



# Cisco WLAN 8.0

## Common Criteria Security Target

---

Version 1.0

September, 2016



Americas Headquarters:

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

© 2016 Cisco Systems, Inc. All rights reserved.

## Table of Contents

1	SECURITY TARGET INTRODUCTION .....	8
1.1	ST and TOE Reference .....	8
1.2	TOE Overview .....	8
1.2.1	TOE Product Type .....	9
1.2.2	Supported non-TOE Hardware/ Software/ Firmware .....	9
1.3	TOE DESCRIPTION .....	9
1.4	TOE Evaluated Configuration.....	11
1.5	Physical Scope of the TOE.....	12
1.6	Logical Scope of the TOE.....	17
1.6.1	Security Audit .....	18
1.6.2	Cryptographic Support.....	18
1.6.3	User Data Protection .....	20
1.6.4	Identification and authentication.....	20
1.6.5	Security Management .....	20
1.6.6	Protection of the TSF, and Resource Allocation .....	21
1.6.7	TOE Access .....	21
1.6.8	Trusted path/Channels .....	22
1.7	Excluded Functionality .....	22
2	Conformance Claims.....	23
2.1	Common Criteria Conformance Claim .....	23
2.2	Protection Profile Conformance.....	23
2.3	Protection Profile Conformance Claim Rationale.....	23
2.3.1	TOE Appropriateness.....	23
2.3.2	TOE Security Problem Definition Consistency.....	23
2.3.3	Statement of Security Requirements Consistency .....	24
3	SECURITY PROBLEM DEFINITION.....	25
3.1	Assumptions.....	25
3.2	Threats .....	25
3.3	Organizational Security Policies .....	26
4	SECURITY OBJECTIVES.....	27

4.1	Security Objectives for the TOE .....	27
4.2	Security Objectives for the Environment .....	28
5	SECURITY REQUIREMENTS .....	29
5.1	Conventions.....	29
5.2	TOE Security Functional Requirements .....	29
5.3	SFRs Drawn from the WLANPP .....	31
5.3.2	Cryptographic Support (FCS).....	34
5.3.3	User data protection (FDP).....	37
5.3.1	Identification and authentication (FIA) .....	37
5.3.1	Security management (FMT).....	39
5.3.2	Protection of the TSF (FPT) .....	41
5.3.3	Resource Allocation (FRU) .....	42
5.3.4	TOE Access (FTA).....	42
5.3.1	Trusted Path/Channels (FTP).....	42
5.4	TOE SFR Dependencies Rationale for SFRs Found in the WLANPP .....	43
5.5	Security Assurance Requirements.....	43
5.5.1	SAR Requirements.....	43
5.5.2	Security Assurance Requirements Rationale .....	43
5.6	Assurance Measures.....	44
6	TOE Summary Specification .....	45
6.1	TOE Security Functional Requirement Measures.....	45
7	Annex A: Key Zeroization .....	55
7.1	Key Zeroization.....	55
8	Annex B: References.....	58

## List of Tables

TABLE 1 ACRONYMS.....	5
TABLE 2 TERMS & DEFINITIONS .....	6
TABLE 3 ST AND TOE IDENTIFICATION.....	8
TABLE 4 IT ENVIRONMENT COMPONENTS.....	9
TABLE 5 HARDWARE MODELS AND SPECIFICATIONS .....	12
TABLE 6 FIPS REFERENCES – CONTROLLERS AND APs .....	18
TABLE 7 TOE PROVIDED CRYPTOGRAPHY .....	19
TABLE 8 EXCLUDED FUNCTIONALITY .....	22
TABLE 9 PROTECTION PROFILES.....	23
TABLE 10 TOE ASSUMPTIONS .....	25
TABLE 11 THREATS.....	25
TABLE 12 ORGANIZATIONAL SECURITY POLICIES.....	26
TABLE 13 SECURITY OBJECTIVES FOR THE TOE .....	27
TABLE 14 SECURITY OBJECTIVES FOR THE ENVIRONMENT.....	28
TABLE 15 SECURITY FUNCTIONAL REQUIREMENTS.....	29
TABLE 16: AUDITABLE EVENTS .....	31
TABLE 17: ASSURANCE MEASURES.....	43
TABLE 18 ASSURANCE MEASURES.....	44
TABLE 19 HOW TOE SFRS MEASURES .....	45
TABLE 20: TOE KEY ZEROIZATION .....	55
TABLE 21: REFERENCES .....	58

## List of Figures

FIGURE 1: TOE DEPLOYMENT DIAGRAM.....	11
---------------------------------------	----

## List of Acronyms

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

**Table 1 Acronyms**

<b>Acronyms / Abbreviations</b>	<b>Definition</b>
AAA	Administration, Authorization, and Accounting
ACL	Access Control Lists
AES	Advanced Encryption Standard
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
CSU	Channel Service Unit
DHCP	Dynamic Host Configuration Protocol
DSU	Data Service Unit
DTLS	Datagram Transport Layer Security (see RFC 4347)
EAL	Evaluation Assurance Level
ESP	Encapsulating Security Payload
GE	Gigabit Ethernet port
GTK	Group Temporal Key
HTTP	Hyper-Text Transport Protocol
HTTPS	Hyper-Text Transport Protocol Secure
ICMP	Internet Control Message Protocol
ISR	Integrated Service Router
IT	Information Technology
NAS	Network Access Server
OS	Operating System
PBKDF2	Password-Based Key Derivation Function version 2
PoE	Power over Ethernet
PP	Protection Profile
SA	Security Association
SFP	Small-form-factor pluggable port
SHA	Secure Hash Algorithm (see SHS)
SHS	Secure Hash Standard
SIP	Session Initiation Protocol
SSHv2	Secure Shell (version 2)
ST	Security Target
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
WIC	WAN Interface Card
WLAN	Wireless Local Area Network
WLANPP	WLAN Protection Profile

Table 2 Terms &amp; Definitions

Terms	Definitions
Access Point	Provides the network interface that enables wireless client hosts access to a wired network. Once authenticated as trusted nodes on the wired infrastructure, the APs provide the encryption service on the wireless network between the wireless client and the RF interface of the AP.
Authentication Server	An authentication server on the wired network which receives authentication credentials from wireless clients for authenticating.
EAP	Stands for the extensible authentication protocol (EAP). EAP is a protocol that supports the communication of other authentication protocols. EAP uses its own start and end messages which allows it to then support any number of third-party messages between supplicants and an authentication server.
EAP-TLS	EAP-TLS (RFC 2716) stands for Extensible Authentication Protocol-Translation Layer Security. It uses the TLS protocol (RFC 2246) authentication hand shaking implementation for 802.1x authentication. EAP-TLS uses PKI to authenticate both the authentication server and the wireless client.
IEEE 802.1X	IEEE standard for port-based network access control that defines an authentication mechanism to devices (wireless clients) to attach to a wired network. The main components needed to support IEEE 802.1X is the supplicant (wireless client), authenticator (the TOE), and authentication server.
Management Frame Protection	A wireless technology enabling one access point to validate a neighboring Access Point's management frames.
WPA2	Wi-Fi Protected Access

## 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), the WLAN (WLAN). This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements, and the IT security functions provided by the TOE which meet the set of requirements. Administrators of the TOE will be referred to as administrators, Authorized Administrators, TOE administrators, semi-privileged, privileged administrators, and security administrators in this document.

# 1 SECURITY TARGET INTRODUCTION

The Security Target contains the following sections:

- ◆ Security Target Introduction [Section 1]
- ◆ Conformance Claims [Section 2]
- ◆ Security Problem Definition [Section 3]
- ◆ Security Objectives [Section 4]
- ◆ IT Security Requirements [Section 5]
- ◆ TOE Summary Specification [Section 6]

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 3 ST and TOE Identification**

Name	Description
<b>ST Title</b>	WLAN
<b>ST Version</b>	1.0
<b>Publication Date</b>	September, 2016
<b>Vendor and ST Author</b>	Cisco Systems, Inc.
<b>TOE Reference</b>	WLAN
<b>TOE Hardware Models</b>	Cisco 2504, 5508, 7510, 8510, and WiSM2 Controllers; Cisco 1142, 1262, 1530, 1552, 1570 series, 1600 series, 1700 series, 2600 series, 2700 series, 3502, 3600 series with 3000M add-on module, and 3700 series APs, and ISR 891 integrated AP.
<b>TOE Software Version</b>	Cisco Wireless LAN Controller: <b>8.0.132.0</b>
<b>Keywords</b>	WLAN, Wireless, Controller, Access Point, Data Protection, Authentication

## 1.2 TOE Overview

The Cisco WLAN TOE combines a purpose-built Wireless LAN Controller with wireless access points to create a WLAN Access System. The Cisco WLAN TOE provides secure 802.11



wireless communications between wireless clients and an organization's wired network. The TOE includes the WLAN Controller and wireless access point hardware models as defined in Table 3 in section 1.1 and WLAN software.

### 1.2.1 TOE Product Type

The Target of Evaluation (TOE) is a Wireless LAN (WLAN) Access System comprised of multiple products operating together to provide secure wireless access to wired and wireless networks end-to-end wireless encryption, and centralized administration of all WLAN controllers and APs in the system.

### 1.2.2 Supported non-TOE Hardware/ Software/ Firmware

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

**Table 4 IT Environment Components**

Component	Required	Usage/Purpose Description for TOE performance
Management Workstation	Yes	This includes any IT Environment Management workstation with a SSH client and TLS-enabled browser installed that is used by the TOE administrator for remote administration of the TOE. The SSH client must support SSHv2, and the browser must support TLS.
AAA Server	Yes	This includes any IT environment RADIUS server that provides authentication services for wireless clients and optionally for TOE administrators.
Syslog Server	Yes	This includes any syslog server to which the TOE would transmit syslog messages over TLS.
Certificate Authority	Yes	This includes any IT Environment Certification Authority on the TOE network. This can be used to provide the TOE with a valid certificate during certificate enrollment.
NTP Server	No	The TOE supports communications with an NTP server in order to synchronize the date and time on the TOE with the NTP server's date and time.

## 1.3 TOE DESCRIPTION

The TOE is comprised of two main components inclusive of software and hardware on. A Cisco WLAN Access System deployment includes one or more Wireless Controllers each of which controls multiple APs and one or more Access Points (APs) to provide connectivity to wireless clients.

The hardware models within the TOE are: Cisco 2504, 5508, 7510, 8510, and WiSM2 Controllers; Cisco 1142, 1262, 1530, 1552, 1570 series, 1600 series, 1700 series, 2600 series, 2700 series, 3502, 3600 series, 3700 series, and ISR 891 integrated APs. The software is Cisco WLAN 8.0.132.0 running on the controllers and includes Cisco IOS running on the APs.

The WLAN controllers that comprise the TOE have common security-relevant hardware characteristics, as do the access points. These hardware differences affect only non-TSF relevant

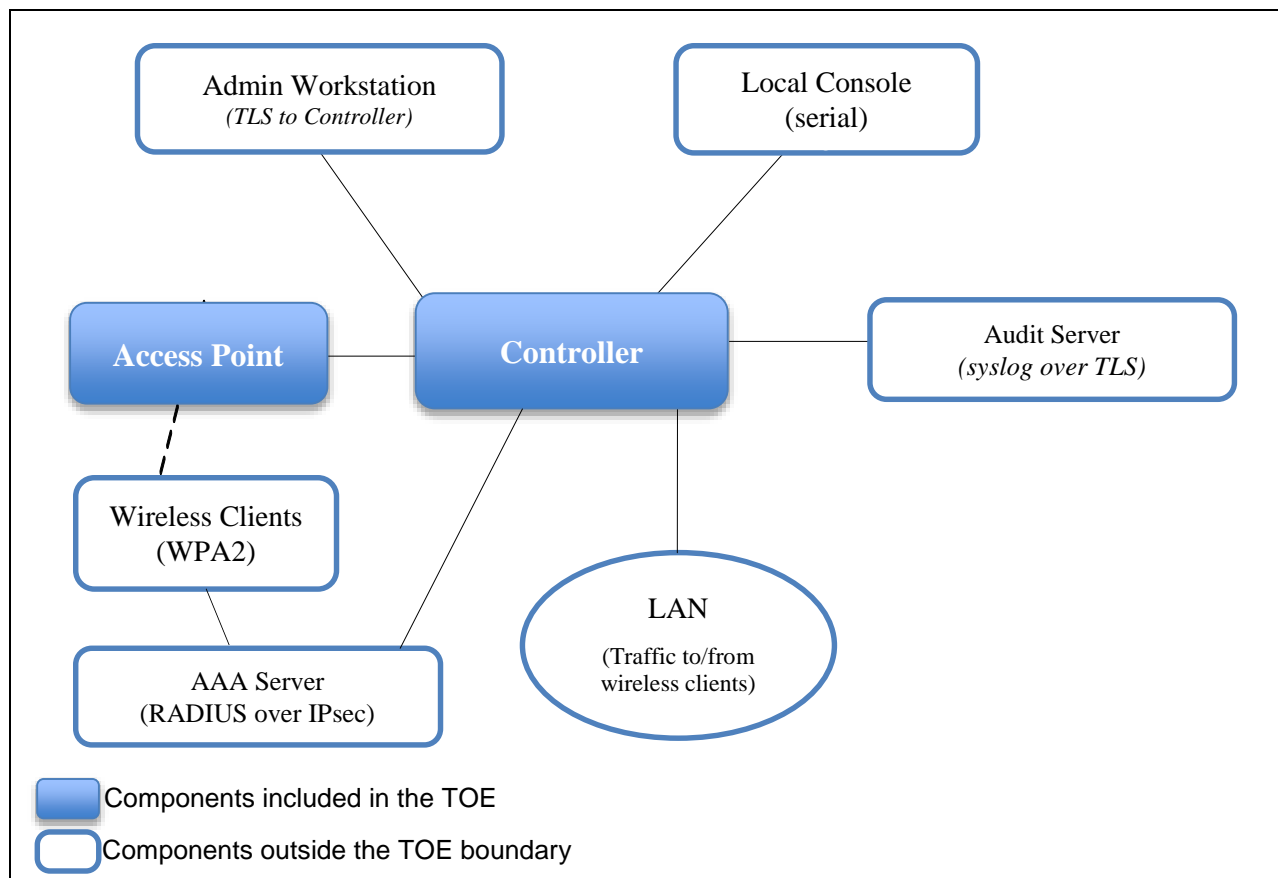
functions (such as throughput and amount of storage) and therefore support security-relevant hardware equivalency of the controllers and of the access points.

