title | PP | Applicable | Exclusion Rational |
|---|---|---|---|---|
| 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 | TOE does not claim FCS_NTP_EXT.1 |
| TD0527 | Updates to Certificate Revocation Testing (FIA_X509_EXT.1) | [NDcPP] | Yes | |

## 2.3. Protection Profile Conformance Claim Rationale

### 2.3.1. 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.

### 2.3.2. 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 [MOD_WLAN_AS] 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 [MOD_WLAN_AS] for which conformance is claimed verbatim. All concepts covered in the Protection Profile's Statement of Security Objectives are included in the Security Target.

### 2.3.3. Statement of Security Requirements Consistency

The Security Functional Requirements included in the Security Target represent the Security Functional Requirements specified in [NDcPP] and [MOD_WLAN_AS] 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.

# 3. 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 [MOD_WLAN_AS].

## 3.1. Assumptions

**Table 8. 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).<br><br>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.<br><br>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. |

## 3.2. Threats

**Table 9. 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 | Devices on a protected network may be exposed to threats presented by devices located outside the protected network, which may attempt to conduct unauthorized activities. If malicious external devices are able to communicate with devices on the protected network, or if devices on the protected network can establish communications with those external devices (e.g., as a result of nonexistent or insufficient WLAN data encryption that exposes the WLAN data in transit to rogue elements), then those internal devices may be susceptible to the unauthorized disclosure of information. |
| T.NETWORK_ACCESS | Devices located outside the protected network may seek to exercise services located on the protected network that are intended to be only accessed from inside the protected network or only accessed by entities using an authenticated path into the protected network. |
| T.TSF_FAILURE | Security mechanisms of the TOE generally build up from a primitive set of mechanisms (e.g., memory management, privileged modes of process execution) to more complex sets of mechanisms. Failure of the primitive mechanisms could lead to a compromise in more complex mechanisms, resulting in a compromise of the TOE Security Functionality (TSF). |

| | |
|---|---|
| T.DATA_INTEGRITY | Devices on a protected network may be exposed to threats presented by devices located outside the protected network, which may attempt to modify the data without authorization. If known malicious external devices are able to communicate with devices on the protected network or if devices on the protected network can establish communications with those external devices then the data contained within the communications may be susceptible to a loss of integrity. |
| T.REPLAY_ATTACK | If an unauthorized individual successfully gains access to the system, the adversary may have the opportunity to conduct a “replay” attack. This method of attack allows the individual to capture packets traversing throughout the wireless network and send the packets at a later time, possibly unknown by the intended receiver. |

## 3.3. Organizational Security Policies

**Table 10. 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. |

# 4. 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.

## 4.1. 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 [MOD_WLAN_AS].

**Table 11. 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 to maintain confidentiality and allow for detection of modification of TSF data that is transmitted outside 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 shut down to ensure that data cannot be passed without adhering to the TOE's security policies. |
| 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. |

## 4.2. 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 [MOD_WLAN_AS].

**Table 12. 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.<br><br>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<br>■ 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<br>■ correctly implement ND functionality (e.g., ensure virtual networking is properly configured to support network traffic, management channels, and audit reporting).<br>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.<br>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 the network traffic of monitored networks. |

# 5. 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], [MOD_WLAN_AS], and NIAP Technical Decisions.

## 5.1. Conventions

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

**Table 13. 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 14. Security Functional Requirements**

| Class Name | Component Identification | Component Name | Drawn From |
|---|---|---|---|
| FAU: Security Audit | FAU_GEN.1 | Audit data generation | [NDcPP] |
| | FAU_GEN.1/WLAN | WLAN Audit data generation | [MOD_WLAN_AS] |

| Class Name | Component Identification | Component Name | Drawn From |
|---|---|---|---|
| | FAU_GEN.2 | User Identity Association | [NDcPP] |
| | FAU_GEN_EXT.1 | Security Audit Generation | [NDcPP] [MOD_WLAN_AS] |
| | FAU_STG.1 | Protected Audit Trail Storage | [NDcPP] |
| | FAU_STG_EXT.1 | Protected Audit Event Storage | [NDcPP] [MOD_WLAN_AS] |
| | FAU_STG_EXT.4 | Protected Local Audit Event Storage for Distributed TOEs | [NDcPP] [MOD_WLAN_AS] |
| | FAU_STG_EXT.5 | Protected Remote Audit Event Storage for Distributed TOEs | [NDcPP] |
| FCO: Communication | FCO_CPC_EXT.1 | Component Registration Channel Definition | [NDcPP] [MOD_WLAN_AS] |
| FCS: Cryptographic Support | FCS_CKM.1 | Cryptographic Key Generation | [NDcPP] |
| | FCS_CKM.2 | Cryptographic Key Establishment (Refined) | [NDcPP] |
| | FCS_CKM.1/WPA | Cryptographic Key Generation (Symmetric Keys for WPA2 Connections) | [MOD_WLAN_AS] |
| | FCS_CKM.2/PMK | Cryptographic Key Distribution (PMK) | [MOD_WLAN_AS] |
| | FCS_CKM.2/GTK | Cryptographic Key Distribution (GTK) | [MOD_WLAN_AS] |
| | FCS_CKM.2/DISTRIB | Cryptographic Key Distribution | [MOD_WLAN_AS] |
| | FCS_CKM.4 | Cryptographic Key Destruction | [NDcPP] |
| | FCS_COP.1/DataEncryption | Cryptographic Operation (AES Data Encryption/Decryption) | [NDcPP] [MOD_WLAN_AS] |

| Class Name | Component Identification | Component Name | Drawn From |
|---|---|---|---|
| | 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 | [MOD_WLAN_AS] |
| | 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_DTLSS_EXT.2 | DTLS Server Protocol with Mutual Authentication | [NDcPP] |
| | FCS_DTLSC_EXT.1 | DTLS Client Protocol without Mutual Authentication | [NDcPP] |
| | FCS_DTLSC_EXT.2 | DTLS Client Support for Mutual Authentication | [NDcPP] |
| | FCS_HTTPS_EXT.1 | HTTPS Protocol | [NDcPP] |
| | FCS_TLSS_EXT.1 | TLS Server Protocol | [NDcPP] |

| Class Name | Component Identification | Component Name | Drawn From |
|---|---|---|---|
| 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 | [MOD_WLAN_AS] |
| | FIA_UIA_EXT.1 | User Identification and Authentication | [NDcPP] |
| | FIA_UAU_EXT.2 | Password-based Authentication Mechanism | [NDcPP] |
| | FIA_UAU.6 | Re-authenticating | [MOD_WLAN_AS] |
| | FIA_UAU.7 | Protected Authentication Feedback | [NDcPP] |
| | FIA_8021X_EXT.1 | 802.1X Port Access Entity (Authenticator) Authentication | [MOD_WLAN_AS] |
| | 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] |

| Class Name | Component Identification | Component Name | Drawn From |
|---|---|---|---|
| | FMT_SMF.1 | Specification of Management Functions | [NDcPP] |
| | FMT_SMF.1/AccessSystem | Specification of Management Functions (WLAN Access Systems) | [MOD_WLAN_AS] |
| | FMT_SMR_EXT.1 | No Administration from Client | [MOD_WLAN_AS] |
| | FMT_SMR.2 | Restrictions on Security Roles | [NDcPP] |
| 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 | [MOD_WLAN_AS] |
| | 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] [MOD_WLAN_AS] |
| 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 | [MOD_WLAN_AS] |
| FTP: Trusted path/channels | FTP_ITC.1 | Inter-TSF trusted channel | [NDcPP] [MOD_WLAN_AS] |

| Class Name | Component Identification | Component Name | Drawn From |
|---|---|---|---|
| | FTP_ITC.1/Client | Inter-TSF Trusted Channel (WLAN Client Communications) | [MOD_WLAN_AS] |
| | FTP_TRP.1/Admin | Trusted Path | [NDcPP] |

## 5.2.Class: Security Audit (FAU)

### 5.2.1. FAU_GEN.1 – Audit Data Generation

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

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

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

*c) 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 15.*

**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 15*].

**Table 15. 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.<br><br>Disabling communications between a pair of components. | Identities of the endpoints pairs enabled or disabled. |
| FCS_CKM.1 | None. | None. |
| FCS_CKM.2 | 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. |
| FCS_IPSEC_EXT.1 | Failure to establish an IPsec SA. | Reason for failure. |
| FCS_TLSC_EXT.1/RADsec | Failure to establish a TLS session | Reason for failure. |
| FCS_TLSC_EXT.1/EST | Failure to establish a TLS session | Reason for failure. |
| FCS_TLSC_EXT.2 | None. | None. |
| FCS_DTLSS_EXT.1 | Failure to establish a DTLS session | Reason for failure |

| SFR | Auditable Event | Additional Audit Record Contents |
|---|---|---|
| | Detected replay attacks | Identity (e.g., source IP address) of the source of the replay attack. |
| FCS_DTLSS_EXT.2 | Failure to authenticate the client | Reason for failure |
| FCS_DTLSC_EXT.1 | Failure to establish a DTLS session | Reason for failure |
| FCS_DTLSC_EXT.2 | Detected replay attacks | Source of the replay attack |
| FCS_SSHS_EXT.1 | Failure to establish an SSH session | Reason for failure. |
| FCS_HTTPS_EXT.1 | Failure to establish a HTTPS session. | Reason for failure. |
| FCS_TLSS_EXT.1 | Failure to establish a TLS session | Reason for failure. |
| FIA_AFL.1 | Unsuccessful login attempts limit is met or exceeded. | 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.7 | None. | None. |
| FIA_X509_EXT.1/Rev | Unsuccessful attempt to validate a certificate<br><br>Any addition, replacement or removal of trust anchors in the TOE's trust store. | Reason for failure of certificate validation<br><br>Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store. |

| SFR | Auditable Event | Additional Audit Record Contents |
|---|---|---|
| FIA_X509_EXT.1/ITT | Unsuccessful attempt to validate a certificate<br><br>Any addition, replacement or removal of trust anchors in the TOE's trust store. | Reason for failure of certificate validation<br><br>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.2 | None. | None. |
| FPT_SKP_EXT.1 | None. | None. |
| FPT_APW_EXT.1 | None. | None. |
| FPT_ITT.1 | Initiation of the trusted channel.<br><br>Termination of the trusted channel.<br><br>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 | None. | None. |

| SFR | Auditable Event | Additional Audit Record Contents |
|---|---|---|
| FPT_TUD_EXT.1 | Initiation of update. result of the update attempt (success or failure) | None. |
| FTA_SSL_EXT.1 (if "terminate the session" is selected) | The termination of a local session by the session locking mechanism. | None. |
| 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. |
| FTP_ITC.1 | Initiation of the trusted channel.<br>Termination of the trusted channel.<br>Failure of the trusted channel functions. | Identification of the initiator and target of failed trusted channels establishment attempt. |
| FTP_TRP.1/Admin | Initiation of the trusted path.<br>Termination of the trusted path.<br>Failures of the trusted path functions. | None. |

### 5.2.2. FAU_GEN.1/WLAN – WLAN Audit Data Generation

**FAU_GEN.1.1/WLAN** 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. [Auditable events listed in the Auditable Events table (Table 16)

d. Failure of wireless sensor communication]

**Table 16. WLAN Auditable Events**

| SFR | Auditable Event | Additional Audit Record Contents |
|---|---|---|
| FCS_CKM.1/WPA | None. | None. |
| FCS_CKM.2/DISTRIB | None. | None. |
| FCS_CKM.2/GTK | None. | None. |
| FCS_CKM.2/PMK | None. | None. |
| FCS_RADSEC_EXT.1 | None. | None. |
| FCS_IPSEC_EXT.1 | Protocol failures.<br>Establishment or Termination of an IPsec SA. | Reason for failure. Non-TOE endpoint of connection.<br>Non-TOE endpoint of connection. |
| FIA_8021X_EXT.1 | Attempts to access the 802.1X controlled port prior to successful completion of the authentication exchange.<br>Failed authentication attempt. | Provided client identity (e.g. Media Access Control [Media Access Control (MAC)] address).<br>Provided client identity (e.g. MAC address). |
| FIA_UAU.6 | Attempts to re-authenticate. | Origin of the attempt (e.g., IP address). |
| FIA_PSK_EXT.1 | None. | None. |
| FMT_SMF.1/AccessSystem | None. | None. |
| FMT_SMR_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_TST_EXT.1 | Execution of TSF self-test.<br>Detected integrity violations. | None.<br>The TSF code file that caused the integrity violation. |
| FTA_TSE.1 | Denial of a session establishment due to the session establishment mechanism. | Reason for denial, origin of establishment attempt. |

| SFR | Auditable Event | Additional Audit Record Contents |
|---|---|---|
| FTP_ITC.1 | Failed attempts to establish a trusted channel (including IEEE 802.11).<br><br>Detection of modification of channel data. | Identification of the initiator and target of channel. |

### 5.2.3. 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.

### 5.2.4. 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.

### 5.2.5. 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.

### 5.2.6. 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.

### 5.2.7. 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 |

### 5.2.8. 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].

## 5.3.Class: Communication Partner Control (FCO)

### 5.3.1. 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.

***Application Note:*** *The registration channel requirement (FPT_ITT.1/Join) is satisfied by FPT_ITT.1.*

## 5.4.Class: Cryptographic Support (FCS)

### 5.4.1. FCS_CKM.1 – Cryptographic Key Generation (Refinement)

**FCS_CKM.1.1** 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;

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

### 5.4.2. FCS_CKM.2 – Cryptographic Key Establishment (Refinement)

**FCS_CKM.2.1** 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";

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

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

**FCS_CKM.1.1/WPA** 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 [*256 bits and [128 bits]*] **and using a Random Bit Generator as specified in FCS_RBG_EXT.1** that meet the following: [*IEEE 802.11-2020 and* [*IEEE 802.11ax-2021*]].

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

**FCS_CKM.2.1/GTK** The TSF shall distribute **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 802.11-2020 for the packet format and timing considerations*] **and does not expose the cryptographic keys**.

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

**FCS_CKM.2.1/PMK** The TSF shall **receive the 802.11 PMK** in accordance with a specified cryptographic key distribution method: [*from 802.1X Authorization Server*] that meets the following: [*IEEE 802.11-2020*] **and does not expose the cryptographic keys.**

### 5.4.6. FCS_CKM.2/DISTRIB – Cryptographic Key Distribution (802.11 Keys)

**FCS_CKM.2.1/DISTRIB** The TSF shall distribute **the IEEE 802.11 keys** in accordance with a specified key distribution method: [*trusted channel protocol specified in FPT_ITT.1(Base-PP)*] that meets the following: [*standards specified in the various iterations of FCS_COP.1*] **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.*

### 5.4.7. 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.*

### 5.4.8. 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 Advanced Encryption Standard (AES) used in **Cipher Block Chaining (CBC), CCM mode Protocol (CCMP)** and [*Galois-Counter Mode (GCM),* ***GCMP***] **modes** and cryptographic key sizes **256 bits and** [*128-bits*] that meet the following: AES as specified in ISO 18033-3, **CBC as specified in ISO 10116, CCMP as specified in NIST SP800-38C and IEEE 802.11-2020,** [*GCM as specified in ISO 19772*, ***GCMP as specified in NIST SP800-38D and IEEE 802.11ax-2021***].

### 5.4.9. 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, 3072 bits*],
- 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

].

### 5.4.10. 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.*

### 5.4.11. 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*] and cryptographic key sizes [*160, 256, 384*] **and message digest sizes** [**160, 256, 384**] **bits** that meet the following: *ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2"*.

### 5.4.12. 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), HMAC_DRBG (any)].

**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, [*1*] software-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.

### 5.4.13. 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 [*256 (for DH Group 19), 384 (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)] 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 [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].