Core hardware features of the WLAN controllers and APs include:

- Central processor that supports all system operations;
- Dynamic memory, used by the central processor for all system operation.
- Flash memory (EEPROM), used to store the software image.
- USB port (v2.0) (note, none of the USB devices are included in the TOE).
  - Type A for Storage, all Cisco supported USB flash drives.
  - Type mini-B as console port in the front.
- Non-volatile read-only memory (ROM) is used to store the bootstrap program and power-on diagnostic programs.
- Non-volatile random-access memory (NVRAM) is used to store controller configuration parameters that are used to initialize the system at start-up.
- Physical network interfaces (minimally two) (e.g. multiple RJ45 10/100/1000 Mb Ethernet ports on Controllers, or Ethernet plus wireless radio interface on APs). Some models have a fixed number and/or type of interfaces; some models have slots that accept additional network interfaces.

The following figure shows a sample TOE deployment, and the logical interconnections to/from TOE components.

Figure 1: TOE Deployment Diagram



## 1.4 TOE Evaluated Configuration

The evaluated configuration of the TOE consists of at least one WLAN controller and at least one wireless access point (as identified in section 1.5 below) and includes the WLAN software running on the controllers, and IOS software running on the access points. The software image “bundle” installed to controllers includes the controller’s software image and also includes IOS software images for all the supported AP models, which receive their IOS image directly from the controller when they are ‘joined’ with a controller.

The deployed TOE will mediate traffic flows across several networks: at least one wireless network, and multiple wired networks including at least one IPsec tunnel to AAA and syslog servers. Each AP provides connectivity for one or more wireless network and for one wired network that will carry traffic between the AP and its controller.






The TOE can be administered using any of: a local console connection (CLI) to the Controllers or TLS/HTTPS (GUI) to the Controllers. No direct administration of the APs is supported once the APs have joined a controller, at which point APs are administered via a controller.




The operational environment of the TOE will include at least one RADIUS server for authentication of wireless clients and optionally for authentication of TOE administrators. The environment will also include an audit (syslog) server, and a Certificate Authority (CA) server, and may include NTP servers for clock synchronization.



## 1.5 Physical Scope of the TOE




The TOE is a hardware and software solution that makes up the router models as follows: Cisco 2504, 5508, 7510, 8510, and WiSM2 Controllers; Cisco 1142, 1262, 1530, 1552, 1570 series, 1600 series, 1700 series, 2600 series, 2700 series, 3502, 3600 series with 3000M add-on module, 3700 series APs, and ISR 891 integrated APs. The network, on which they reside, is considered part of the environment. The TOE guidance documentation that is considered to be part of the TOE can be found listed in the Cisco WLAN Common Criteria Operational User Guidance and Preparative Procedures document and are downloadable from the <http://cisco.com> web site. The TOE is comprised of the following physical specifications as described in Table 5 below:



**Table 5 Hardware Models and Specifications**

Hardware Platform	Picture and Part Numbers (Where '*' = licensing options or country-specific radio identifier.)	Interfaces and Features
Cisco 2504 Wireless Controller 	AIR-CT2504-5-K9 AIR-CT2504-15-K9 AIR-CT2504-25-K9 AIR-CT2504-50-K9	Cisco 2500 Series Wireless Controller enables system-wide wireless functions in small to medium-sized enterprises and branch offices. Designed for 802.11n performance, Cisco 2500 Series Wireless Controllers are entry-level controllers that support management of up to 75 access points.
Cisco 5500 Series Wireless LAN Controller 	AIR-CT5508-12-K9 AIR-CT5508-25-K9 AIR-CT5508-50-K9 AIR-CT5508-100-K9 AIR-CT5508-250-K9 AIR-CT5508-500-K9	Cisco 5500 Series Wireless LAN Controller supports up to 500 access points. The Cisco 5508 Wireless LAN Controller supports 12, 25, 50, 100, 250 or 500 access points. FIPS Kit AIR-CT5508FIPSKIT=.
Cisco Flex 7500 Series Cloud Controllers 	AIR-CT7510-300-K9 AIR-CT7510-500-K9 AIR-CT7510-1K-K9 AIR-CT7510-2K-K9 AIR-CT7510-3K-K9 AIR-CT7510-6K-K9	Cisco 7500 Series Cloud Controllers can manage wireless access points in up to 6000 branch locations, or 6000 access points and 64,000 clients.
Cisco 8500 Series Wireless Controllers 	AIR-CT8510-300-K9 AIR-CT8510-500-K9 AIR-CT8510-1K-K9 AIR-CT8510-3K-K9 AIR-CT8510-6K-K9 AIR-CT8510-SP-K9 AIR-CT85DC-SP-K9	Cisco 8500 Series Wireless Controllers provide right-to-use license enablement (with EULA agreement) for faster time to deployment, with the flexibility to add additional access points (up to 6000 access points).
Wireless Integrated Service Module 2 (WiSM2) for Catalyst 6500 	WS-SVC-WISM-1-K9 WS-SVC-WISM2-1-K9 WS-SVC-WISM2-3-K9 WS-SVC-WISM2-5-K9	Cisco WiSM2 is a hardware service module for the Catalyst 6500 switch chassis. Each WiSM2 blade supports up to 300 Access Points. The Supervisor 720 provides routing and switching to support network connectivity to the management interface of the WiSM2.  The WiSM2 controllers support the following 5 chassis configurations: 6503, 6504, 6506, 6509 and 6513. The chassis vary in the number of slots they provide, but this difference does not affect the security functionality claimed by the


Hardware Platform	Picture and Part Numbers (Where '*' = licensing options or country-specific radio identifier.)	Interfaces and Features
		<p>TOE.</p> <p>Though the 6500 chassis is not part of the physical TOE boundary, the evaluated configuration requires that the Catalyst 6500 be installed with its FIPS Kit, Cisco product number CVPN6500FIPS/KIT.</p>
<p>Cisco Aironet 1142 AG Series Access Point</p> 	<p>AIR-LAP1142N-A-K9  AIR-LAP1142N-C-K9  AIR-LAP1142N-E-K9  AIR-LAP1142N-P-K9  AIR-LAP1142N-K-K9  AIR-LAP1142N-N-K9  AIR-LAP1142N-S-K9  AIR-LAP1142N-T-K9  AIR-LAP1142N-I-K9</p>	<p>The Cisco Aironet 1142 AG Series IEEE 802.11a/b/g/n Access Point is a fixed-configuration dual-band Access Point. The Cisco 1142 AG Series IEEE 802.11a/b/g/n Access Point provides two radios each with diversity antennas that provide omni-directional coverage. The TOE's physical boundary includes the listed Cisco Aironet 1142 AG Series Access Points which are considered hardware components of the TOE. This module is within the TOE boundary.</p>
<p>Cisco Aironet 1262 AG Series Access Point</p> 	<p>AIR-LAP1262N-A-K9  AIR-LAP1262N-*-K9  (Where '*' is the country-specific radio type identifier.)</p>	<p>The Cisco Aironet 1262 AG Series IEEE 802.11a/b/g/n Access Point is a fixed-configuration dual-band Access Point. The Cisco 1262 AG Series IEEE 802.11a/b/g/n Access Point provides two radios each with diversity antennas that provide omni-directional coverage. The TOE's physical boundary includes the listed Cisco Aironet 1262 AG Series Access Points which are considered hardware components of the TOE. This module is within the TOE boundary.</p>
<p>1530e and 1530i  'e' = external antenna  'i' = internal antenna</p> 	<p>AIR-CAP1532I-A-K9  AIR-CAP1532E-A-K9  AIR-CAP1532I-*-K9  AIR-CAP1532E-*-K9  (Where '*' is the country-specific radio type identifier.)</p>	<p>10/100/1000BASE-T autosensing (RJ-45)  Management console port (RJ-45)  Antenna:</p> <ul style="list-style-type: none"> <li>• 2.4 GHz, gain 4.0 dBi, horizontal beamwidth 360°</li> <li>• 5 GHz, gain 4.0 dBi, horizontal beamwidth 360°</li> </ul> <p>Data Rates Supported:</p> <ul style="list-style-type: none"> <li>• 802.11a/b/g/n multiple-input multiple-output (MIMO), with two or three spatial streams and up to 300-Mbps.</li> </ul>

Hardware Platform	Picture and Part Numbers (Where '*' = licensing options or country-specific radio identifier.)	Interfaces and Features
<p>1552e/eu/c/cu/h/i  'e' = external dual-band antennas  eu = external single-band antennas  c = integrated cable modem, plus integrated dual-band antenna  cu = integrated cable modem, plus external dual-band antennas  h = hazardous location housing for environments like oil and gas refineries, chemical plants, mining pits, and manufacturing factories, plus options similar to 1552E  'i' = integrated dual-band antenna</p>	 <p>Cisco Aironet 1552E/1552EU</p> <ul style="list-style-type: none"> <li>• AIR-CAP1552E-A-K9</li> <li>• AIR-CAP1552E-*-K9</li> <li>• AIR-CAP1552EU-A-K9</li> <li>• AIR-CAP1552EU-*-K9</li> </ul> <p>Cisco Aironet 1552C/1552CU Access Point with DOCSIS 3.0 Cable Modem</p> <ul style="list-style-type: none"> <li>• AIR-CAP1552C-A-K9</li> <li>• AIR-CAP1552C-*-K9</li> <li>• AIR-CAP1552CU-A-K9</li> <li>• AIR-CAP1552CU-*-K9</li> </ul> <p>Cisco Aironet 1552H Hazardous Location Access Point</p> <ul style="list-style-type: none"> <li>• AIR-CAP1552H-A-K9</li> <li>• AIR-CAP1552H-*-K9</li> </ul> <p>Cisco Aironet 1552I Integrated Antenna Access Point</p> <ul style="list-style-type: none"> <li>• AIR-CAP1552I-A-K9</li> <li>• AIR-CAP1552I-*-K9</li> </ul>	<p>10/100/1000BASE-T autosensing (RJ-45)  Management console port (RJ-45)  C and CU models have an integrated cable modem interface (with DOCSIS 3.0/EuroDOCSIS 3.0 (8x4 HFC) compliant cable modem)  Antenna (where the '*' in the sample part numbers in this table represent country-specific radio frequency ranges):</p> <ul style="list-style-type: none"> <li>• 2.4 GHz, gain 4.0 dBi, horizontal beamwidth 360°</li> <li>• 5 GHz, gain 4.0 dBi, horizontal beamwidth 360°</li> </ul> <p>Data Rates Supported:</p> <ul style="list-style-type: none"> <li>• 802.11a: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps</li> <li>• 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps</li> <li>• 802.11n data rates (2.4 GHz1 and 5 GHz): 6.5 to 300 Mbps</li> </ul>
<p>Cisco Aironet 1570 Series Outdoor Access Point</p> 	<p>Cisco Aironet 1572EAC (External Antenna, AC Power Model)</p> <ul style="list-style-type: none"> <li>• AIR-AP1572EAC-x-K9</li> </ul> <p>Cisco Aironet 1572IC (Internal Antenna, PoC Model)</p> <ul style="list-style-type: none"> <li>• AIR-AP1572IC1-x-K9</li> <li>• AIR-AP1572IC2-x-K9</li> <li>• AIR-AP1572IC3-x-K9</li> <li>• AIR-AP1572IC4-x-K9</li> </ul> <p>Cisco Aironet 1572EC (External Antenna, PoC Model)</p> <ul style="list-style-type: none"> <li>• AIR-AP1572EC1-x-K9</li> <li>• AIR-AP1572EC2-x-K9</li> <li>• AIR-AP1572EC3-x-K9</li> <li>• AIR-AP1572EC4-x-K9</li> </ul>	<p>The Cisco Aironet 1570 Series IEEE 802.11a/b/g/n/ac is a fixed-configuration outdoor Access Point. The TOE's physical boundary includes the listed Cisco Aironet 1570 Series Access Points which are considered hardware components of the TOE. This module is within the TOE boundary.</p> <p>Data Rates Supported:</p> <ul style="list-style-type: none"> <li>• 802.11b/g (2.4 GHz): 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps</li> <li>• 802.11n data rates (2.4 GHz1 and 5 GHz): 6.5 to 450 Mbps</li> <li>• 802.11a (5 GHz): 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps</li> <li>• 802.11ac (5 GHz): 6.5 to 1300 Mbps</li> </ul>

Hardware Platform	Picture and Part Numbers (Where '*' = licensing options or country-specific radio identifier.)	Interfaces and Features
1600e and 1600i 'e' = external antenna 'i' = internal antenna	 <p>AIR-CAP1602I-x-K9 (quantity = 1)            AIR-CAP1602I-xK910 (qty. 10)            AIR-CAP1602E-x-K9 (quantity = 1)            AIR-CAP1602E-xK910 (qty. 10)</p>	10/100/1000BASE-T autosensing (RJ-45) Management console port (RJ-45) Antenna: <ul style="list-style-type: none"> <li>• 2.4 GHz, gain 4.0 dBi, horizontal beamwidth 360°</li> <li>• 5 GHz, gain 4.0 dBi, horizontal beamwidth 360°</li> </ul> Data Rates Supported: <ul style="list-style-type: none"> <li>• 802.11a: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps</li> <li>• 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps</li> </ul> 802.11n data rates (2.4 GHz <sup>1</sup> and 5 GHz): 6.5 to <b>300 Mbps</b>
Cisco Aironet 1700 Series Access Point 	Cisco Aironet 1700i <ul style="list-style-type: none"> <li>• AIR-CAP1702I- x-K9</li> <li>• AIR-CAP1702I- xK910</li> </ul>	The Cisco Aironet 1700i Series IEEE 802.11a/b/g/n/h/d Access Point is a fixed-configuration dual-band Access Point with Integrated Antenna providing omni-directional coverage. The TOE's physical boundary includes the listed Cisco Aironet 1700i Series Access Points which are considered hardware components of the TOE. This module is within the TOE boundary. Dual-band, controller-based 802.11a/g/n/ac 2x10/100/1000BASE-T autosensing (RJ-45) Management console port (RJ-45) <ul style="list-style-type: none"> <li>• 2.4 GHz, gain 4 dBi, internal omni, horizontal beamwidth 360°</li> <li>• 5 GHz, gain 4 dBi, internal omni, horizontal beamwidth 360°</li> </ul> Data Rates Supported: <ul style="list-style-type: none"> <li>• 802.11a: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps</li> <li>• 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps</li> <li>• 802.11n data rates (2.4 GHz<sup>1</sup> and 5 GHz): 6.5 to 300 Mbps</li> </ul>
2600e and 2600i 'e' = external antenna 'i' = internal antenna 	AIR-CAP2602I-*K9 (quantity 1) AIR-CAP2602I-*K910 (qty. 10) AIR-CAP2602E-*K9 (quantity 1) AIR-CAP2602E-*K910 (qty. 10)	10/100/1000BASE-T autosensing (RJ-45) Management console port (RJ-45) Antenna: <ul style="list-style-type: none"> <li>• 2.4 GHz, gain 4.0 dBi, horizontal beamwidth 360°</li> <li>• 5 GHz, gain 4.0 dBi, horizontal beamwidth 360°</li> </ul> Data Rates Supported: <ul style="list-style-type: none"> <li>• 802.11a: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps</li> <li>• 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps</li> <li>• 802.11n data rates (2.4 GHz<sup>1</sup> and 5 GHz): 6.5 to 450 Mbps</li> </ul>

Hardware Platform	Picture and Part Numbers (Where '*' = licensing options or country-specific radio identifier.)	Interfaces and Features
2700e and 2700i 'e' = external antenna 'i' = internal antenna	AIR-CAP2702I-*-K9 (quantity 1) AIR-CAP2702I-*K910 (qty. 10) AIR-CAP2702E-*-K9 (quantity1) AIR-CAP2702E-*K910 (qty. 10)	10/100/1000BASE-T autosensing (RJ-45) Management console port (RJ-45) Antenna: <ul style="list-style-type: none"> <li>• 2.4 GHz, gain 4.0 dBi, horizontal beamwidth 360°</li> <li>• 5 GHz, gain 4.0 dBi, horizontal beamwidth 360°</li> </ul> Data Rates Supported: <ul style="list-style-type: none"> <li>• 802.11a: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps</li> <li>• 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps</li> <li>• 802.11n data rates (2.4 GHz<sup>1</sup> and 5 GHz): 6.5 to 450 Mbps</li> </ul>
3500e and 3500i '2I' models have dual-band integrated antenna '1I' models have single-band integrated antenna '2E' models have dual-band external antennas '1E' models have single-band external antennas	 AIR-CAP3502I-x-K9 AIR-CAP3502I-xK910 (qty. 10) AIR-CAP3501I-x-K9 AIR-CAP3502E-x-K9 AIR-CAP3502E-xK910 (qty. 10) AIR-CAP3501E-x-K9	10/100/1000BASE-T autosensing (RJ-45) Management console port (RJ-45) Antenna: <ul style="list-style-type: none"> <li>• 2.4 GHz, gain 4.0 dBi, horizontal beamwidth 360°</li> <li>• 5 GHz, gain 4.0 dBi, horizontal beamwidth 360°</li> </ul> Data Rates Supported: <ul style="list-style-type: none"> <li>• 802.11a: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps</li> <li>• 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps</li> <li>• 802.11n data rates (2.4 GHz<sup>1</sup> and 5 GHz): 6.5 to 300 Mbps</li> </ul>
3600e and 3600i 'e' = external antenna 'i' = internal antenna  <i>Optional IEEE 802.11ac Adaptive Radio Module to increase wireless data throughput rates, range, and capacity.</i> AIR-RM3000AC-x-K9 AIR-RM3000MACxK910(qty. 10)  <i>Optional Cisco AIR-RM3000M Monitor Module helps avoid RF interference to obtain better coverage and performance on the wireless network.</i> AIR-RM3000M AIR-RM3000M-10(qty. 10)	 AIR-CAP3602I-x-K9 AIR-CAP3602I-xK910 (qty. 10) AIR-CAP3602E-x-K9 AIR-CAP3602E-xK910 (qty. 10)	10/100/1000BASE-T autosensing (RJ-45) Management console port (RJ-45) Antenna: <ul style="list-style-type: none"> <li>• 2.4 GHz, gain 4.0 dBi, horizontal beamwidth 360°</li> <li>• 5 GHz, gain 4.0 dBi, horizontal beamwidth 360°</li> </ul> Data Rates Supported: <ul style="list-style-type: none"> <li>• 802.11a: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps</li> <li>• 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps</li> <li>• 802.11n data rates (2.4 GHz<sup>1</sup> and 5 GHz): 6.5 to 216.7 Mbps</li> <li>• Optional 802.11ac module (5 GHz) : 6.5 to 1300 Mbps</li> </ul>



Hardware Platform	Picture and Part Numbers (Where '*' = licensing options or country-specific radio identifier.)	Interfaces and Features
3700e, 3700i and 3700p  'i' = internal antenna 'p' = narrow-beamwidth antenna  All 3700 models include IEEE 802.11ac Adaptive Radio Module	AIR-CAP3702I-x-K9 AIR-CAP3702I-xK910 (qty. 10) AIR-CAP3702E-x-K9 AIR-CAP3702E-xK910 (qty. 10) AIR-CAP3702P-x-K9 AIR-CAP3702P-xK910 (qty. 10)	10/100/1000BASE-T autosensing (RJ-45) Management console port (RJ-45) Antenna: <ul style="list-style-type: none"> <li>• 2.4 GHz, gain 4.0 dBi, horizontal beamwidth 360°</li> <li>• 5 GHz, gain 4.0 dBi, horizontal beamwidth 360°</li> </ul> Data Rates Supported: <ul style="list-style-type: none"> <li>• 802.11a: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps</li> <li>• 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps</li> <li>• 802.11n data rates (2.4 GHz and 5 GHz): 6.5 to 450 Mbps</li> <li>• 802.11ac module (5 GHz) : 6.5 to 1300 Mbps</li> </ul>
891 ISR integrated AP 	CISCO891W-AGN-A-K9 CISCO891W-AGN-N-K9 C891FW-A-K9 C891FW-E-K9	<ul style="list-style-type: none"> <li>• Support for CleanAir technology on Cisco 897 and 891F</li> <li>• Automatic rate selection for 802.11a/g/n</li> <li>• Noncaptive RPTNC omnidirectional dipole antennae; 2-dBi gain @ 2.4 GHz, 5-dBi gain @ 5 GHz</li> <li>• 2 x 3 MIMO radio operation</li> <li>• Wi-Fi 802.11n Draft v2.0 certified</li> </ul>

## 1.6 Logical Scope of the TOE

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

1. Security Audit
2. Cryptographic Support
3. User Data Protection
4. Identification and Authentication
5. Security Management
6. Protection of the TSF, and Resource Allocation
7. TOE Access
8. Trusted Path/Channels

These features are described in more detail in the subsections below. In addition, the TOE implements all RFCs of the PP as necessary to satisfy testing/assurance measures prescribed therein.

### 1.6.1 Security Audit

The Cisco WLAN provides extensive auditing capabilities. The TOE can audit events related to cryptographic functionality, identification and authentication, and administrative actions. The Cisco WLAN generates an audit record for each auditable event. Each security relevant audit event has the date, timestamp, event description, and subject identity. The administrator configures auditable events, performs back-up operations, and manages audit data storage. The TOE provides the administrator with a circular audit trail or a configurable audit trail threshold to track the storage capacity of the audit trail. Audit logs are transmitted over an encrypted channel to an external audit server.

### 1.6.2 Cryptographic Support

The TOE provides cryptography in support of:

- IPsec to secure communications between the WLC and RADIUS server.
- TLS/HTTPS for secure remote administration using WebGUI.
- TLS to secure communications between WLC remote syslog server.
- Data TLS to secure communications between APs and WLC.
- WPA2 to secure communications between APs and wireless clients.

This cryptography in WLC and AP TOE components has been validated for conformance to the requirements of FIPS 140-2 Level 2. See Table 6 for CMVP certificate references.

**Table 6 FIPS References – Controllers and APs**

Model	CMVP#	AES	AES-CCM	HMAC	DRBG	RSA	SHS
<b>Controllers</b>							
2504	#2497	#1348, #2894, #2895		#1830, #1831, #1840, #787	#526	#1524	#1230, #2437, #2438
5508	#2365	#2894, #2895, and #1348		#1840, #1830, #1831, and #787	#526	#1524	#1230, #2437, #2438
7510	#2497	#1348, #2894, #2895		#1830, #1831, #1840, #787	#526	#1524	#1230, #2437, #2438
8510	#2497	#1348, #2894, #2895		#1830, #1831, #1840, #787	#526	#1524	#1230, #2437, #2438
WiSM	#2497	#1348, #2894,		#1830, #1831,	#526	#1524	#1230, #2437,

Model	CMVP#	AES	AES-CCM	HMAC	DRBG	RSA	SHS
		#2895		#1840, #787			#2438
<b>APs &amp; Integrated APs</b>							
1142	#2421	#2817	#2336	#1764	#481	#1471	#2361
1262	#2421	#2335	#2335	#1764	#481	#1471	#2361
1530	#2421	#2817, #2450	#2450	#1764	#481	#1471	#2361
1552	#2421	#2817	#2335	#1764	#481	#1471	#2361
1570	#2421	#2901	#2334	#1836	#534	#1529	#2441
1600 Series	#2421	#2901	#2846	#1836	#534	#1529	#2441
1700 Series	#2421	#2901	#2334	#1836	#534	#1529	#2441
2600 Series	#2421	#2901	#2334	#1836	#534	#1529	#2441
2700 Series	#2421	#2901	#2334	#1836	#534	#1529	#2441
3502	#2421	#2335	#2335	#1836	#534	#1529	#2441
3600 Series	#2421	#2234	#2234	#1836	#534	#1529	#2441
3700 Series	#2421	#2901,	#2334	#1836	#534	#1529	#2441
891 ISR integrated AP		#2817	#2611	#1764, #1618	#481	#1471	#2361, #2194

The cryptographic services provided by the TOE are described in Table 7 below.

**Table 7 TOE Provided Cryptography**

Cryptographic Service	Use within the TOE
IPsec	Secure communications between controller and RADIUS server.
TLS	<ul style="list-style-type: none"> <li>Establishment and subsequent data transfer of a remote TLS/HTTPS session between the WebGUI and authorized administrator.</li> <li>Protection of WLC syslog messages.</li> </ul>
RSA Signature Services	Used in IPsec session establishment. Used in TLS session establishment. Used in X.509 certificate signing.

Cryptographic Service	Use within the TOE
SP 800-90 RBG	Used in IPsec session establishment. Used in TLS session establishment. Used to generate Group Temporal Key (GTK).
SHS	Used to provide IPsec traffic integrity verification. Used to provide TLS traffic integrity verification.
AES	Used to encrypt IPsec session traffic. Used to encrypt TLS session traffic.
AES-CCMP	Used in WPA2 over-the-air encryption/decryption.

### 1.6.3 User Data Protection

The TOE ensures that all information flows from the TOE do not contain residual information from previous traffic. Residual data is never transmitted from the TOE, and when packets must be padded, they are padded with zeros.

### 1.6.4 Identification and authentication

The TOE provides authentication services for administrative users of the TOE who connect locally to the CLI via serial console of the WLAN Controller or remotely to the GUI over TLS. The TOE requires administrators to authenticate prior to being granted access to any of the management functionality. The TOE can be configured to require a minimum password length and to enforce mandatory password complexity rules. All of the local and remote CLI and GUI connections the TOE support password-based authentication of administrators against either a local user database or remote RADIUS server.

For authentication of wireless clients a RADIUS server must be used (AAA servers are outside the TOE boundary). The TOE requires the wireless client to perform 802.1X authentication, relying on an authentication server to authenticate the client, before providing network access. The TOE acts as a pass through device between the wireless client and authentication server.

The TOE facilitates authentication of wireless clients by performing the role of authenticator in an 802.1X authentication exchange. During an 802.1X authentication exchange, wireless client authentication is relayed by the WLC to a RADIUS server. The TOE will block access to the port until the authentication server returns an authentication success message and 802.11 temporal keys are derived and installed on the wireless client and AP. The TOE provides IPsec to protect the transfer of the Pairwise Master Key the WLC receives from the RADIUS server.

### 1.6.5 Security Management

Through CLI, and GUI of the Controller, the TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. Functions available to authorized administrators include, but are not limited to:

- Enabling, disabling, and configuring audit collection.
- Modifying the behavior of cryptographic functions;

- Configuring security of communications to/from an external servers including RADIUS and syslog servers;
- Adding/removing/modifying administrative accounts including specifying a maximum number of successive failed authentication attempts that will be permitted by remote administrators;
- Defining inactivity timeout limits for interactive interfaces to terminate inactive sessions;
- Creating custom login banners for interactive interfaces to be displayed at time of login.

Accounts with access to CLI and GUI can have read-write access, or can be assigned to lesser sets of privileges that can be custom-defined. Authorized administrators are users who have successfully authenticated to the TOE, and have been granted the necessary privilege to perform some administrative actions, which may be limited to read-only actions.

### 1.6.6 Protection of the TSF, and Resource Allocation

The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication, and access controls to limit configuration to Authorized Administrators. The TOE prevents reading of plaintext cryptographic keys and passwords. Additionally none of the components of the TOE includes a general-purpose operating systems and access to the memory space is restricted to only system functions.