### 5.4.14. 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 [5656, 6668, 8308 section 3.1, 8332].

**FCS_SSHS_EXT.1.2** The TSF shall ensure that the SSH protocol implementation supports the following user 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 [*65,824*] 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, aes128-gcm@openssh.com, aes256-gcm@openssh.com].

**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, implicit] 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] 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.

### 5.4.15. 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].

### 5.4.16. 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*

### 5.4.17. 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

]

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*

### 5.4.18. 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.

### 5.4.19. 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_128_GCM_SHA256 as defined in RFC 5289

]

and no other ciphersuites.

**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 [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 4346 (TLS1.1) or RFC 5246 (TLS1.2)].

### 5.4.20. FCS_DTLSS_EXT.2 – DTLS Server Support for Mutual Authentication

**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 [

- Not implement any administrator override mechanism

].

**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.

### 5.4.21. 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_128_GCM_SHA256 as defined in RFC 5289

and no other ciphersuites

].

**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.

### 5.4.22. FCS_DTLSC_EXT.2 – DTLS Client Support for Mutual Authentication

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

**FCS_DTLSC_EXT.2.2** The TSF shall [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

### 5.4.23. 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.

### 5.4.24. 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, 3072 bits*], *ECDHE curves* [*secp256r1, secp384r1*] *and no other curves*].

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

## 5.5.Class: Identification and Authentication (FIA)

### 5.5.1. 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 Administrator from successfully establishing a 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 a remote session using any authentication method that involves a password until an Administrator defined time period has elapsed].

### 5.5.2. 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 [*1*] and [*127*] characters.

### 5.5.3. 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 [lengths from 1 to 127 characters];
- 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.

### 5.5.4. 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.

### 5.5.5. FIA_UAU_EXT.2 – Password-based Authentication Mechanism

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

### 5.5.6. 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*]].

### 5.5.7. 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**.

### 5.5.8. 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.

### 5.5.9. 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.

### 5.5.10. 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.

### 5.5.11. 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].

### 5.5.12. 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.

## 5.6.Class: Security Management (FMT)

### 5.6.1. 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*.

### 5.6.2. FMT_MOF.1/Services – Management of Security Functions Behavior

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

### 5.6.3. 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*.

### 5.6.4. 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*.

### 5.6.5. 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*.

### 5.6.6. FMT_SMF.1 – Specification of Management Functions

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

- *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*

]

### 5.6.7. FMT_SMF.1/AccessSystem – Specification of Management Functions (WLAN Access Systems)

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

[

*- Configure the security policy for each wireless network, including:*

*- Security type*

*- Authentication protocol*

*- Client credentials to be used for authentication*

*- Service Set Identifier (SSID)*

*- If the SSID is broadcasted*

*- Frequency band set to [2.4 GHz, 5 GHz, 6 GHz ]*

*- Transmit power level*

]

### 5.6.8. FMT_SMR_EXT.1 – No Administration from Client

**FMT_SMR_EXT.1.1** The TSF shall ensure that the ability to administer remotely the TOE from a wireless client shall be disabled by default.

### 5.6.9. 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.

## 5.7.Class: Protection of the TSF (FPT)

### 5.7.1. 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.

### 5.7.2. 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 shall prevent the reading of plaintext administrative passwords.

### 5.7.3. 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*].

### 5.7.4. 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].

### 5.7.5. FPT_TST_EXT.1 – TSF Testing

**FPT_TST_EXT.1.1:** 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,* ***in no other circumstances***] to demonstrate the correct operation of the TSF: **integrity verification 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**, [***correct operation of cryptographic functions***].

### 5.7.6. 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 [no other TOE firmware/software version].

**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.

### 5.7.7. 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**].

## 5.8.Class: TOE Access (FTA)

### 5.8.1. 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.

### 5.8.2. 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*.

### 5.8.3. FTA_SSL.4 – User-initiated Termination

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

### 5.8.4. 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.

### 5.8.5. FTA_TSE.1 – TOE Session Establishment

**FTA_TSE.1.1** 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.*

## 5.9.Class: Trusted Path/Channels (FTP)

### 5.9.1. FTP_ITC.1 – Inter-TSF Trusted Channel

**FTP_ITC.1.1** The TSF shall **be capable of using IEEE 802.1X , [*Internet Protocol Security (IPsec), Remote Authentication Dial In User Service (RADIUS) over Transport Layer Security (TLS)*] and** [*TLS*] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: **802.1X authentication server**, audit server, [*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* ]

### 5.9.2. FTP_ITC.1/Client Inter-TSF Trusted Channel (WLAN Client Communications)

**FTP_ITC.1.1/Client** The TSF shall **be capable of using WPA3-Enterprise, WPA2-Enterprise and** [***none***] **as defined by IEEE 802.11-2020** to provide a **trusted** communication channel between itself and **WLAN clients** 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/Client** The TSF shall permit [*the authorized IT entities*] to initiate communication via the trusted channel.

**FTP_ITC.1.3/Client** The TSF shall initiate communication via the trusted channel for [*no services*].

### 5.9.3. 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*.

## 5.10. TOE SFR Dependencies Rationale

The Security Functional Requirements included in the ST represent all mandatory, optional, and selection-based SFRs specified in [NDcPP] and [MOD_WLAN_AS] 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.

## 5.11. Security Assurance Requirements Rationale

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

## 5.12. 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 19. Assurance Measures**

| Assurance Component | Rationale |
|---|---|
| ASE_INT.1<br>ASE_CCL.1<br>ASE_OBJ.1<br>ASE_ECD.1<br>ASE_REQ.1<br>ASE_SPD.1<br>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<br>AGD_PRE.1 | Cisco will provide the guidance documents with the ST. |
| ALC_CMC.1<br>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. |

# 6. TOE Summary Specification

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

**Note:** Extra instances of a WLC or AP TOE component are permitted in the evaluated configuration. Extra instances of a TOE component maintain SFRs in the exact same role and manner as the original instance of the TOE component in the evaluated configuration. There are no differences.

**Table 20. TSS Rationale**

| TOE SFR | Component Implemented | Rationale |
|---|---|---|
| FAU_GEN.1<br>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.<br><br>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.<br><br>A mapping is provided in table 24 to show which auditable events are covered by which components of the TOE.<br><br>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<br>FAU_STG.1</td><td>WLC, AP</td><td>The Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.12 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.
<table>
<tr><th>Transmitting Component</th><th>Storing Component</th></tr>
<tr><td>AP</td><td>WLC</td></tr>
</table>
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.<br><br>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.<br><br>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.</td></tr>
</table>

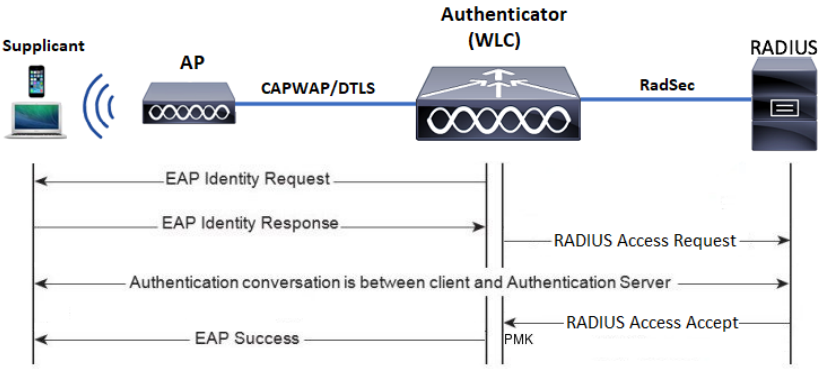
| TOE SFR | Component Implemented | Rationale |
|---|---|---|
| FAU_STG_EXT.4<br>FAU_STG_EXT.5 | WLC, AP | The AP maintains the audit data in a transmission buffer and continues to do so until the AP has transferred its contents to the WLC where it is stored locally. |
| FCO_CPC_EXT.1 | WLC, AP | At 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.<br><br>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.<br><br>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:<br><br>■ 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.<br><br>■ 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.<br><br>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.<br><br>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.<br><br>The Administrator may remove an AP from the authorization list, thereby disabling the AP from joining the WLC. |