Authorized administrators have the option to verify the integrity of software updates using cryptographic signatures prior to the software updates being installed. Self-testing is performed during boot-up to verify correct operation of system hardware and the cryptographic module. When power-on self-tests (POST) fail for any controller or AP, the device will not progress to an operational mode (e.g. will not forward network traffic, nor authenticate wireless clients or administrators, etc.).

System resources used to support administrative interfaces are protected by allowing authorized administrators to limit the number of concurrent sessions. TOE components will detect and drop (not forward) replayed packets received at network interfaces (including wireless radio interfaces).

Each TOE component internally maintains the date and time, and clocks are synchronized among components. This date and time is used as the timestamp that is applied to audit records generated by the TOE. Administrators can update the TOE's clock manually, and/or can configure the TOE to use NTP to synchronize the TOE's clock with an external time source.

### 1.6.7 TOE Access

Administrative sessions can be set to terminate after a configurable idle-time limit. Once a session has been terminated the TOE requires administrators to re-authenticate to establish a new session. A customizable login-banner can be displayed at the CLI and GUI login prompts prior to allowing any administrative access to the TOE.

Wireless client session establishment can be restricted by day, time, and 'location', which can be an IP address or WLAN ID.

### 1.6.8 Trusted path/Channels

The wireless connections between the APs and wireless clients are secured using Wi-Fi Protected Access 2 (WPA2). Specifically, the TOE uses Advanced Encryption Standard – Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP), as defined in the WPA2 standard. TSF data (command and control data, audit data, etc.) transmitted among controllers and APs of the TOE are secured with Data TLS (for CAPWAP over DTLS) using ciphersuites required by the WLANPP for the TLS connections. Securing user data between TOE components is optional, but is not a requirement of the WLANPP, and thus is outside the scope of evaluation.

Communications to/from non-TOE servers including RADIUS and syslog servers are secured using IPsec or TLS.

Remote administrators can establish trusted communication paths to controllers using TLS/HTTPS. Once APs are joined to the TOE, they are not managed directly through console connection or remote administrative interface, but instead are managed through the controller's administrative interfaces.

Inter-TOE communication is secured as follows:

- Communication among Controllers and APs uses Data TLS.

## 1.7 Excluded Functionality

The following functionality is excluded from the evaluation.

**Table 8 Excluded Functionality**

Excluded Functionality	Exclusion Rationale
Non-FIPS 140-2 mode of operation on the TOE	This mode of operation includes non-FIPS allowed operations.
WLC management using SSH or SNMP	Remote administration of the WLC is provided by the WebGUI over TLS/HTTPS.

These services will be disabled by configuration. The exclusion of this functionality does not affect compliance to the Protection Profile for Wireless Local Area Network (WLAN) Access Systems.

## 2 CONFORMANCE CLAIMS

### 2.1 Common Criteria Conformance Claim

The TOE and ST are compliant with the Common Criteria (CC) Version 3.1, Revision 4, dated: September 2012. For a listing of Assurance Requirements claimed see section 5.5.

The TOE and ST are CC Part 2 extended and CC Part 3 conformant.

### 2.2 Protection Profile Conformance

The TOE and ST are conformant with the Protection Profiles as listed in Table 9 below:

**Table 9 Protection Profiles**

Protection Profile	Version	Date
Protection Profile for Wireless Local Area Network (WLAN) Access Systems (WLANPP)	1.0	01 December, 2011

### 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 Profile:

- Protection Profile for Wireless Local Area Network (WLAN) Access Systems, v1.0

This ST applies the following NIAP Technical Decisions:

- TD0002: FIA\_PMG\_EXT.1 Requirement in WLAN AS PP v1.0
- TD0010: WLAN AS PP Flawed Statement of FAU\_SEL.1
- TD0021: Update to Limits on SA Lifetimes for IKE v1 and IKE v2
- TD0022: Removal of Image Verification Test for WLAN AS PP
- TD0036: Removal of Low-level Crypto Failure Audit in WLAN AS PP

#### 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 the Protection Profile for Wireless Local Area Network (WLAN) Access Systems, version (none) 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 the WLANv1.0 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 the WLANv1.0 for which conformance is claimed verbatim. All concepts covered in the Protection Profile's Statement of Security Requirements are included in this Security Target. Additionally, the Security Assurance Requirements included in this Security Target are identical to the Security Assurance Requirements included in section 4.3 of the WLANv1.0



### 3 SECURITY PROBLEM DEFINITION

This chapter identifies the following:

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

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

#### 3.1 Assumptions

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

**Table 10 TOE Assumptions**

Assumption	Description of Assumption
A.NO_GENERAL_PURPOSE	It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available to the TOE, other than those services necessary for the operation, administration and support of the TOE.
A.NO_TOE_BYPASS	Information cannot flow between the wireless client and the internal wired network without passing through the TOE.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

#### 3.2 Threats

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

**Table 11 Threats**

Threat	Description of Threat
T.ADMIN_ERROR	An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
T.RESOURCE_EXHAUSTION	A process or user may deny access to TOE services by exhausting critical resources on the TOE.

Threat	Description of Threat
T.TSF_FAILURE	Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
T.UNAUTHORIZED_ACCESS	A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
T.UNAUTHORIZED_UPDATE	A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
T.UNDETECTED_ACTIONS	Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.
T.USER_DATA_REUSE	User data may be inadvertently sent to a destination not intended by the original sender.

### 3.3 Organizational Security Policies

The following table lists the Organizational Security Policies imposed by an organization to address its security needs.

**Table 12 Organizational Security Policies**

Policy	Policy Description
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.
P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE.
P.ADMIN_ACCESS	Administrators shall be able to administer the TOE both locally and remotely through protected communications channels.
P.COMPATIBILITY	The TOE must meet Request for Comments (RFC) requirements for implemented protocols to facilitate inter-operation with other network equipment (e.g., certificate authority, NTP server) using the same protocols.
P.EXTERNAL_SERVERS	The TOE must support standardized (RFCs) protocols for communication with a centralized audit server and a RADIUS authentication server.

## 4 SECURITY OBJECTIVES

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

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

### 4.1 Security Objectives for the TOE

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

**Table 13 Security Objectives for the TOE**

TOE Objective	Objective Description
O.AUTH_COMM	The TOE will provide a means to ensure users are not communicating with some other entity pretending to be the TOE, and that the TOE is communicating with an authorized IT entity and not some other entity pretending to be an authorized IT entity.
O.CRYPTOGRAPHIC_FUNCTIONS	The TOE shall provide cryptographic functions (i.e., encryption/decryption and digital signature operations) to maintain the confidentiality and allow for detection of modification of TSF data that is transmitted between physically separated portions of the TOE, or stored outside the TOE.
O.DISPLAY_BANNER	The TOE will display an advisory warning regarding use of the TOE.
O.FAIL_SECURE	The TOE shall fail in a secure manner following failure of the power-on self tests.
O.PROTECTED_COMMUNICATIONS	The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
O.PROTOCOLS	The TOE will ensure that standardized protocols are implemented in the TOE to RFC and/or Industry specifications to ensure interoperability, that also support communication with a centralized audit server and a RADIUS authentication server.
O.REPLAY_DETECTION	The TOE will provide a means to detect and reject the replay of authentication data and other TSF data and security attributes.
O.RESIDUAL_INFORMATION_CLEARING	The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated.
O.RESOURCE_AVAILABILITY	The TOE shall provide mechanisms that mitigate user attempts to exhaust TOE resources (e.g., persistent storage).
O.ROBUST_TOE_ACCESS	The TOE will provide mechanisms that control an administrator's logical access to the TOE and to control administrative access from a wireless client.
O.SESSION_LOCK	The TOE shall provide mechanisms that mitigate the risk of unattended sessions being hijacked.

TOE Objective	Objective Description
O.SYSTEM_MONITORING	The TOE will provide the capability to generate audit data and send those data to an external IT entity.
O.TIME_STAMPS	The TOE shall provide reliable time stamps and the capability for the administrator to set the time used for these timestamps.
O.TOE_ADMINISTRATION	The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE, and provide protections for logged-in administrators.
O.TSF_SELF_TEST	The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly.
O.VERIFIABLE_UPDATES	The TOE will provide the capability to help ensure that any updates to the TOE can be verified by the administrator to be unaltered and (optionally) from a trusted source.
O.WIRELESS_CLIENT_ACCESS	The TOE will provide the capability to restrict a wireless client in connecting to the TOE.

## 4.2 Security Objectives for the Environment

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

**Table 14 Security Objectives for the Environment**

Environmental Objective	Objective Description
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available to the TOE, other than those services necessary for the operation, administration and support of the TOE.
OE.NO_TOE_BYPASS	Information cannot flow between external and internal networks located in different enclaves without passing through the TOE.
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the IT environment.
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

## 5 SECURITY REQUIREMENTS

This section identifies the Security Functional Requirements for the TOE. The Security Functional Requirements included in this section are derived from Part 2 of the *Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, dated: September 2012* and all international interpretations.

### 5.1 Conventions

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

- Assignment: Indicated with *italicized* text;
- Refinement: Indicated with **bold** text;
- Selection: Indicated with underlined text;
- Iteration: Indicated by appending the iteration number in parenthesis, e.g., (1), (2), (3).
- Where operations were completed in the WLANPP itself, the formatting used in the WLANPP has been retained.

Explicitly stated SFRs are identified by having a label ‘EXT’ after the requirement name for TOE SFRs. Formatting conventions outside of operations and iterations matches the formatting specified within the WLANPP.

### 5.2 TOE Security Functional Requirements

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

**Table 15 Security Functional Requirements**

Class Name	Component Identification	Component Name
FAU: Security audit	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User Identity Association
	FAU_SEL.1	Selective Audit
	FAU_STG.1	Protected Audit Trail Storage (Local Storage)
	FAU_STG_EXT.1	External Audit Trail Storage
	FAU_STG_EXT.3	Action in Case of Loss of Audit Server Connectivity
FCS: Cryptographic support	FCS_CKM.1(1)	Cryptographic Key Generation (Symmetric Keys for WPA2 Connections)
	FCS_CKM.1(2)	Cryptographic Key Generation (Asymmetric Keys)
	FCS_CKM.2(1)	Cryptographic Key Distribution (PMK)
	FCS_CKM.2(2)	Cryptographic Key Distribution (GTK)
	FCS_CKM_EXT.4	Cryptographic Key Zeroization
	FCS_COP.1(1)	Cryptographic Operation (Data Encryption/Decryption)
	FCS_COP.1(2)	Cryptographic Operation (Cryptographic Signature)
FCS_COP.1(3)	Cryptographic Operation (Cryptographic Hashing)	

Class Name	Component Identification	Component Name
	FCS_COP.1(4)	Cryptographic Operation (Keyed-Hash Message Authentication)
	FCS_COP.1(5)	Cryptographic Operation (WPA2 Data Encryption/Decryption)
	FCS_HTTPS_EXT.1	Extended: HTTP Security (HTTPS)
	FCS_IPSEC_EXT.1	Extended: Internet Protocol Security (IPsec) Communications
	FC_SSH_EXT.1	Extended: Secure Shell (SSH)
	FCS_RBG_EXT.1	Extended: Cryptographic Operation (Random Bit Generation)
	FCS_TLS_EXT.1	Extended: Transport Layer Security (TLS)
FDP: User data protection	FDP_RIP.2	Full Residual Information Protection
FIA: Identification and authentication	FIA_AFL.1	Authentication Failure Handling
	FIA_PMG_EXT.1	Password Management
	FIA_UIA_EXT.1	User Identification and Authentication
	FIA_UAU_EXT.5	Password-based Authentication Mechanisms
	FIA_UAU.6	Re-authenticating
	FIA_UAU.7	Protected Authentication Feedback
	FIA_8021X_EXT.1	Extended: 802.1X Port Access Entity (Authenticator) Authentication
	FIA_PSK_EXT.1	Extended: Pre-Shared Key Composition
	FIA_X509_EXT.1	Extended: X509 Certificates
FMT: Security management	FMT_MOF.1	Management of Security Functions Behavior
	FMT_MTD.1(1)	Management of TSF Data (General TSF data)
	FMT_MTD.1(2)	Management of TSF Data (Reading of Authentication Data)
	FMT_MTD.1(3)	Management of TSF Data (Reading of all Symmetric Keys)
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Restrictions on Security Roles
FPT: Protection of the TSF	FPT_ITT.1	Basic Internal TSF Data Transfer Protection
	FPT_FLS.1	Fail Secure
	FPT_RPL.1	Replay Detection
	FPT_STM.1	Reliable Time Stamps
	FPT_TST_EXT.1	Extended: TSF Testing
	FPT_TUD_EXT.1	Extended: Trusted Update
FRU: Resource Utilization	FRU_RSA.1	Maximum Quotas
FTA: TOE Access	FTA_SSL_EXT.1	TSF-initiated Session Locking
	FTA_SSL.3	TSF-initiated Termination
	FTA_SSL.4	User-initiated Termination
	FTA_TAB.1	Default TOE Access Banners
	FTA_TSE.1	TOE Session Establishment
FTP: Trusted path/channels	FTP_ITC.1	Trusted Channel
	FTP_TRP.1	Trusted Path

## 5.3 SFRs Drawn from the WLANPP

### 5.3.1.1 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 administrative actions;
- d) [Specifically defined auditable events listed in Table 16: Auditable Events].

**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 PP/ST, [*information specified in column three of Table 16: Auditable Events*].

**Table 16: Auditable Events**

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None.	
FAU_GEN.2	None.	
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating.	None.
FAU_STG.1	None.	
FAU_STG_EXT.1	None.	
FAU_STG_EXT.3	Loss of connectivity.	None.
FCS_CKM.1(1)	Failure of the key generation activity.	None.
FCS_CKM.1(2)	Failure of the key generation activity.	None.
FCS_CKM.2(1)	Failure of the key distribution activity.	None.
FCS_CKM.2(2)	Failure of the key distribution activity, including failures related to wrapping the GTK.	Identifier(s) for intended recipients of wrapped key.
FCS_CKM_EXT.4	Failure of the key zeroization process.	Identity of subject requesting or causing zeroization, identity of object or entity being cleared.
FCS_COP.1(1)	Failure of the encryption of decryption.	Cryptographic mode of operation, name/identifier of object being encrypted/decrypted.
FCS_COP.1(2)	Failure of cryptographic signature.	Cryptographic mode of operation, name/identifier of object being signed/verified.
FCS_COP.1(3)	Failure of hashing function.	Cryptographic mode of operation, name/identifier of object being hashed.
FCS_COP.1(4)	Failure in Cryptographic Hashing or Non-	Cryptographic mode of operation,

Requirement	Auditable Events	Additional Audit Record Contents
	Data Integrity.	name/identifier of object being hashed.
FCS_COP.1(5)	Failure of WPA2 encryption or decryption.	Cryptographic mode of operation, name/identifier of object being encrypted/decrypted, non-TOE endpoint of connection (IP address).
FCS_HTTPS_EXT.1	Protocol failures Establishment/Termination of a HTTPS session.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.
FCS_IPSEC_EXT.1	Protocol failures. Establishment/Termination of an IPsec SA. Negotiation “down” from an IKEv2 to IKEv1 exchange.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.
FC_SSH_EXT.1	Protocol failures Establishment/Termination of an SSH session	Reason for failure Non-TOE endpoint of connection (IP address) for both successes and failures.
FCS_RBG_EXT.1	Failure of the randomization process.	None.
FCS_TLS_EXT.1	Protocol failures. Establishment/Termination of a TLS session.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.
FDP_RIP.2	None.	
FIA_AFL.1	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_PMG_EXT.1	None.	
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Provided user identity, origin of the attempt (e.g., IP address).
FIA_UAU_EXT.5	All use of the authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.6	Attempts to re-authenticate.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	
FIA_8021X_EXT.1	Attempts to access to the 802.1X controlled port.	Provided client identity (IP address).
FIA_PSK_EXT.1	None.	
FIA_X509_EXT.1	Attempts to load certificates. Attempts to revoke certificates.	None.
FMT_MOF.1	None.	
FMT_MTD.1(1)	None.	
FMT_MTD.1(2)	None.	
FMT_MTD.1(3)	None.	
FMT_SMF.1	None.	
FMT_SMR.1	None.	
FPT_ITT.1	None.	
FPT_FLS.1	Failure of the TSF.	Indication that the TSF has failed with the type of failure that occurred.
FPT_RPL.1	Detected replay attacks.	Identity of the user that was the subject



Requirement	Auditable Events	Additional Audit Record Contents
		of the replay attack. Identity (e.g., source IP address) of the source of the replay attack.
FPT_STM.1	None.	
FPT_TST_EXT.1	Execution of this set of TSF self-tests.	For integrity violations, the TSF code file that caused the integrity violation.
FPT_TUD_EXT.1	Detected integrity violations.	No additional information.
FRU_RSA.1	Maximum quota being exceeded.	Resource identifier.
FTA_SSL_EXT.1	Locking of an interactive session by the session locking mechanism. Any attempts at unlocking of an interactive session.	None.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.
FTA_SSL.4	Terminating a session by quitting or logging off.	None.
FTA_TAB.1	None.	
FTA_TSE.1	Denial of a session establishment due to the session establishment mechanism.	Reason for denial, origin of establishment attempt.
FTP_ITC.1	All attempts to establish a trusted channel. Detection of modification of channel data.	Identification of the initiator and target of channel.
FTP_TRP.1	All attempts to establish a remote administrative session. Detection of modification of session data.	Identification of the initiating IT entity (e.g., IP address).

### 5.3.1.2 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.

#### 5.3.1.1 FAU\_SEL.1 Selective Audit

FAU\_SEL.1.1 The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes:

- a) event type;
- b) success of auditable security events;
- c) failure of auditable security events; and
- d) *[no other attributes]*.

**Application Note:** The above SFR applies NIAP Technical Decision TD0010

### 5.3.1.2 FAU\_STG.1 Protected Audit Trail Storage (Local Storage)

**FAU\_STG.1.1 Refinement:** The TSF shall protect [2 *megabytes*] locally stored audit records in the audit trail from unauthorized deletion.

**FAU\_STG.1.2** The TSF shall be able to *prevent* unauthorized modifications to the stored audit records in the audit trail.

### 5.3.1.3 FAU\_STG\_EXT.1 External Audit Trail 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 implementing the [TLS] protocol.

### 5.3.1.4 FAU\_STG\_EXT.3 Action in Case of Loss of Audit Server Connectivity

**FAU\_STG\_EXT.3.1** The TSF shall [*be able to write message to the local audit store*] if the link to the external IT entity collecting the audit data generated by the TOE is not available.

## 5.3.2 Cryptographic Support (FCS)

### 5.3.2.1 FCS\_CKM.1(1) Cryptographic Key Generation (Symmetric Keys for WPA2 Connections)

**FCS\_CKM.1.1(1) Refinement:** The TSF shall **derive symmetric** cryptographic keys in accordance with a specified cryptographic key **derivation** algorithm [PRF-384] with specified cryptographic key size [128 bits] **using a Random Bit Generator as specified in FCS\_RBG\_EXT.1 and** that meet the following: [802.11-2007].

### 5.3.2.2 FCS\_CKM.1(2) Cryptographic Key Generation (Asymmetric Keys)

**FCS\_CKM.1.1(2) Refinement:** The TSF shall generate **asymmetric** cryptographic keys **used for key establishment** in accordance with [

- NIST Special Publication 800-56B, “Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography” for RSA-based key establishment schemes]

and specified cryptographic key sizes equivalent to, or greater than, a symmetric key strength of 112 bits.

### 5.3.2.3 FCS\_CKM.2(1) Cryptographic Key Distribution (PMK)

**FCS\_CKM.2.1(1) Refinement:** The TSF shall distribute **the 802.11 Pairwise Master Key** in accordance with a specified cryptographic key distribution method: [**receive from 802.1X Authorization Server**] that meets the following: [802.11-2007] **and does not expose the cryptographic keys.**

### 5.3.2.4 FCS\_CKM.2(2) Cryptographic Key Distribution (GTK)

**FCS\_CKM.2.1(2) Refinement:** The TSF shall distribute **Group Temporal Key** in accordance with a specified cryptographic key distribution method: [AES Key Wrap in an EAPOL-Key frame] that meets the following: [RFC 3394 for AES Key Wrap, 802.11-2007 for the packet format and timing considerations] **and does not expose the cryptographic keys.**

### 5.3.2.1 FCS\_CKM\_EXT.4 Cryptographic Key Zeroization

**FCS\_CKM\_EXT.4.1** The TSF shall zeroize all plaintext secret and private cryptographic keys and CSPs when no longer required.

### 5.3.2.2 FCS\_COP.1(1) Cryptographic Operation (Data Encryption/Decryption)

**FCS\_COP.1.1(1) Refinement:** The TSF shall perform [*encryption and decryption*] in accordance with a specified cryptographic algorithm [*AES operating in [CBC mode]*] and cryptographic key sizes 128-bits, 256-bits, and [**192 bits**] that meets the following:

- **FIPS PUB 197, “Advanced Encryption Standard (AES)”**
- [NIST SP 800-38A]

### 5.3.2.3 FCS\_COP.1(2) Cryptographic Operation (Cryptographic Signature)

**FCS\_COP.1.1(2) Refinement:** The TSF shall perform cryptographic signature services in accordance with a [

RSA Digital Signature Algorithm (rDSA) with a key size (modulus) of 2048 bits or greater that meets the following:

[FIPS PUB 186-3, “Digital Signature Standard”]

### 5.3.2.4 FCS\_COP.1(3) Cryptographic Operation (Cryptographic Hashing)

**FCS\_COP.1.1(3) Refinement:** The TSF shall perform [*cryptographic hashing services*] in accordance with a specified cryptographic algorithm [**SHA-1, SHA-256**] **and message digest sizes [160, 256] bits** that meet the following: FIPS Pub 180-3, “Secure Hash Standard.”

### 5.3.2.5 FCS\_COP.1(4) Cryptographic Operation (Keyed-Hash Message Authentication)

**FCS\_COP.1.1(4) Refinement:** The TSF shall perform **keyed-hash message authentication** in accordance with a specified cryptographic algorithm **HMAC-** [**SHA-1**], key size [**160 bits**] **and message digest size of [160] bits** that meet the following: **FIPS PUB 198-1, “The Keyed-Hash Message Authentication Code”, and FIPS PUB 180-3, “Secure Hash Standard”.**

### 5.3.2.1 FCS\_COP.1(5) Cryptographic Operation (WPA2 Data Encryption/Decryption)

**FCS\_COP.1.1(5) Refinement:** The TSF shall perform **encryption and decryption in accordance with the specified cryptographic algorithm AES CCMP and cryptographic key size of 128 bits** that meet the following: **FIPS PUB 197, NIST SP 800-38C and IEEE 802.11-2007.**

### 5.3.2.2 FCS\_HTTPS\_EXT.1 Explicit: HTTPS

**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 as specified in FCS\_TLS\_EXT.1.

### 5.3.2.3 FCS\_IPSEC\_EXT.1 Explicit: IPSEC

**FCS\_IPSEC\_EXT.1.1** The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using the cryptographic algorithms AES-CBC-128, AES-CBC-256 (both specified by RFC 3602), [no other algorithms], and using [IKEv1 as defined in RFCs 2407, 2408, 2409, RFC 4109, and [no other RFCs for hash functions]] for connections to the Authentication Server and [no other servers].

**FCS\_IPSEC\_EXT.1.2** The TSF shall ensure that only ESP confidentiality and integrity security service is used.

**FCS\_IPSEC\_EXT.1.3** The TSF shall ensure that IKEv1 Phase 1 exchanges use only main mode.

**FCS\_IPSEC\_EXT.1.4** The TSF shall ensure that [IKEv1 SA lifetimes are able to be limited by 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs].

**Application Note:** The above SFR applies NIAP Technical Decision TD0021

**FCS\_IPSEC\_EXT.1.5** The TSF shall generate the secret value  $x$  used in the IKE Diffie-Hellman key exchange (" $x$ " in  $g^x \bmod p$ ) using the random bit generator specified in FCS\_RBG\_EXT.1, and having a length of at least [224] bits.

**FCS\_IPSEC\_EXT.1.6** The TSF shall generate nonces used in IKE exchanges in a manner such that the probability that a specific nonce value will be repeated during the life a specific IPsec SA is less than  $1$  in  $2^{[112]}$ .

**FCS\_IPSEC\_EXT.1.7** The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP) and [no other DH groups].

**FCS\_IPSEC\_EXT.1.8** The TSF shall ensure that all IKE protocols implement peer authentication using Pre-shared Keys and [rDSA] that use X.509v3 certificates that conform to RFC 4945.

**FCS\_IPSEC\_EXT.1.9** 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 [IKEv1]

Phase 1] 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 [IKEv1 Phase 2] connection.

#### 5.3.2.4 FCS\_RBG\_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

**FCS\_RBG\_EXT.1.1** The TSF shall perform all random bit generation (RBG) services in accordance with [NIST Special Publication 800-90 using [CTR\_DRBG (AES)]] seeded by an entropy source that accumulates entropy from at least one TSF-hardware-based noise source.

**FCS\_RBG\_EXT.1.2** The deterministic RBG shall be seeded with a minimum of [256 bits] of entropy at least equal to the greatest bit length of the keys and authorization factors that it will generate.

#### 5.3.2.5 FCS\_TLS\_EXT.1 Explicit: TLS

**FCS\_TLS\_EXT.1.1** The TSF shall implement one or more of the following protocols [TLS 1.0 (RFC 2246), TLS 1.1 (RFC 4346)] supporting the following ciphersuites:

Mandatory Ciphersuites:

TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA

TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA

TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA

TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA

Optional Ciphersuites:

[None ].

### 5.3.3 User data protection (FDP)

#### 5.3.3.1 FDP\_RIP.2 Full Residual Information Protection

**FDP\_RIP.2.1** The TSF shall ensure that any previous information content of a resource is made unavailable upon the [allocation of the resource to] all objects.

### 5.3.1 Identification and authentication (FIA)

#### 5.3.1.1 FIA\_AFL.1 Authentication Failure Handling

**FIA\_AFL.1.1 Refinement:** The TSF shall detect when an **Authorized Administrator configurable positive integer of successive** unsuccessful authentication attempts occur related to **administrators attempting to authenticate remotely**.

**FIA\_AFL.1.2** When the defined number of unsuccessful authentication attempts has been **met**, the TSF shall [prevent the offending remote administrator from successfully authenticating until an Authorized Administrator defined time period has elapsed].

### 5.3.1.2 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: [“!”, “@”, “#”, “\$”, “%”, “^”, “&”, “\*”, “(“, and “)”];
2. Minimum password length shall be settable by the Security Administrator, and support passwords of 15 characters or greater;

**Application Note:** The above SFR applies NIAP Technical Decision TD0002

### 5.3.1.3 FIA\_UIA\_EXT.1 User Identification and Authentication

**FIA\_UIA\_EXT.1.1** The TSF shall allow responses to 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;
- [Display a login prompt.]

**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.

### 5.3.1.1 FIA\_UAU\_EXT.5 Password-based Authentication Mechanism

**FIA\_UAU\_EXT.5.1** The TSF shall provide a local password-based authentication mechanism, [RADIUS] to perform administrative user authentication.

**FIA\_UAU\_EXT.5.2** The TSF shall ensure that administrative users with expired passwords are [required to create a new password after correctly entering the expired password].

### 5.3.1.2 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, [and following TSF-initiated locking (FTA\_SSL)].

### 5.3.1.3 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.

### 5.3.1.4 FIA\_8021X\_EXT.1 802.1X 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.

### 5.3.1.5 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 and [no other protocols].

**FIA\_PSK\_EXT.1.2** The TSF shall be able to accept text-based pre-shared keys that:

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

**FIA\_PSK\_EXT.1.3** The TSF shall condition the text-based pre-shared keys by using [AES].

**FIA\_PSK\_EXT.1.4** The TSF shall be able to [accept] bit-based pre-shared keys.

### 5.3.1.6 FIA\_X509\_EXT.1 Extended: X.509 Certificates

**FIA\_X509\_EXT.1.1** The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for IPsec and [TLS] connections.

**FIA\_X509\_EXT.1.2** The TSF shall store and protect certificate(s) from unauthorized deletion and modification.

**FIA\_X509\_EXT.1.3** The TSF shall provide the capability for Authorized Administrators to load X.509v3 certificates into the TOE for use by the security functions specified in this PP.