<table>
<tr>
<td>FCS_CKM.1<br>FCS_CKM.2</td>
<td>WLC, AP</td>
<td>The following table describes the key generation algorithms the TOE implements to generate asymmetric keys used for device authentication:
<table>
<tr><th>Scheme</th><th>Standard</th><th>Key Size/ NIST Curve</th><th>SFR</th><th>Service</th></tr>
<tr><td rowspan="4">RSA</td><td rowspan="4">FIPS PUB 186-4</td><td rowspan="4">2048<br>3072</td><td>FCS_SSHS_EXT.1</td><td>SSH Remote Administration</td></tr>
<tr><td>FCS_TLSC_EXT.1 /RADsec<br><br>FCS_TLSC_EXT.2</td><td>RADsec</td></tr>
<tr><td>FCS_TLSS_EXT.1</td><td>HTTPS Remote Administration</td></tr>
<tr><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</td><td>FCS_TLSS_EXT.1</td><td>HTTPS Remote Administration</td></tr>
<tr><td rowspan="2">ECC</td><td rowspan="2">FIPS PUB 186-4</td><td rowspan="2">P-256</td><td>FCS_IPSEC_EXT.1</td><td>Transmit generated audit data to an external IT entity</td></tr>
<tr><td>FCS_TLSC_EXT.1/EST<br><br>FCS_TLSC_EXT.2</td><td>EST Client</td></tr>
<tr><td>ECC</td><td>FIPS PUB 186-4</td><td>P-384</td><td>FCS_DTLSS_EXT.1<br>FCS_DTLSS_EXT.2</td><td>DTLS Server</td></tr>
<tr><td>ECC</td><td>FIPS PUB 186-4</td><td>P-384</td><td>FCS_DTLSC_EXT.1<br>FCS_DTLSC_EXT.2</td><td>DTLS Client</td></tr>
</table>
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.</td>
</tr>
</table>

The following table shows the key generation algorithms the TOE implements to generate asymmetric keys used for **key establishment**:

| Scheme | Standard | Key Size/ NIST Curve | SFR | Service |
|---|---|---|---|---|
| RSA | FIPS PUB 186-4 | 2048 | FCS_TLSC_EXT.1 /RADsec<br><br>FCS_TLSC_EXT.2 | RADsec |
| RSA | FIPS PUB 186-4 | 2048<br>3072 | FCS_TLSS_EXT.1 | HTTPS Remote Administration |
| ECC | FIPS PUB 186-4 | P-256<br>P-384 | FCS_IPSEC_EXT.1 | Transmit generated audit data to an external IT entity |
| | | | FCS_SSHS_EXT.1 | SSH Remote Administration |
| ECC | FIPS PUB 186-4 | P-256<br>P-384<br>P-521 | FCS_TLSC_EXT.1/EST<br><br>FCS_TLSC_EXT.2 | EST Client |
| | | | FCS_DTLSC_EXT.1<br>FCS_DTLSC_EXT.2 | DTLS Client |
| ECC | FIPS PUB 186-4 | P-384 | FCS_DTLSS_EXT.1<br>FCS_DTLSS_EXT.2 | DTLS Server |
| ECC | FIPS PUB 186-4 | P-256<br>P-384 | FCS_TLSS_EXT.1 | HTTPS Remote Administration |

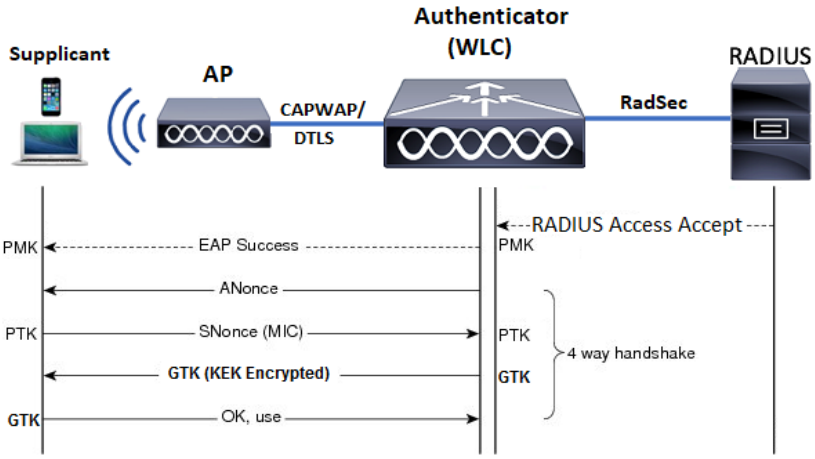
<table>
<tr><th>TOE SFR</th><th>Component Implemented</th><th>Rationale</th></tr>
<tr><td></td><td></td><td>The following table shows the methods the TOE implements for key establishment:
<table>
<tr><th>Scheme</th><th>Standard</th><th>SFR</th><th>Service</th></tr>
<tr><td rowspan="2">RSAES-PKCS1-v1_5</td><td rowspan="2">Section 7.2 of RFC 3447</td><td>FCS_TLSC_EXT.1 /RADsec<br><br>FCS_TLSC_EXT.2</td><td>RADsec</td></tr>
<tr><td>FCS_TLSS_EXT.1</td><td>HTTPS Remote Administration</td></tr>
<tr><td rowspan="8">EC-DH</td><td rowspan="8">NIST SP 800-56A Revision 2</td><td>FCS_TLSS_EXT.1</td><td>HTTPS Remote Administration</td></tr>
<tr><td>FCS_IPSEC_EXT.1</td><td>Transmit generated audit data to an external IT entity</td></tr>
<tr><td>FCS_SSHS_EXT.1</td><td>SSH Remote Administration</td></tr>
<tr><td>FCS_TLSC_EXT.1/EST<br><br>FCS_TLSC_EXT.2</td><td>EST Client</td></tr>
<tr><td>FCS_DTLSS_EXT.1<br>FCS_DTLSS_EXT.2</td><td>DTLS Server</td></tr>
<tr><td>FCS_DTLSC_EXT.1<br>FCS_DTLSC_EXT.2</td><td>DTLS Client</td></tr>
</table></td></tr>
</table>

| | | |
|---|---|---|
| FCS_CKM.1/WPA<br>FCS_CKM.2/PMK<br>FCS_CKM.2/GTK<br>FCS_CKM.2/DISTRIB<br>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].<br><br>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.<br><br>**Figure 2. EAP Message Exchange**<br>  <br><br>'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.<br><br>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).<br><br>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.<br><br>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 802.11-2020] and [IEEE 802.11ax-2021] 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 a 128-bit 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 3 below represents the four-way handshake exchanges.

**Figure 3. Four-Way Handshake**




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.<br><br>3. The Authenticator derives the GTK from its GMK.<br><br>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.<br><br>4. The Supplicant sends an EAPOL-Key frame to confirm that the temporal keys were installed and encrypted transmissions are ready to begin.<br><br>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.<br><br>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:<br><br>1. The Authenticator sends the updated GTK protected with the KEK to the Supplicant for installation.<br><br>2. The Supplicant sends an acknowledgement message indicating the TOE can begin using the new GTK.<br><br>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.<br><br>Certification testing performed by the Wi-Fi Alliance demonstrates the TOE implements the IEEE 802.11-2020 standard correctly. Refer to Table 23 for identification of the relevant Wi-Fi Alliance certificates.<br><br>During development of the TOE, there are various tests and documentation produced to ensure the TOE conforms to RFCs 2865 and 3579. Requirements contained within the RFCs were analyzed, developed, and rigorously tested to ensure the TOE conforms to RFCs 2865 and 3579 and the overall product performs as expected. |

| TOE SFR | Component Implemented | Rationale |
|---|---|---|
| FCS_CKM.4 | WLC, AP | The TOE destroys private keys, session keys, and Critical Security Parameters (CSP) used to generate keys as specified in table 21. |

<table>
<tr>
<td>FCS_COP.1/<br>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:<br>■ CBC as specified in ISO 10116;<br>■ GCM mode as specified in ISO 19772;<br>■ CCMP mode as specified in NIST SP800-38C and IEEE 802.11-2020;<br>■ GCMP mode as specified in NIST SP800-38D and IEEE 802.11ax-2021.<br>The TOE uses the AES encryption algorithm in the following protocols:<br>■ SSH – GCM and CBC mode with key sizes of 128 bits and 256 bits;<br>■ HTTPS (TLS Server) – GCM and CBC mode with a key size of 128 and 256 bits;<br>■ TLS Client (RADsec) – CBC mode with a key size of 128 bits;<br>■ TLS Client (EST) – GCM mode with a key size of 128 bits and 256 bits;<br>■ DTLS Client (CAPWAP) – GCM mode with a key size of 128 bits<br>■ DTLS Server (CAPWAP) – GCM mode with a key size of 128 bits;<br>■ IPsec - GCM mode with key sizes of 128 bits and 256 bits;<br>■ WPA3/2-Enterprise: CCMP and GCMP modes and key sizes of 128 and 256 bits as listed in the table below:
<table>
<tr><th>AP</th><th>Modes</th><th>Key Sizes</th></tr>
<tr><td>Catalyst 9166I<br>Catalyst 9166D1<br>Catalyst 9164I<br>Catalyst 9162I<br>Catalyst 9136I<br>Catalyst 9130AX</td><td>GCMP, CCMP</td><td>128, 256</td></tr>
</table>
</td>
</tr>
</table>

| TOE SFR | Component Implemented | Rationale |
|---|---|---|
| | | <table><tr><td>Catalyst 9124AX<br><br>Catalyst IW9167</td><td></td><td></td></tr></table><br>Refer to Table 22 for identification of the relevant CAVP certificates. |
| FCS_COP.1/SigGen | WLC, AP | 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 bits and 3072 bits, as specified in FIPS PUB 186-4, "Digital Signature Standard." Refer to Table 22 for identification of the relevant CAVP certificates. |
| 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 180-4 "Secure Hash Standard." Refer to Table 22 for identification of the relevant CAVP certificates.<br><br>Hash functions are used in the TOE as follows:<br><br>■ SSH – SHA-1, SHA-256, SHA-384, and SHA-512<br>■ HTTPS (TLS Server) – SHA-256 and SHA-384<br>■ TLS Client (RADsec) – SHA-1<br>■ TLS Client (EST) – SHA-256 and SHA-384<br>■ DTLS Client (CAPWAP) – SHA-256<br>■ DTLS Server (CAPWAP) – SHA-256<br>■ 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 operating on 1024-bit blocks of data, with key sizes and message digest sizes of 160-bits, 256 bits and 384 bits respectively as specified in ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2". |

| TOE SFR | Component Implemented | Rationale |
|---|---|---|
| FCS_RBG_EXT.1 | WLC, AP | The WLC TOE Component 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.<br><br>The AP TOE Component implements a NIST-approved HMAC DRBG, as specified in ISO/IEC 18031:2011. This DRBG is seeded with a software 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:<br>■ AES-GCM-128 and AES-GCM-256<br>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).<br>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.<br>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.<br>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.<br>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.<br><br>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 RSA X.509v3 certificates or pre-shared keys. IKE separates negotiation into two phases: IKE_SA and CHILD_SA. IKE_SA creates the first tunnel, which protects later ISAKMP negotiation messages. The key negotiated in IKE_SA enables IKE peers to communicate securely in CHILD_SA. During CHILD_SA 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:<br><br>■ The negotiation of mutually acceptable IPsec options between peers (including peer authentication parameters, either signature based or pre-shared key based),<br><br>■ The establishment of additional Security Associations to protect packets flows using Encapsulating Security Payload (ESP), and<br><br>■ The agreement of secure bulk data encryption AES keys for use with ESP.<br><br>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. The Administrator must ensure the IKEv2 IKE SA is always configured to be greater than or equal to the strength of the IKEv2 Child SA (ESP).<br><br>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 DH group 19 and DH group 20 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).<br><br>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.<br><br>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.<br><br>The TOE supports IKEv2 session establishment. The TOE supports configuration of session lifetimes for both IKE_SA SAs and CHILD_SA SAs. The time values for IKE_SA SAs can be limited up to 24 hours and for CHILD_SA SAs up to 8 hours. The CHILD_SA SA lifetimes can also be configured by an Administrator based on number of bytes. The TOE supports Diffie-Hellman Groups 19 and 20.<br><br>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)<br><br>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 length of at least 256 bits for DH Group 19 or 384 for DH Group 20.. 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.<br><br>The TOE supports authentication of IPsec peers using pre-shared keys, and ECDSA or RSA X.509 certificates. Pre-shared keys must be entered |

| TOE SFR | Component Implemented | Rationale |
|---|---|---|
| | | 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.<br><br>For peer authentication using RSA certificates, the TOE validates the presented identifier provided supporting the following fields and types: SAN: IP address, SAN: Fully Qualified Domain Name (FQDN). Simultaneous use of the same identifier type in both the CN and SAN fields is not supported.<br><br>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.<br><br>SAN example: alt-subject-name eq <peer.cisco.com><br><br>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.<br><br>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. |

| | | |
|---|---|---|
| FCS_SSHS_EXT.1 | WLC | The TSF implements SSHv2 conformant to RFCs 4251, 4252, 4253, 4254, 5656, 6668, 8308 section 3.1, and 8332 to provide a secure command line interface for remote administration. The TOE uses rsa-sha2-512 and rsa-sha2-256 for host key authentication and uses ssh-rsa for client or user password-based authentication.<br><br>SSHv2 connections will be dropped if the TOE receives a packet larger than 65,824 bytes. Large packets are detected by the SSHv2 implementation and dropped internal to the SSH process.<br><br>The TSF's SSH transport implementation supports the following encryption algorithms:<br><br>■ aes128-cbc<br>■ aes256-cbc<br>■ aes128-gcm@openssh.com<br>■ aes256-gcm@openssh.com<br><br>All connection attempts from remote SSH clients requesting any other encryption algorithm is denied.<br><br>The TSF's SSH transport implementation supports the following MAC algorithms when aes128-cbc or aes-256-cbc is used:<br><br>■ hmac-sha2-256<br><br>When aes128-gcm@openssh.com or aes256-gcm@openssh.com is used as the encryption algorithm the MAC algorithm is implicit.<br><br>All connection attempts from remote SSH clients requesting any other MAC algorithm is denied.<br><br>The TSF's SSH transport implementation supports the following public-key algorithms for Hostkey authentication:<br><br>■ rsa-sha2-256<br>■ rsa-sha2-512<br><br>The TSF's SSH transport implementation supports the following public-key algorithms for Client Authentication:<br><br>■ ssh-rsa |

| TOE SFR | Component Implemented | Rationale |
|---|---|---|
| | | The public-key algorithm is consistent with the RSA digital signature algorithm in FCS_COP.1/SigGen.<br><br>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.<br><br>The TSF's SSH key exchange implementation supports the following key exchange algorithm:<br><br>■ ecdh-sha2-nistp256<br><br>■ ecdh-sha2-nistp384<br><br>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<br>FCS_DTLSS_EXT.2 | WLC | The TSF implements DTLS 1.2 conformant to RFC 6347 supporting the following ciphersuites:<br>■ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289<br>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.<br>The TSF provides mutual authentication of DTLS clients using X.509v3 certificates.<br>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.<br>DTLS Server key establishment is implemented as follows:<br>By default, the secp384r1 NIST elliptic curve will be used. 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.<br>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.<br>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 |

| TOE SFR | Component Implemented | Rationale |
|---|---|---|
| | | 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.<br><br>The DN is compared to the expected identifier as follows:<br><br>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. |