## 5.3.1 Security management (FMT)

### 5.3.1.1 FMT\_MOF.1 Management of Security Functions Behavior

**FMT\_MOF.1.1 Refinement:** The TSF shall restrict the ability to **enable, disable, determine and modify the behavior of all of the security functions of the TOE identified in this PP to the Authorized Administrator.**

### 5.3.1.2 FMT\_MTD.1(1) Management of TSF Data (for general TSF data)

**FMT\_MTD.1.1** The TSF shall restrict the ability to *manage* the *TSF data* to the *Authorized Administrators*.

### 5.3.1.3 FMT\_MTD.1(2) Management of TSF Data (Reading of Authentication Data)

**FMT\_MTD.1.1(2) Refinement:** The TSF shall **prevent reading** of the **password-based authentication data**.

### 5.3.1.4 FMT\_MTD.1(3) Management of TSF Data (for reading of all symmetric keys)

**FMT\_MTD.1.1(3) Refinement:** The TSF shall **prevent** *reading of all pre-shared keys, symmetric key, and private keys*.

### 5.3.1.5 FMT\_SMF.1 Specification of Management Functions

**FMT\_SMF.1.1** The TSF shall be capable of performing the following management functions:

- *Ability to configure the list of TOE services available before an entity is identified and authenticated, as specified in FIA\_UIA.1, respectively.*
- *Ability to configure the cryptographic functionality.*
- *Ability to update the TOE, and to verify the updates using the digital signature capability (FCS\_COP.1(2)) and [no other functions].*
- *Ability to configure the TOE advisory notice and consent warning message regarding unauthorized use of the TOE.*
- *Ability to configure all security management functions identified in other sections of the PP.*

### 5.3.1.6 FMT\_SMR.1 Security Management Roles

**FMT\_SMR.1.1** The TSF shall maintain the roles:

- Authorized Administrator;
- [No other roles]

**FMT\_SMR.1.2** The TSF shall be able to associate users with roles.

**FMT\_SMR.1.3** The TSF shall ensure that the conditions

- Authorized Administrator role shall be able to administer the TOE locally;
- Authorized Administrator role shall be able to administer the TOE remotely;
- The ability to remotely administer the TOE remotely from a wireless client shall be disabled by default;



are satisfied.

## 5.3.2 Protection of the TSF (FPT)

### 5.3.2.1 FPT\_FLS.1 Fail Secure

**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.**

### 5.3.2.1 FPT\_ITT.1 Basic Internal TSF Data Transfer Protection

**FPT\_ITT.1.1 Refinement:** The TSF shall protect TSF data from *disclosure and protect it from modification* when it is transmitted between separate parts of the TOE **through the use [TLS]**.

### 5.3.2.1 FPT\_RPL.1 Replay Detection

**FPT\_RPL.1.1** The TSF shall detect replay for the following entities: [*network packets terminated at the TOE*].

**FPT\_RPL.1.2** The TSF shall perform: [*reject the data*] when replay is detected.

### 5.3.2.2 FPT\_STM.1 Reliable time stamps

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

### 5.3.2.1 FPT\_TST\_EXT.1: Extended: TSF Testing

**FPT\_TST\_EXT.1.1** The TSF shall run a suite of self tests during initial start-up (on power on) to demonstrate the correct operation of the TSF.

### 5.3.2.2 FPT\_TUD\_EXT.1 Extended: Trusted Update

**FPT\_TUD\_EXT.1.1** The TSF shall provide authorized administrators the ability to query the current version of the TOE firmware/software.

**FPT\_TUD\_EXT.1.2** The TSF shall provide authorized administrators the ability to initiate updates to TOE firmware/software.

**FPT\_TUD\_EXT.1.3** The TSF shall provide a means to verify firmware/software updates to the TOE using a digital signature mechanism and [no other functions] prior to installing those updates.

### 5.3.3 Resource Allocation (FRU)

#### 5.3.3.1 FRU\_RSA.1 Maximum Quotas

**FRU\_RSA.1.1** The TSF shall enforce maximum quotas of the following resources: [*TLS/HTTPS services supporting administrative GUI to Controllers, [no other resources]*] that [individual user, subjects] can use [simultaneously].

### 5.3.4 TOE Access (FTA)

#### 5.3.4.1 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 Authorized Administrator specified time period of inactivity.

#### 5.3.4.2 FTA\_SSL.3 TSF-initiated Termination

**FTA\_SSL.3.1 Refinement:** The TSF shall terminate a **remote** interactive session after an **Authorized Administrator-configurable time interval of session inactivity**.

#### 5.3.4.3 FTA\_SSL.4 User-initiated Termination

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

#### 5.3.4.4 FTA\_TAB.1 Default TOE Access Banners

**FTA\_TAB.1.1 Refinement:** Before establishing an **administrative user** session the TSF shall be capable of displaying an **Authorized Administrator-specified advisory notice and consent** warning message regarding unauthorized use of the TOE.

#### 5.3.4.1 FTA\_TSE.1 TOE Session Establishment

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

### 5.3.1 Trusted Path/Channels (FTP)

#### 5.3.1.1 FTP\_ITC.1 Inter-TSF trusted channel

**FTP\_ITC.1.1 Refinement:** The TSF shall use **802.11-2007, IPsec, and [TLS]** to provide a **trusted** communication channel between itself and **all authorized IT entities** 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 [*connections with RADIUS servers (from WLC over IPsec) and syslog servers (from WLC over TLS)*].

### 5.3.1.1 FTP\_TRP.1 Trusted Path

**FTP\_TRP.1.1 Refinement:** The TSF shall use [**TLS/HTTPS**] to provide a **trusted** communication path between itself and **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 detection of modification of the communicated data.*

**FTP\_TRP.1.2 Refinement:** The TSF shall permit **remote administrators** to initiate communication via the trusted path.

**FTP\_TRP.1.3** The TSF shall require the use of the trusted path for *initial administrator authentication and all remote administration actions.*

## 5.4 TOE SFR Dependencies Rationale for SFRs Found in the WLANPP

The WLAN PP v1.0 contains all the requirements claimed in this Security Target. As such the dependencies are not applicable since the PP itself has been approved.

## 5.5 Security Assurance Requirements

### 5.5.1 SAR Requirements

The TOE assurance requirements for this ST are taken directly from the WLANPP which are derived from Common Criteria Version 3.1, Revision 3. The assurance requirements are summarized in the table below.

**Table 17: Assurance Measures**

Assurance Class	Components	Components Description
DEVELOPMENT	ADV_FSP.1	Basic Functional Specification
GUIDANCE DOCUMENTS	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative User guidance
LIFE CYCLE SUPPORT	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM coverage
TESTS	ATE_IND.1	Independent testing - conformance
VULNERABILITY ASSESSMENT	AVA_VAN.1	Vulnerability analysis

### 5.5.2 Security Assurance Requirements Rationale

This Security Target claims conformance to the WLANPP version 1.0.

## 5.6 Assurance Measures

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

**Table 18 Assurance Measures**

Component	How requirement will be met
ADV_FSP.1	The functional specification describes the external interfaces of the TOE; such as the means for a user to invoke a service and the corresponding response of those services. The description includes the interface(s) that enforces a security functional requirement, the interface(s) that supports the enforcement of a security functional requirement, and the interface(s) that does not enforce any security functional requirements. The interfaces are described in terms of their purpose (general goal of the interface), method of use (how the interface is to be used), parameters (explicit inputs to and outputs from an interface that control the behavior of that interface), parameter descriptions (tells what the parameter is in some meaningful way), and error messages (identifies the condition that generated it, what the message is, and the meaning of any error codes). The development evidence also contains a tracing of the interfaces to the SFRs described in this ST.
AGD_OPE.1	The Administrative Guide provides the descriptions of the processes and procedures of how the administrative users of the TOE can securely administer the TOE using the interfaces that provide the features and functions detailed in the guidance.
AGD_PRE.1	The Installation Guide describes the installation, generation, and startup procedures so that the users of the TOE can put the components of the TOE in the evaluated configuration.
ALC_CMC.1	The Configuration Management (CM) document(s) describes how the consumer (end-user) of the TOE can identify the evaluated TOE (Target of Evaluation). The CM document(s), identifies the configuration items, how those configuration items are uniquely identified, and the adequacy of the procedures that are used to control and track changes that are made to the TOE. This includes details on what changes are tracked, how potential changes are incorporated, and the degree to which automation is used to reduce the scope for error.
ALC_CMS.1	
ATE_IND.1	Cisco will provide the TOE for testing.
AVA_VAN.1	Cisco will provide the TOE for testing.

## 6 TOE SUMMARY SPECIFICATION

### 6.1 TOE Security Functional Requirement Measures

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

**Table 19 How TOE SFRs Measures**

TOE SFRs	How the SFR is Met
FAU_GEN.1	<p>The TOE generates an audit record that is stored internally within the TOE whenever an audited event occurs. The types of events that cause audit records to be generated include, cryptography related events, events related to the enforcement of information flow policies, identification and authentication related events, and administrative events (the specific events and the contents of each audit record are listed in Table 16: Auditable Events. Each of the events is specified in the syslog internal to the TOE 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 writing of timestamps into audit records can be enabled or disabled, and must remain enabled for all security-relevant logging (not required for debugging) in the certified configuration.</p>
FAU_GEN.2	<p>The TOE shall ensure that each auditable event is associated with the user that triggered the event and as a result they are traceable to a specific user. For example a human user, 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.</p>
FAU_SEL.1	<p>The TOE supports pre-selection (enabling and disabling) of audit messages based on event type, and success or failure. Authorized administrators can use facilities (auth-private/authorization/user) along with severity level (success or failure) to filter the set of events.</p> <p><b>Facility</b> A single facility may be configured using auth-private, authorization, or user facilities. Alternatively, multiple facilities may be used by selecting local1, local2, local3, or local4.</p> <p>The following facilities are supported:</p> <ul style="list-style-type: none"> <li>• auth-private = Authorization system (private).</li> <li>• authorization = Authorization system.</li> <li>• user = User process.</li> <li>• local1= Enables user and auth-private facility.</li> <li>• local2=Enables user and authorization facility.</li> <li>• local3=Enables authorization and auth-private facility.</li> <li>• local4=Enables user, authorization and auth-private facility.</li> </ul> <p><b>Severity Level</b> All Successful Audit events will be logged with severity as Informational (severity 6) and all Failure events are logged with severity as Errors/Warnings (severities 3/severity 4).</p> <p>The standard syslog severity levels are:</p> <ul style="list-style-type: none"> <li>• Emergencies = Severity level 0</li> <li>• Alerts = Severity level 1</li> <li>• Critical = Severity level 2</li> </ul>

TOE SFRs	How the SFR is Met
	<ul style="list-style-type: none"> <li>• Errors = Severity level 3</li> <li>• Warnings = Severity level 4</li> <li>• Notifications = Severity level 5</li> <li>• Informational = Severity level 6</li> <li>• Debugging = Severity level 7</li> </ul>
FAU_STG.1	<p>The TOE 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 interactive users (via CLI or GUI) are able to clear the local logging buffer. Controller logs are stored locally on the Controller and are viewable via CLI or GUI on the Controller.</p> <p>The AP system event log may be viewed from the controller CLI. Access points log all system messages (with a severity level less than or equal to notifications, i.e. 0-5) to the access point event log. The event log can contain up to 1024 lines of messages, with up to 128 characters per line. When the event log becomes filled, the oldest message is removed to accommodate a new event message. The event log is saved in a file on the access point flash, which ensures that it is saved through a reboot cycle. To minimize the number of writes to the access point flash, the contents of the event log are written to the event log file during normal reload and crash scenarios only.</p> <p>The Controller audit log is able to store up 2MB of messages with each message of size 256 bytes. When the local logging limit is reached, the oldest messages overwritten to accommodate the new message.</p>
FAU_STG_EXT.1 FAU_STG_EXT.3	<p>The TOE is configured to export audit records to one or more external servers, and protects communications with an external syslog server.</p> <p>Since the syslog connection to the syslog server could fail independently of the IPsec tunnel, the TOE is configured to use TCP syslog instead of the default UDP syslog. TCP is a connection-oriented protocol, which requires a response (acknowledgement) from the syslog server for every packet sent from the TOE, whereas UDP is connectionless, so would not expect a response to the TOE from the syslog server. When a connection to an audit server via TLS fails, or cannot be established, a message about the failure will (if configured) be written to the local logging buffer and/or to the Controller console.</p> <p>The syslog daemon on the Controller maintains a small amount of messages in a queue (a transmission buffer separate from the local logging buffer), and continues to do so if the communication with the syslog server goes down. If the TCP syslog connection fails, the TOE will buffer a small amount of audit records on the TOE when it discovers it can no longer communicate with its configured syslog server, and will transmit the buffer contents when connectivity to the syslog server is restored.</p>
FCS_CKM.1(1) FCS_CKM.1(2)	<p>The TOE implements a Deterministic Random Bit Generator (DRBG) for Diffie-Hellman key establishment (conformant to NIST SP 800-56A), and for RSA key establishment schemes (conformant to NIST SP 800-56B). The TOE does not implement elliptic-curve-based key establishment schemes.</p> <p>The TOE derives GTK and PTK keys for WPA2 connections using a DRBG. See tables 6 and 7 for certificate numbers.</p>
FCS_CKM.2(1) FCS_CKM.2(2) FIA_8021X_EXT.1	<p>The TOE operates as the ‘authenticator’ as part of the 802.1X authentication exchange between wireless clients (the ‘suplicants’) and a RADIUS server, and generates keys for WPA2 connections to secure communications between access points and wireless client once the client has been authenticated. WPA2 uses AES CCMP with 128 bit key size for data encryption/decryption in accordance with FIPS PUB 197, NIST SP 800-38C, and IEEE 802.11-2007.</p> <p>The use of 802.1X results in three communication paths used during the authentication</p>