| TOE SFR | Component Implemented | Rationale |
|---|---|---|
| FCS_DTLSC_EXT.1<br>FCS_DTLSC_EXT.2 | AP | The TSF implements DTLS 1.2 conformant to RFC 6347 supporting the following ciphersuites:<br>■ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289<br>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.<br>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.<br>The TSF provides client-side certificates to support DTLS mutual authentication.<br>During internal channel communication between the AP and WLC, if there is a Message Authentication Code (MAC) verification failure, the AP will silently discard the record and continue with the connection. The AP will increment its DTLS packet error counter.<br>The AP 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. |

| | | |
|---|---|---|
| FCS_HTTPS_EXT.1<br>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:<br>■ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289<br>■ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289<br>■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289<br>■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289<br>■ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289<br>■ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289<br>■ TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246<br>■ TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246<br>■ TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288<br>■ TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288<br>■ TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268<br>■ TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268<br>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.<br>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:<br>■ 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. |

| TOE SFR | Component Implemented | Rationale |
|---|---|---|
| | | ■ 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.<br><br>If a named curve is not configured, the secp256r1 NIST elliptic curve will be used by default.<br><br>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.<br><br>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<br>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:<br>■ TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268<br>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.<br>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:<br>■ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289<br>■ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289<br>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.<br>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 1 and maximum of 127 characters. A minimum password length of 8 is recommended. |
| 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.<br><br>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.<br><br>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 authentication, 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<br>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, remotely access the CLI over SSH, and HTTPS remote administrative interfaces.<br><br>Administrative access to the TOE is facilitated through a local password-based authentication mechanism 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 (local CLI, remote SSH CLI, or remote Web 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.<br><br>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 Local CLI and SSH 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.<br><br>Prior to authentication at each interactive administrative interfaces (Local CLI, SSH CLI, and Web 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.<br><br>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 CC 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. |

| TOE SFR | Component Implemented | Rationale |
|---|---|---|
| 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. The TOE supports pre-shared key lengths of 22 characters. In addition, lengths of 1 to 127 characters are also supported. A minimum pre-shared key length of 22 is recommended. Pre-shared keys can also be entered as HEX ("bit-based") values. |
| 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.<br><br>The TOE ensures the extendedKeyUsage field includes:<br><br>■ The Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) for server certificates used in TLS.<br><br>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. |

| TOE SFR | Component Implemented | Rationale |
|---|---|---|
| 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. 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. |
| FMT_MOF.1/ Services<br><br>FMT_MOF.1/ Functions<br><br>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.<br><br>Only the authorized Administrator on the WLC may:<br>■ Initiate manual updates of the TOE software;<br>■ Start and Stop services. The following services are in-scope:<br>o Web Server, SSH and IPsec<br>■ Modify the security function behavior including:<br>o Transmission of audit data to an external syslog server;<br><br>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.<br><br>The TOE provides the ability for the Authorized Administrator to manage cryptographic keys. The Authorized Administrator can generate key pairs to be used in the TLS, IPsec, and SSH protocols. The Authorized Administrator may also zeroize the private keys. Zeroization of these keys is provided in Table 21 below. |

| TOE SFR | Component Implemented | Rationale |
|---|---|---|
| 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.<br><br>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. |

| | | |
|---|---|---|
| FMT_SMF.1<br><br>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.<br><br>The TOE provides all capabilities necessary to securely manage the TOE and the services provided by the TOE. The management functionality of the TOE is provided through the TOE CLI. The Authorized Administrator can perform all management functions by accessing the TOE directly via local console cable or remote administration. The specific management capabilities available from the TOE include:<br><br>■ Local and remote administration of the TOE and the services provided by the TOE;<br><br>■ Configure an advisory notice and consent warning message to be displayed at login prior to gaining access to administrative functions;<br><br>■ 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;<br><br>■ Ability to configure thresholds for SSH rekeying;<br><br>■ Ability to configure lifetime for IPsec Sas<br><br>■ Ability to re-enable the Administrator account<br><br>■ Initiate updates of the TOE software;<br><br>■ Change the number of consecutive incorrect password attempts and the block out time duration;<br><br>■ Configure the cryptographic functionality and manage cryptographic keys;<br><br>■ Set the time and date;<br><br>■ Start and Stop services. The following services are in-scope:<br><br>o Web Server, SSH and IPsec<br><br>■ Ability to configure audit behavior;<br><br>■ Ability to configure the reference identifier for the peer; |

| TOE SFR | Component Implemented | Rationale |
|---|---|---|
| | | ■ Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors;<br>■ Ability to import X.509v3 certificates to the TOE's trust store;<br>■ Ability to manage the trusted public keys database<br>■ 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. |

| TOE SFR | Component Implemented | Rationale |
|---|---|---|
| FMT_SMF.1/AccessSystem | WLC | The TOE provides management functions for the WLAN Access System. The authorized Administrator can specify the following security policy parameters in the WebGUI under Configuration -> Tags & Profiles -> WLANs:<br>■ The General tab provides the ability to define the SSID and if the SSID is Broadcasted.<br>■ The General tab provides configuration options to set the frequency band (2.4 GHz, 5 GHz, 6 GHz)<br>■ The Security tab provides the following configuration options for WPA2/WPA3 encryption:<br>o AES(CCMP128)<br>o CCMP256<br>o GCMP128<br>o GCMP256<br>■ The Security Tab provides the following configuration options for Authentication:<br>o 802.1X<br>o 802.1X-SHA256<br>o SUITEB-1X<br>o SUITEB192-1X<br>If a wireless client attempts to connect to TOE with a non-supported security type, the client's authentication attempt will fail and the connection to the WLAN is rejected.<br>The authorized Administrator can adjust transmit power of APs by navigating in the WebGUI to Configuration -> Radio Configurations -> RRM -> 6 GHz /5 GHz / 2.4 GHz -> TPC. The Administrator can set the following:<br>■ Max Power Level Assignment<br>■ MIn Power Level Assignment |

| TOE SFR | Component Implemented | Rationale |
|---|---|---|
| FMT_SMR_EXT.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.<br><br>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.<br><br>When the configuration file is viewed by the Administrator, the TOE prevents displaying of pre-shared keys. |
| 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.<br><br>The CC Configuration Guide instructs the Administrator to use the `algorithm-type sha256` sub-command when passwords are created or updated. The sha256 sub-command is password type 8 which uses PBKDF2. |

| TOE SFR | Component Implemented | Rationale |
|---|---|---|
| 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.<br><br>The TOE relies upon date and time information for the following security functions:<br><br>■ To deny establishment of connections from wireless clients based on a configured time restriction (FTA_TSE.1);<br><br>■ To monitor local and remote interactive administrative sessions for inactivity (FTA_SSL_EXT.1, FTA_SSL.3);<br><br>■ Validating X.509 certificates to determine if a certificate has expired (FIA_X509_EXT.1/Rev, FIA_X509_EXT.1/ITT);<br><br>■ To determine when SSH session keys have expired and to initiate a rekey (FCS_SSHS_EXT.1);<br><br>■ To determine when IKEv2 SA lifetimes have expired and to initiate a rekey (FCS_IPSEC_EXT.1);<br><br>■ To determine when IPsec Child SA lifetimes have expired and to initiate a rekey (FCS_IPSEC_EXT.1);<br><br>■ 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 the cryptographic modules. 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 and the TOE component will automatically reboot. If the Administrator observes a cryptographic self-test failure, they should contact Cisco Technical Support. These tests are sufficient to verify correct operation of cryptographic modules. The suite of self-tests tests include:<br>■ 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.<br>■ 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.<br>■ SHA-1/256/384/512 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.<br>■ HMAC (HMAC-SHA-1) 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.<br>■ Software Integrity Test - The Software Integrity Test is run automatically whenever the module is loaded and confirms the module has maintained its integrity.<br>■ ECDSA Signature Test – This test takes a known plaintext value and Private/Public key pair and used the public key to encrypt the data. |

| TOE SFR | Component Implemented | Rationale |
|---|---|---|
| | | 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.<br><br>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:<br><br>`test crypto self-test`<br><br>All TOE components (WLC and AP) will automatically verify the integrity of the stored image when loaded for execution.<br><br>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 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.<br><br>All hardware WLC appliances will display at bootup a message that the image was successfully validated:<br><br>`"RSA Signed RELEASE Image Signature Verification Successful."`<br><br>After boot, the authorized administrator can also manually verify the digital signature by executing on the WLC:<br><br>`verify bootflash:<image or package name>`<br><br>The AP will perform a digital signature verification check on its stored image. When successfully validated the AP will display at bootup:<br><br>`"Image signing verification success, continue to run…"`<br><br>If integrity of the stored image is not successfully verified the image will not boot or execute. |

| | | |
|---|---|---|
| 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:<br><br>`show version \| include Cisco IOS XE Software`<br><br>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:<br><br>`show ap image`<br><br>The Administrator can download updates (new software images) appropriate for controller hardware. Software images are made available via Cisco.com.<br><br>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:<br><br>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.<br><br>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 authentic. If they do not match the image will not install.<br><br>AP software images are embedded in the WLC image and are not downloaded separately from Cisco.com. The AP will perform a digital signature verification check on the image it receives from the WLC.<br><br>The WLC image will become active after the Administrator reboots it during the trusted update process as instructed in the CC Configuration Guide. When the WLC reboots the Access Points will automatically reboot. After the AP boots it will download it's new image from the WLC. |

| TOE SFR | Component Implemented | Rationale |
|---|---|---|
| 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. |
| FTA_SSL_EXT.1<br>FTA_SSL.3 | WLC | 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.<br><br>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. |
| FTA_SSL.4 | WLC | 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 both local and remote administrative sessions by entering the `logout` or `exit` command. |
| FTA_TAB.1 | WLC | 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. |
| FTA_TSE.1 | WLC | The Administrator can deny establishment of wireless client sessions based on time and day attributes. 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.<br><br>To deny access to a SSID, the Administrator can create a calendar profile that covers all 24 hours recurring daily. The SSID is the name for a wireless network (WLAN) defined by the Security Administrator. |

<table>
<tr><th>TOE SFR</th><th>Component Implemented</th><th>Rationale</th></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 802.11-2020 (WPA2/WPA3)</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>

## 6.1. Key Zeroization

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

**Table 21. 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.<br>`# 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. |

| Key | Description | Storage Location | Zeroization Method |
|---|---|---|---|
| SSH Private Key | Used in establishing a secure SSH session | NVRAM | Overwritten with 0x00 by using the following command:<br>#crypto key zeroize <label> |
| 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:<br>#crypto key zeroize <label> |
| RADIUS Preshared key | This shared secret was manually entered for RADIUS authentication to the RADIUS Server. | SDRAM | Overwritten automatically with 0x00 when RADIUS is no longer in use. |
| | | NVRAM | Overwritten with a new value of the key.<br>(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. |

| Key | Description | Storage Location | Zeroization Method |
|---|---|---|---|
| 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:`<br>`#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. |
| 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:`<br>`#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.<br>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.<br>Zeroized on Power Cycle |

| Key | Description | Storage Location | Zeroization Method |
|---|---|---|---|
| 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.<br><br>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.<br><br>Zeroized on Power Cycle |

## 6.2. CAVP Certificates

The table below lists the CAVP certificates for the TOE.

**Table 22. CAVP Certificates**

| SFR | Algorithm | Selection | Implementation | TOE Component(s) | Certificate Number(s) |
|---|---|---|---|---|---|
| FCS_CKM.1 – Cryptographic Key Generation | RSA | 2048<br>3072 | CiscoSSL FOM 7.3 | Catalyst 9800-80<br>Catalyst 9800-40<br>Catalyst 9800-L<br>Catalyst 9800-CL | A2111<br>A4595 |
| | ECDSA | P-256<br>P-384<br>P-521 | CiscoSSL FOM 7.3 | Catalyst 9166I<br>Catalyst 9166D1<br>Catalyst 9164I<br>Catalyst 9162I<br>Catalyst 9136I<br>Catalyst 9130AX<br>Catalyst 9124AX<br>Catalyst IW9167<br>Catalyst 9800-80<br>Catalyst 9800-40<br>Catalyst 9800-L<br>Catalyst 9800-CL | A2111<br>A4595 |
| FCS_CKM.2 – Cryptographic Key Establishment | RSA | RSAES-PKCS1-v1_5 | CiscoSSL FOM 7.3 | Catalyst 9800-80<br>Catalyst 9800-40<br>Catalyst 9800-L<br>Catalyst 9800-CL | CCTL Tested |
| | KAS-ECC | P-256<br>P-384<br>P-521 | CiscoSSL FOM 7.3 | Catalyst 9166I<br>Catalyst 9166D1<br>Catalyst 9164I<br>Catalyst 9162I<br>Catalyst 9136I<br>Catalyst 9130AX<br>Catalyst 9124AX<br>Catalyst IW9167<br>Catalyst 9800-80<br>Catalyst 9800-40<br>Catalyst 9800-L<br>Catalyst 9800-CL | A2111<br>A4595 |
| | | P-256<br>P-384 | IC2M Rel5a | Catalyst 9800-80<br>Catalyst 9800-40<br>Catalyst 9800-L<br>Catalyst 9800-CL | A1462 |
| FCS_CKM.1/WPA – Cryptographic Key Generation (Symmetric Keys for WPA2 Connections) | PRF-384 – IEEE 802.11-2020<br>PRF-704 – IEEE 802.11ax-2021 | HMAC-SHA1<br>HMAC-SHA384 | CiscoSSL FOM 7.3 | Catalyst 9800-80<br>Catalyst 9800-40<br>Catalyst 9800-L<br>Catalyst 9800-CL | A2111<br>A4595 |

| | | | | | |
|---|---|---|---|---|---|
| FCS_CKM.2/GTK – Cryptographic Key Distribution (GTK) | AES | AES-KW-128 | CiscoSSL FOM 7.3 | Catalyst 9800-80<br>Catalyst 9800-40<br>Catalyst 9800-L<br>Catalyst 9800-CL | A2111<br>A4595 |
| | HMAC | HMAC-SHA1 | CiscoSSL FOM 7.3 | Catalyst 9800-80<br>Catalyst 9800-40<br>Catalyst 9800-L<br>Catalyst 9800-CL | A2111<br>A4595 |
| FCS_COP.1/DataEncryption – AES Data Encryption/Decryption | AES | AES-GCM-128 | CiscoSSL FOM 7.3 | Catalyst 9166I<br>Catalyst 9166D1<br>Catalyst 9164I<br>Catalyst 9162I<br>Catalyst 9136I<br>Catalyst 9130AX<br>Catalyst 9124AX<br>Catalyst IW9167 | A2111 |
| | | AES-CBC-128<br>AES-CBC-256<br>AES-GCM-128<br>AES-GCM-256 | CiscoSSL FOM 7.3 | Catalyst 9800-80<br>Catalyst 9800-40<br>Catalyst 9800-L<br>Catalyst 9800-CL | A2111<br>A4595 |
| | | AES-CBC-128<br>AES-CBC-256<br>AES-GCM-128<br>AES-GCM-256 | IC2M Rel5a | Catalyst 9800-80<br>Catalyst 9800-40<br>Catalyst 9800-L<br>Catalyst 9800-CL | A1462 |
| | | AES-CCMP-128<br>AES-CCMP-256<br><br>AES-GCMP-128<br>AES-GCMP-256 | Qualcomm Radio Chipset | Catalyst 9166I<br>Catalyst 9166D1<br>Catalyst 9164I<br>Catalyst 9162I<br>Catalyst 9136I<br>Catalyst 9130AX<br>Catalyst 9124AX<br>Catalyst IW9167 | AES 5663 |
| FCS_COP.1/SigGen – Cryptographic Operation (Signature Generation and Verification) | RSA | 2048<br>3072 | CiscoSSL FOM 7.3<br>IC2M Rel5a | Catalyst 9800-80<br>Catalyst 9800-40<br>Catalyst 9800-L<br>Catalyst 9800-CL | A2111<br>A4595<br>A1462 |
| | ECDSA | P-256<br>P-384 | CiscoSSL FOM 7.3 | Catalyst 9166I<br>Catalyst 9166D1<br>Catalyst 9164I<br>Catalyst 9162I<br>Catalyst 9136I<br>Catalyst 9130AX<br>Catalyst 9124AX<br>Catalyst IW9167 | A2111 |