TOE SFRs	How the SFR is Met
	<p>exchange, two with the TOE as an endpoint and one with TOE acting as a transfer point only between the wireless client(s) and RADIUS server(s).</p> <ol style="list-style-type: none"> <li>1. The TOE establishes an EAP over LAN (EAPOL) connection with the wireless client as specified in 802.1X-2007.</li> <li>2. The TOE establishes a RADIUS protocol connection (tunneled in IPsec) with the RADIUS server.</li> <li>3. The wireless client and RADIUS server establish an EAP-TLS session (RFC 5216); in this transaction the TOE merely takes the EAP-TLS packets from its EAPOL/RADIUS endpoint and transfers them to the other endpoint.</li> </ol> <p>When the authentication exchange is completed successfully, the TOE obtains a PMK (Pairwise Master Key) from the RADIUS server and derives (as specified in 802.11-2007) the PTK (Pairwise Transient Key) from the PMK using a random value generated by the RBG (as specified in FCS_RBG_EXT.1), and the HMAC-SHA function (as specified in FCS_COP.1(4)).</p> <p>After generating the Group Temporal Key (GTK), the TOE distributes the GTK to authenticated wireless clients for use in sending broadcast and multicast messages to the clients. The TOE transfers the GTK in a format consistent with 802.11-2007 specifies the format for the transfer and secures the key during transit using the AES Key Wrap method specified in RFC 3394.</p> <p>Certification testing performed by the Wi-Fi Alliance demonstrates the Controllers and APs implement the IEEE 802.1X-2010 standard correctly.</p>
FCS_CKM_EXT.4	<p>The TOE destroys keys and Critical Security Parameters (CSPs) in that none of the symmetric keys, pre-shared keys, or private keys are stored in plaintext form. All CSPs are stored in flash (NVRAM) or RAM. CSPs stored in RAM are zeroized at shutdown, and CSPs stored in flash are zeroized as specified in table 20.</p>
FCS_COP.1(1)	<p>The TOE provides symmetric encryption and decryption capabilities using AES in CBC mode (128, 256, and 192 bits) as described in NIST SP 800-38A. AES is implemented in the following protocols: IPsec, TLS/HTTPS, and DTLS. The relevant certificate numbers are listed in tables 6 and 7 of section 1.6.2, Cryptographic Support.</p>
FCS_COP.1(2)	<p>The TOE provides cryptographic signature services using RSA Digital Signature Algorithm with key size of 2048 and greater as specified in FIPS PUB 186-3, "Digital Signature Standard." The relevant certificate numbers are listed in tables 6 and 7 of section 1.6.2, Cryptographic Support.</p>
FCS_COP.1(3)	<p>The TOE provides cryptographic hashing services using SHA-1 and SHA-256 as specified in FIPS Pub 180-3 "Secure Hash Standard." For TLS and IKE (ISAKMP) hashing and verification of software image integrity the TOE provides SHA-1. For DTLS, the administrator can select SHA-1 or SHA-256. The relevant certificate numbers are listed in tables 6 and 7 of section 1.6.2, Cryptographic Support.</p>
FCS_COP.1(4)	<p>The TOE provides HMAC-SHA1 message authentication within IKE (ISAKMP) payloads. The relevant certificate numbers are listed in tables 6 and 7 of section 1.6.2, Cryptographic Support.</p>
FCS_COP.1(5)	<p>The TOE provides AES CCM encryption/decryption between Access Points and wireless clients. The relevant certificate numbers are listed in tables 6 and 7 of section 1.6.2, Cryptographic Support.</p>
FCS_HTTPS_EXT.1 FCS_TLS_EXT.1	<p>The TOE implements TLS/HTTPS for interactive remote administration of the controller using the GUI. HTTPS is implemented conformant to RFC 2818. TLSv1.0 and TLSv1.1 are implemented conformant to RFC 2246 and RFC 4346 respectively. All four mandatory TLS ciphersuites in FCS_TLS_EXT.1 are supported for remote administrative sessions to</p>

TOE SFRs	How the SFR is Met
	the controller from a client's TLS-enabled web browser.
FCS_IPSEC_EXT.1	<p>The TOE (WLAN Controller) implements IPsec to provide authentication and encryption services to prevent unauthorized viewing or modification of data in transit. The TOE 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 using AES-CBC-128 and AES-CBC-256.</p> <p>The TOE will use IPsec to secure connections with AAA server (RADIUS is required for authentication of wireless clients).</p> <p>IPsec Internet Key Exchange (IKEv1, also called ISAKMP), is the negotiation protocol that lets two peers agree on how to build an IPsec Security Association (SA). The IKE protocols implement Peer Authentication using the rDSA algorithm. IKE separates negotiation into two phases: phase 1 and phase 2. Phase 1 creates the first tunnel, which protects later ISAKMP negotiation messages. Phase 1 establishes the secure channel using Diffie-Hellman (DH) key exchange in which the TOE generates the 'secret value' ("x" in "<math>g^x \text{ mod } p</math>") using a random bit generator (RBG) to ensure the length of "x" is at least 224 bits, and uses output from the RBG to generate nonces of 160 bits for IKEv1. The key negotiated in phase 1 enables IKE peers to communicate securely in phase 2. During Phase 2 IKE establishes the IPsec SA. IKE maintains a trusted channel, referred to as a Security Association (SA), between IPsec peers that is also used to manage IPsec connections, including:</p> <ul style="list-style-type: none"> <li>• The negotiation of mutually acceptable IPsec options between peers (including peer authentication parameters, either signature based or pre-shared key based);</li> <li>• The establishment of additional Security Associations to protect packets flows using Encapsulating Security Payload (ESP); and</li> <li>• The agreement of secure bulk data encryption AES keys for use with ESP.</li> </ul> <p>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.</p> <p>The TOE will be configured to not support aggressive mode for IKEv1 exchanges and to only use main mode.</p> <p>The TOE will be configured to not allow "confidentiality only" ESP mode by ensuring the IKE Policies configured include ESP-encryption.</p> <p>The TOE supports configuration lifetimes of both Phase 1 SAs and Phase 2 SAs.</p> <p>The TOE supports Diffie-Hellman Group 14 (2048-bit keys).</p> <p>Peer authentication uses rDSA (RSA), and can be configured to use pre-shared keys.</p> <p>For rDSA (RSA), the TOE validates the ID Payload provided by the peer, and supports Cert Matching for the following ID Types: IP*_ADDR, FQDN, USER_FQDN, and DN as defined in RFC 4945. 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. If the ID Payload provided by the peer contains an ID Type other than the four mentioned above, the TOE will not use the ID Type for Cert Matching. In this case the TOE will reference its own admin-defined settings to match the peer's IP address to the corresponding trusted CA, and ensure the peer's certificate was signed by that CA. When the TOE transmits its ID Payload it populates the ID payload with SAN (if the SAN is present in the TOE's certificate), or the DN to identify itself to the peer.</p> <p>Pre-shared keys can include a combination of upper and lower case letters, numbers, and special characters and can be 22 characters or longer. Pre-shared keys are generated and</p>



TOE SFRs	How the SFR is Met
	<p>applied to the TOE by the TOE administrator in coordination with the administrator of the remote IPsec endpoint (e.g. RADIUS server).</p> <p>The TOE will enforce administrative configuration of IPsec tunnel parameters to ensure the IPsec SA (Phase 2 SA) is always less than or equal to the size of the IKE SA (Phase 1 SA). The TOE supports AES key sizes of 128 and 256 for both the IKE SA and the IPsec SA and the key sizes for each tunnel can be specified by the administrator such that they are enforced by default whenever tunnels are initiated.</p>
FCS_RBG_EXT.1	<p>The TOE implements a NIST-approved AES-CTR Deterministic Random Bit Generator (DRBG), as specified in SP 800-90.</p> <p>Note: The details that are proprietary will be provided in a separate entropy document.</p>
FDP_RIP.2	<p>The TOE ensures that packets transmitted from the TOE do not contain residual information from previously transmitted packets. Packets that would be less than the required minimum length for the transmission user are padded with zeros. This applies to both data plane traffic and administrative session traffic.</p>
FIA_AFL.1	<p>The WLC provides the authorized administrator the ability to specify the maximum number of unsuccessful authentication attempts through remote administrative interface (not applicable to local console connection), before an offending account will be locked out for an administratively defined time period. When an account attempting to log into an administrative interface reaches the administratively set maximum number of failed authentication attempts, the account will not be granted access to the administrative functionality of the TOE until the time period has elapsed.</p> <p>The ability for the TOE to enforce this requirement is only applicable when accounts are being authenticated to the local user database. When a AAA server is being used to authenticate administrators, the ability to lock accounts after successive failed login attempts is the responsibility of the AAA server, and locked accounts can only be unlocked by an authorized AAA server administrator.</p>
FIA_PMG_EXT.1	<p>The TOE 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: “!”, “@”, “#”, “\$”, “%”, “^”, “&amp;”, “*”, “(”, and “)”). Minimum password length is settable by the Authorized Administrator, and can be configured for minimum password lengths of 15 characters and maximum of 24 characters.</p>
FIA_UIA_EXT.1	<p>The TOE requires all users to be successfully identified and authenticated before allowing any TSF mediated actions to be performed. The requirement applies to users of the Controllers who connect locally to the CLI via serial console or remotely to the GUI over TLS.</p> <p>Administrative access to the TOE is facilitated through administrative interfaces on the Controller through which the TOE mediates all administrative actions. Once a potential (unauthenticated) administrative user attempts to access the TOE through an interactive administrative interface (CLI or GUI), the TOE prompts the user for a user name and password. Only after the authentication credentials are verified will access to the TOE administrative functionality be granted, so no access is allowed to the administrative functionality of the TOE until an administrator is successfully identified and authenticated. Prior to authentication at interactive administrative interfaces (CLI and GUI), the TOE displays a customizable login banner, which can contain an advisory notice and consent warning message regarding unauthorized use of the TOE.</p>
FIA_UAU_EXT.5	<p>The TOE provides a local password based authentication mechanism as well as RADIUS authentication. Local password and RADIUS authentication can be configured for use to authenticate administrative accounts on the WLAN Controller. In their CC-certified configurations the APs do not support any administrative interfaces. The TOE can be</p>

TOE SFRs	How the SFR is Met
	<p>configured to try one or more remote authentication servers, and to fail back (revert) to the local user database if the remote authentication servers are inaccessible.</p> <p>The process for authentication is the same for administrative access whether administration is occurring via a directly connected console cable or remotely via TLS/HTTPS. 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. In cases of login failure, the TOE does not provide to the un-authenticated user a reason for failure.</p>
FIA_UAU.6	<p>When an authorized administrator changes their own password, the TOE requires the administrator to re-enter the old/current password prior to changing the password.</p>
FIA_UAU.7	<p>When an administrator enters their password at the CLI or GUI, each administrative interface displays only ‘*’ (asterisk) characters so that the password is obscured, or the TOE provides no feedback in the password field, and the TOE does not echo any characters back to remote clients as the characters are entered.</p>
FIA_PSK_EXT.1	<p>The TOE supports use of IKEv1 (ISAKMP) pre-shared keys for authentication of IPsec tunnels between the WLC and RADIUS server. Pre-shared keys can be entered as ASCII characters (from 1-128 characters long) and are conditioned by the TOE (using AES) to a bit-based string used by IKE. Pre-shared keys can also be entered as HEX (“bit-based”) values.</p>
FIA_X509_EXT.1	<p>The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for IPsec, TLS, and Data TLS connections. The local certificate repositories on Controllers can only be overwritten with new and replacement certificates by authorized administrators using the administrative interfaces on Controllers. Authorized administrators, when logged into the controller CLI or GUI can initiate the downloading of certificates to a controller from a remote server over TFTP or FTP.</p> <p>Certificates used for authentication of DTLS connections between Controllers and APs are pre-installed when the devices are manufactured, and cannot be modified. These burned-in certificates are a chain of three certificates: public certificate of the Cisco root CA and intermediate CA, and unique device-specific certificates.</p>
FMT_MOF.1 FMT_SMF.1	<p>The TOE provides all the capabilities necessary to securely manage the TOE, though some accounts may not have abilities to perform all functions. For example accounts may be configured as Read-Only instead of Read-Write and therefore would only have ability to “determine” behavior of security functions but would not have the ability to enable, disable or modify behavior.</p> <p>The ability to access administrative interfaces from wireless clients, “Management Via Wireless” is disabled by default and must remain disabled in the CC-certified configuration. Authorized administrators can connect to the TOE (from wired networks) to perform management functions via a directly connected console cable or remotely over TLS/HTTPS and can perform specific management capabilities including, but not limited to:</p> <ul style="list-style-type: none"> <li>• Local and remote administration of the TOE and the services provided by the TOE;</li> <li>• Initiate updates of the TOE software, including certificate-based image integrity verification;</li> <li>• Configure the cryptographic functionality;</li> <li>• Configure an advisory notice and consent warning message to be displayed at login prior to gaining access to administrative functions.</li> <li>• Configure audit generation functions described earlier in this table for</li> </ul>