| | | | | | |
|---|---|---|---|---|---|
| | | P-256 | CiscoSSL FOM 7.3 | Catalyst 9800-80<br>Catalyst 9800-40<br>Catalyst 9800-L<br>Catalyst 9800-CL | A2111<br>A4595 |
| | | | IC2M Rel5a | Catalyst 9800-80<br>Catalyst 9800-40<br>Catalyst 9800-L<br>Catalyst 9800-CL | A1462 |
| FCS_COP.1/Hash – Cryptographic Operation (Hash Algorithm) | SHS | SHA-256 | CiscoSSL FOM 7.3 | Catalyst 9166I<br>Catalyst 9166D1<br>Catalyst 9164I<br>Catalyst 9162I<br>Catalyst 9136I<br>Catalyst 9130AX<br>Catalyst 9124AX<br>Catalyst IW9167 | A2111 |
| | | SHA-1<br>SHA-256<br>SHA-384<br>SHA-512 | CiscoSSL FOM 7.3 IC2M Rel5a | Catalyst 9800-80<br>Catalyst 9800-40<br>Catalyst 9800-L<br>Catalyst 9800-CL | A2111<br>A4595<br>A1462 |
| FCS_COP.1/KeyedHash – Cryptographic Operation (Keyed Hash Algorithm) | HMAC | HMAC-SHA-256 | CiscoSSL FOM 7.3 | Catalyst 9166I<br>Catalyst 9166D1<br>Catalyst 9164I<br>Catalyst 9162I<br>Catalyst 9136I<br>Catalyst 9130AX<br>Catalyst 9124AX<br>Catalyst IW9167 | A2111 |
| | | HMAC-SHA-1<br>HMAC-SHA-256<br>HMAC-SHA-384 | CiscoSSL FOM 7.3 IC2M Rel5a | Catalyst 9800-80<br>Catalyst 9800-40<br>Catalyst 9800-L<br>Catalyst 9800-CL | A2111<br>A4595<br>A1462 |
| FCS_RBG_EXT.1– Random Bit Generation | DRBG | HMAC_DRBG | CiscoSSL FOM 7.3 | Catalyst 9166I<br>Catalyst 9166D1<br>Catalyst 9164I<br>Catalyst 9162I<br>Catalyst 9136I<br>Catalyst 9130AX<br>Catalyst 9124AX<br>Catalyst IW9167 | A2111 |
| | | CTR_DRBG (AES) | CiscoSSL FOM 7.3 IC2M Rel5a | Catalyst 9800-80<br>Catalyst 9800-40<br>Catalyst 9800-L<br>Catalyst 9800-CL | A2111<br>A4595<br>A1462 |

## 6.3. Wi-Fi Alliance Certificates

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

**Table 23. Wi-Fi Alliance Certificates**

| Product | Certification |
|---|---|
| Cisco Catalyst 9800-80 Wireless Controller and Cisco CW9166/CW9166D1 AP | WFA125640 |
| Cisco Catalyst 9800-80 Wireless Controller and Cisco CW9164 AP | WFA120175 |
| Cisco Catalyst 9800-80 Wireless Controller and Cisco CW9162 AP | WFA121201 |
| Cisco Catalyst 9800-80 Wireless Controller and Cisco CW9136 AP | WFA116420 |
| Cisco Catalyst 9800-80 Wireless Controller and Cisco C9130AX AP | WFA98109 |
| Cisco Catalyst 9800-80 Wireless Controller and Cisco C9124AX AP | WFA111158 |
| Cisco Catalyst 9800-80 Wireless Controller and Cisco Catalyst IW9167 | WFA126937 |
| Cisco Catalyst 9800-40 Wireless Controller and Cisco CW9166/CW9166D1 AP | WFA125639 |
| Cisco Catalyst 9800-40 Wireless Controller and Cisco CW9164 AP | WFA120174 |
| Cisco Catalyst 9800-40 Wireless Controller and Cisco CW9162 AP | WFA121198 |
| Cisco Catalyst 9800-40 Wireless Controller and Cisco CW9136 AP | WFA116418 |
| Cisco Catalyst 9800-40 Wireless Controller and Cisco C9130AX AP | WFA98108 |
| Cisco Catalyst 9800-40 Wireless Controller and Cisco C9124AX AP | WFA111157 |
| Cisco Catalyst 9800-40 Wireless Controller and Cisco Catalyst IW9167 | WFA126936 |
| Cisco Catalyst 9800-L Wireless Controller and Cisco CW9166/CW9166D1 AP | WFA125565 |
| Cisco Catalyst 9800-L Wireless Controller and Cisco CW9164 AP | WFA119718 |
| Cisco Catalyst 9800-L Wireless Controller and Cisco CW9162 AP | WFA120300 |
| Cisco Catalyst 9800-L Wireless Controller and Cisco CW9136 AP | WFA122216 |
| Cisco Catalyst 9800-L Wireless Controller and Cisco C9130AX AP | WFA97958 |
| Cisco Catalyst 9800-L Wireless Controller and Cisco C9124AX AP | WFA110437 |
| Cisco Catalyst 9800-L Wireless Controller and Cisco Catalyst IW9167 | WFA126155 |

| Product | Certification |
|---|---|
| Cisco Catalyst 9800-CL Wireless Controller and Cisco CW9166/CW9166D1 AP | WFA125641 |
| Cisco Catalyst 9800-CL Wireless Controller and Cisco CW9164 AP | WFA120176 |
| Cisco Catalyst 9800-CL Wireless Controller and Cisco CW9162 AP | WFA121202 |
| Cisco Catalyst 9800-CL Wireless Controller and Cisco CW9136 AP | WFA116422 |
| Cisco Catalyst 9800 Cloud Wireless Controller and Cisco C9130AX AP | WFA98110 |
| Cisco Catalyst 9800-CL Wireless Controller and Cisco C9124AX AP | WFA111159 |
| Cisco Catalyst 9800-CL Wireless Controller and Cisco Catalyst IW9167 | WFA126938 |

## 6.4. 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 24. 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<br>■ Adding a TOE Access Banner<br>■ 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.<br>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<br>Detected replay attacks; Identity (e.g., source IP address) of the source of the replay attack. |
| FCS_DTLSS_EXT.2 | WLC | Failure to authenticate the client<br>Reason for failure |
| FCS_DTLSC_EXT.1 | AP | Failure to establish a DTLS session; Reason for failure |
| FCS_DTLSC_EXT.2 | AP | Detected replay attacks<br>Source of the replay attack |
| FCS_SSHS_EXT.1 | WLC | Failure to establish an SSH session; Reason for failure |
| FCS_HTTPS_EXT.1<br>FCS_TLSS_EXT.1 | WLC | Failure to establish a HTTPS Session; Reason for failure<br>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<br>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/<br>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, AP | Initiation of the trusted channel.<br>Termination of the trusted channel.<br>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.<br>Termination of the trusted channel.<br>Failure of the trusted channel functions (including IEEE 802.11). |
| FTP_TRP.1/Admin | WLC | Initiation of the trusted path.<br>Termination of the trusted path.<br>Failure of the trusted path functions. |

# 7. References

The documentation listed below was used to prepare this ST.

**Table 25. 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 |
| [MOD_WLAN_AS] | PP-Module for Wireless Local Area Network (WLAN) Access System, Version 1.0, 2022-04-19 |
| [IEEE 802.11-2020] | 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 802.11ax-2021] | Amendment 1: Enhancements for High - Efficiency WLAN |
| [IEEE 802.1X-2020] | 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 |

| Identifier | Description |
|---|---|
| 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 |

## 7.1.Acronyms and Terms

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

**Table 26. 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 |

## 7.2.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.

## 7.3.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.