TOE SFRs	How the SFR is Met
	<p>FAU_SEL.1(1).</p> <ul style="list-style-type: none"> <li>• Enable or disable logging to the local audit log, or to the local console, or to remote syslog servers, and to display the configuration and status of audit functions.</li> <li>• Configure (enable/disable/define/re-define) authentication servers used by the Controller.</li> <li>• Define the length of time that an administrative session can remain inactive before the session is terminated, and can configure serial console and TLS with separate timeout limits.</li> </ul>
<p>FMT_MTD.1(1) FMT_MTD.1(2) FMT_MTD.1(3)</p>	<p>Authorized administrators are able to manage all aspects of the TOE including query, modify, delete, clear, settings, or create authentication credentials, and user identification credentials for users defined in the local user authentication database. Administrators can create users, and assign usernames and passwords, and can delete users and change user passwords. Administrative accounts with access to the interactive interfaces of the TOE are able to modify their own passwords.</p> <p>Though some authorized administrators will have ‘full’ access to the TOE, even those fully-privileged accounts would not have ability to read any plain-text version of password-based authentication data, pre-shared keys, symmetric keys, or private keys. Passwords for administrative accounts can be stored as hash values in the configuration files of each TOE component. The actual hashing process occurs when the current configuration is written or when a password is set or changed. Password hashing is applied to all passwords. Once passwords are stored in their hashed form in the configuration file, they can no longer be viewed in plaintext on the TOE.</p> <p>Pre-shared and symmetric keys can be set by authorized administrators but are not viewable in plaintext form via any normal administrative interface. Private keys can be generated and re-generated on the Controller by authorized administrators, but private keys are not viewable through any administrative interface.</p> <p>The Controller administrator is able to query, modify, and clear (disable), create (enable) the audit data that will be stored locally (buffer), displayed at the local console, or transmitted to syslog server(s) by enabling or disabling any of those logging facility (buffer, console, syslog), and by setting the event type (syslog severity level) for each facility.</p>
<p>FMT_SMR.1</p>	<p>The term “administrator” is used in the WLAN PP, and thus in this ST, to refer all users capable of authenticating to administrative interfaces of the TOE. The Cisco WLAN Access System contains multiple TOE components that offer administrative interface, and each component would authenticate a separate set of accounts. Each account that’s able to authenticate to one of the administrative interfaces of the WLAN Controller is considered an authorized TOE administrator, though not all components can be administered through all admin interfaces.</p> <p>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.</p>
<p>FPT_FLS.1</p>	<p>Whenever a critical failure occurs within the TOE that results in the TOE ceasing operation, the TOE securely disables its interfaces to prevent the unintentional flow of any information to or from the TOE and reloads. So long as the failures persist, the TOE will continue to reload. This functionally prevents any failure from causing an unauthorized</p>

TOE SFRs	How the SFR is Met
	information flow. There are no failures that circumvent this protection.
FPT_ITT.1	<p>The TOE includes two distinct types of components, Controllers and APs that use a secure network protocol for communication.</p> <p>When TSF data is transferred among APs, between APs and controllers, and among controllers, the data is protected from modification and disclosure using CAPWAP (Control And Provisioning of Wireless Access Points, RFC 5415) over Data TLS (RFC 4347 based on TLS1.1, RFC 4346). The TOE implementation of Data TLS supports the same encryption (AES-256) and hashing (SHA-256) options as the WLANPP requires for TLS, and ensures that Data TLS connections will only use ciphersuites consistent with the 'mandatory' list of ciphersuites defined by the WLANPP for FCS_TLS_EXT.1. Controllers and APs mutually authenticate each other using X.509 certificates.</p>
FPT_RPL.1	The TOE detects and drops replay packets for all secure protocols enabled in the certified configuration (IPsec, TLS, and TLS/HTTPS, as well as Data TLS).
FPT_STM.1	The TOE provides a source of date and time information used in audit event timestamps. 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 obtain updated clock settings from their controller after a reboot, and periodically thereafter. Controllers can optionally be set to receive clock updates from an NTP server.
FPT_TST_EXT.1	<p>The hardware components of the TOE perform TSF tests during initial start-up of the component. These include the cryptographic module testing on each TOE component.</p> <p>The TOE runs a suite of self-tests during initial start-up to verify correct operation of cryptographic modules. If any component reports failure for the POST, the system crashes and appropriate information is displayed on the local console, and saved to a crashinfo file on the local flash drive. All ports are blocked from moving to forwarding state during the POST. If all components of all modules pass the POST, the system is placed in FIPS PASS state and ports are allowed to forward data traffic. If any of the tests fail, a message is displayed to the local console. During the system boot process (power on or reboot), all the Power on Startup Test (POST) components for all the cryptographic modules perform the POST for the corresponding component (hardware or software).</p> <p>These tests are sufficient to verify that the correct version of the TOE software is running as well as that the cryptographic operations are all performing as expected. These tests include:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• HMAC Known Answer Test - 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.</li> <li>• RNG/DRBG Known Answer Test - For this test, known seed values are provided to the DRBG implementation. The DRBG uses these values to generate random</li> </ul>

TOE SFRs	How the SFR is Met
	<p>bits. These random bits are compared to known random bits to ensure that the DRBG is operating correctly.</p> <ul style="list-style-type: none"> <li>• DRBG KAT - 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.</li> <li>• SHA-1/256/512 Known Answer Test – For each of the values listed, the SHA implementation is fed known data and key. These values are used to generate a hash. This hash is compared to a known value to verify they match and the hash operations are operating correctly.</li> <li>• HMAC (HMAC-SHA-1/256/512) KATs - For each of the hash values listed, the HMAC implementation is fed known plaintext data and a known key. These values are used to generate a MAC. This MAC is compared to a known MAC to verify that the HMAC and hash operations are operating correctly.</li> <li>• RSA Signature Known Answer Test (both signature/verification) - This test takes a known plaintext value and Private/Public key pair and used the public key to encrypt the data. This value is compared to a known encrypted value to verify that encrypt operation is working properly. The encrypted data is then decrypted using the private key. This value is compared to the original plaintext value to ensure the decrypt operation is working properly.</li> </ul> <p>The Software Integrity Test is run automatically whenever the system image is loaded and confirms through use of digital signature verification that the image file that's about to be loaded was properly signed and has maintained its integrity since being signed. The system image is digitally signed by Cisco prior to being made available for download from CCO.</p>
FPT_TUD_EXT.1	<p>Authorized administrators can query the software version running on each TOE component, and can initiate updates to (replacements of) software images. Software images are made available via Cisco.com, and administrators can download, verify the integrity of, and install new images.</p> <p>When software updates are initiated on the Controller and APs, the update is loaded as a software image “bundle” to the Controller, and the bundle includes the Controller image (appropriate for the Controller hardware), and the AP images for all AP models supported by the TOE. Controller images bundles, and the AP image files contained therein are digitally signed so their integrity can be verified during the boot process, and an image that fails an integrity check will not be loaded.</p>
FRU_RSA.1	<p>The TOE can be configured to protect system resources used to support interactive administrative interfaces by allowing authorized administrators to set a maximum number of concurrent connections used for TLS/HTTPS (GUI). Administrators have the option to protect these system resources by setting configurable limits for the number of concurrent authenticated sessions permitted at each interface.</p> <ul style="list-style-type: none"> <li>• Limiting the number of concurrent GUI (TLS/HTTPS) connections subjects can use simultaneously to Controllers.</li> </ul>
FTA_SSL_EXT.1 FTA_SSL.3	<p>Authorized administrators can configure maximum inactivity time-out values for local and remote administrative sessions. When the idle time limit has been reached, the session will be terminated by the controller, and any administrator who was using the session will be required to initiate and authenticate a new session.</p>
FTA_SSL.4	<p>Administrators are able to initiate termination (logout) of their own authenticated</p>

TOE SFRs	How the SFR is Met
	interactive sessions (CLI and GUI).
FTA_TAB.1	Authorized administrators define a custom login banner that will be displayed to users of the TOE who connect locally to the serial console or remotely over TLS/HTTPS to the Controller.
FTA_TSE.1	Authorized administrators can configure the TOE to deny establishment of connections from wireless clients based on day, time, and location (e.g. which WLAN network or AP the client is attempting to use).
FTP_ITC.1	<p>Secure communications between the TOE and non-TOE entities (other than remote administrators) include communications:</p> <ul style="list-style-type: none"> <li>• To syslog server over TLS from Controllers.</li> <li>• To a RADIUS servers from Controllers over IPsec (for 802.1X authentication of wireless clients or password-based authentication of TOE administrators).</li> <li>• WPA2 to secure communications between APs and wireless clients.</li> </ul>
FTP_TRP.1	Administrative users can securely communicate remotely to the Controller GUI over TLS/HTTPS.

## 7 ANNEX A: KEY ZEROIZATION

### 7.1 Key Zeroization

The following table describes the key zeroization referenced by FCS\_CKM\_EXT.4 provided by the TOE.

**Table 20: TOE Key Zeroization**

Name	Description	Zeroization
Diffie-Hellman Shared Secret	The shared secret used in Diffie-Hellman (DH) exchange. Created per the Diffie-Hellman Exchange.	Zeroized on Power Cycle or using the following command: > switchconfig key-zeroize controller  Overwritten with: 0x00
Diffie Hellman private key	The private key used in Diffie-Hellman (DH) Exchange	Zeroized on Power Cycle or using the following command: > switchconfig key-zeroize controller  Overwritten with: 0x00
Skey_id	Used for deriving other keys in IKE v1.	Zeroized on Power Cycle or using the following command: > switchconfig key-zeroize controller  Overwritten with: 0x00
IKE session encrypt key	Used for IKE payload protection.	Zeroized on Power Cycle or using the following command: > switchconfig key-zeroize controller  Overwritten with: 0x00
IKE session authentication key	Used for IKEv1/IKEv2 payload integrity verification.	Zeroized on Power Cycle or using the following command: > switchconfig key-zeroize controller  Overwritten with: 0x00
ISAKMP preshared	This shared secret was manually entered for IKE pre-shared key based authentication.	Overwrite with new secret
IPsec encryption key	Used to secure IPsec traffic	Zeroized using the following command: > switchconfig key-zeroize controller Overwritten with: 0x0d
IPsec authentication key	Used to authenticate the IPsec peer.	Zeroized on Power Cycle or using the following command: > switchconfig key-zeroize controller  Overwritten with: 0x00
DTLS Pre-Master Secret	Generated by approved DRBG for Used to derive the DTLS Encryption/Decryption Key and DTLS Integrity	Zeroized on Power Cycle or using the following command:

Name	Description	Zeroization
	Key.	> switchconfig key-zeroize controller  Overwritten with: 0x00
DTLS Master Secret	Derived from DTLS PreMaster Secret. Used to derive the DTLS Encryption/Decryption Key and DTLS Integrity Key.	Zeroized on Power Cycle or using the following command: > switchconfig key-zeroize controller  Overwritten with: 0x00
DTLS Encryption/Decryption Key (CAPWAP session keys)	Session Keys used to encrypt/decrypt CAPWAP control messages.	Zeroized on Power Cycle or using the following command: > switchconfig key-zeroize controller  Overwritten with: 0x00
DTLS Integrity Key	This key is used for integrity checks on CAPWAP control messages.	Zeroized on Power Cycle or using the following command: > switchconfig key-zeroize controller  Overwritten with: 0x00
HTTPS TLS Pre-Master secret	Shared secret created using asymmetric cryptography from which new HTTPS session keys can be created.	Zeroized on Power Cycle or using the following command: > switchconfig key-zeroize controller  Overwritten with: 0x00
HTTPS TLS Encryption Key	AES key used to encrypt TLS data.	Zeroized on Power Cycle or using the following command: > switchconfig key-zeroize controller
HTTPS TLS Integrity Key	HMAC-SHA-1 key used for HTTPS integrity protection	Zeroized on Power Cycle or using the following command: > switchconfig key-zeroize controller
TLS Pre-Master Secret	Shared secret used to generate new TLS session keys for syslog.	Zeroized on Power Cycle or using the following command: > switchconfig key-zeroize controller
TLS Encryption Key	Used for TLS integrity protection of syslog messages.	Zeroized on Power Cycle or using the following command: > switchconfig key-zeroize controller
TLS Integrity Key	Used for TLS integrity protection of syslog messages	Zeroized on Power Cycle or using the following command: > switchconfig key-zeroize controller
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.	Zeroized on Power Cycle or using the following command: > switchconfig key-zeroize controller



Name	Description	Zeroization
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.	Zeroized on Power Cycle or using the following command: > switchconfig key-zeroize controller
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.	Zeroized on Power Cycle or using the following command: > switchconfig key-zeroize controller
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.	Zeroized on Power Cycle or using the following command: > switchconfig key-zeroize controller
RADIUS server shared secret	This is the shared secret between the RADIUS server and Controller.	Overwrite with new secret

## 8 ANNEX B: REFERENCES

The following documentation was used to prepare this ST:

**Table 21: References**

Identifier	Description
[800-38A]	NIST Special Publication 800-38A Recommendation for Block 2001 Edition Recommendation for Block Cipher Modes of Operation Methods and Techniques December 2001
[800-38C]	NIST Special Publication 800-38C Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality
[800-56A]	NIST Special Publication 800-56A, March, 2007 Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised)
[800-56B]	NIST Special Publication 800-56B Recommendation for Pair-Wise, August 2009 Key Establishment Schemes Using Integer Factorization Cryptography
[800-90]	NIST Special Publication 800-90A Recommendation for Random Number Generation Using Deterministic Random Bit Generators January 2012
[CC_PART1]	Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated September 2012, version 3.1, Revision 4, CCMB-2012-09-001
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated September 2012, version 3.1, Revision 4, CCMB-2012-09-002
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated September 2012, version 3.1, Revision 4, CCMB-2012-09-003
[CEM]	Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated September 2012, version 3.1, Revision 4, CCMB-2012-09-004
[FIPS 140-2]	FIPS PUB 140-2 Federal Information Processing Standards Publication Security Requirements for Cryptographic Modules May 25, 2001
[FIPS PUB 180-3]	FIPS PUB 180-3 Federal Information Processing Standards Publication Secure Hash Standard (SHS) October 2008
[FIPS PUB 186-2]	FIPS PUB 186-2 Federal Information Processing Standards Publication 2000 January 27
[FIPS PUB 186-3]	FIPS PUB 186-3 Federal Information Processing Standards Publication Digital Signature Standard (DSS) June, 2009
[FIPS PUB 198-1]	Federal Information Processing Standards Publication The Keyed-Hash Message Authentication Code (HMAC) July 2008
[IEEE 802.11-2007]	802.11-2007 - 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
[WLANPP]	Protection Profile for Wireless Local Area Network (WLAN) Access Systems, version 1.0, December, 2011