Cisco Converged Access

Common Criteria Security Target

Version 1.2

November 6, 2015

Americas Headquarters:

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

Table of Contents

List of Tables

List of Figures

List of Acronyms

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

Table 1 Acronyms

Acronyms / Abbreviations	Definition
AAA	Administration, Authorization, and Accounting
ACL	Access Control Lists
AES	Advanced Encryption Standard
CA	Certificate Authority
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
Cisco CA	Cisco Converged Access
CM	Configuration Management
CSU	Channel Service Unit
DHCP	Dynamic Host Configuration Protocol
DSU	Data Service Unit
DTLS	Datagram Transport Layer Security
EAL	Evaluation Assurance Level
ESP	Encapsulating Security Payload
GE	Gigabit Ethernet port
HTTP	Hyper-Text Transport Protocol
HTTPS	Hyper-Text Transport Protocol Secure
ICMP	Internet Control Message Protocol
IT	Information Technology
LAN	Local Area Network
NCS	Cisco Prime Network Control System
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
SHS	Secure Hash Standard
SIP	Session Initiation Protocol
SPD	Security Policy Database
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
WCS	Cisco Wireless Control System
WLAN	Wireless LAN
WLANPP	WLAN Protection Profile

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 Cisco Converged Access (Cisco CA) Wireless LAN Controllers and Wireless Access Points. 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. The Common Criteria Functional Specification is met through the description of management interfaces in the Security Target and the parameters described within the Common Criteria Guidance Documentation as well as the Cisco Documentation for Cisco CA.

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 2 ST and TOE Identification

Name	Description
ST Title	Cisco Converged Access
ST Version	1.2
Publication Date	November 6, 2015
Vendor and ST Author	Cisco Systems, Inc.
TOE Reference	Cisco Converged Access
TOE Hardware Models	Cisco Catalyst 3650, 3850, and WLC 5760 with APs 1532e/i, 1572eac/ic/ec, 1600i/e, 1700i, 2600i/e, 2700i/e, 3500i/e, 3600i/e with 3000M add-on module, 3700i/e/p, and 1552e
TOE Software Version	IOS XE 3.6.3E
Keywords	WLAN, Wireless, Controller, Switch, Data Protection, Authentication

1.2 TOE Overview

The Cisco Converged Access TOE combines a purpose-built switching and WLAN controller platforms with wireless access points to create a WLAN Access System. The WLAN Access System provides secure wireless access to a wired network by controlling the link between the wireless client and that wired network. The Cisco CA TOE includes the WLAN Controller and Wireless Access Point hardware models as defined in Table 2 in section 1.1 and the IOS XE and IOS software.

1.2.1 TOE Product Type

The Cisco CA controllers are switch platforms that provide connectivity and security services across multiple interconnected devices each operating in a fully-managed, secure state where each controller can manage multiple Access Points, and each AP can support multiple concurrent connections from wireless clients. The Cisco CA solution includes a combination of one or more

controllers, with one or more wireless access points, and provides authentication services, encrypted communications, audit message generation, routing, switching, and bridging among connected wired and wireless networks.

1.2.2 Supported non-TOE Hardware/ Software/ Firmware

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

Table 3 IT Environment Components

Component	Required	Usage/Purpose Description for TOE performance
Management Workstation	Yes	This includes any IT Environment management workstation with an SSH client to support TOE administration.
AAA Server	Yes	This includes any IT environment RADIUS server that provides authentication services for wireless clients and optionally for TOE administrators, and optionally TACACS+ server for authentication of TOE administrators.
Syslog Server	Yes	This includes any syslog server to which the TOE would transmit syslog messages over IPsec.
Cisco Prime™ Infrastructure	No	Provides a centralized management server platform for remote administration (using SNMPv3 over IPsec) of multiple WLAN Controllers.
Cisco Mobility Services Engine (MSE)	No	Provides advanced spectrum analysis, and Cisco Adaptive Wireless Intrusion Prevention System (wIPS) to detect, track, and trace rogue devices, interferers, Wi-Fi clients, and RFID tags as well as to identify over-the-air threats, with location and mitigation capabilities.
Certificate Authority	No	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.
Cisco Prime Network Control System (NCS)	No	The Cisco Prime Network Control System (NCS) provides converged user and access management for wired and wireless networks with visibility into endpoint connectivity—regardless of device, network, or location, and endpoint identity policy monitoring through integration with Cisco Identity Services Engine (ISE).
Cisco Wireless Control System (WCS),	No	The Cisco Wireless Control System (WCS) is a software product that provides a centralized management service for Cisco WLAN products including the APs, Controllers and MSEs. WCS also provides centralized management for the Wireless Intrusion Prevention (wIPS), forwarding wIPS profiles to the MSE for further distribution. The WCS component is required to maintain a WCS administrator role whose purpose is to configure wIPS and monitor and review wIPS records.
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

This section provides an overview of the Cisco Converged Access Target of Evaluation (TOE). The TOE is comprised of both software and hardware. The hardware is comprised of the following: Cisco Catalyst 3650, 3850, and WLC 5760 with APs 1532e/i, 1572eac/ic/ec, 1600i/e, 1700i, 2600i/e, 2700i/e, 3500i/e, 3600i/e with 3000M add-on module, 3700i/e/p, and 1552e. The software is comprised of the Universal Cisco Internet Operating System (IOS) XE software

release IOS XE 3.6.3E installed on the controller(s), which includes AP images of IOS 15.3(3)JN3 that gets installed to APs as they join a controller.

The Cisco Converged Access 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.

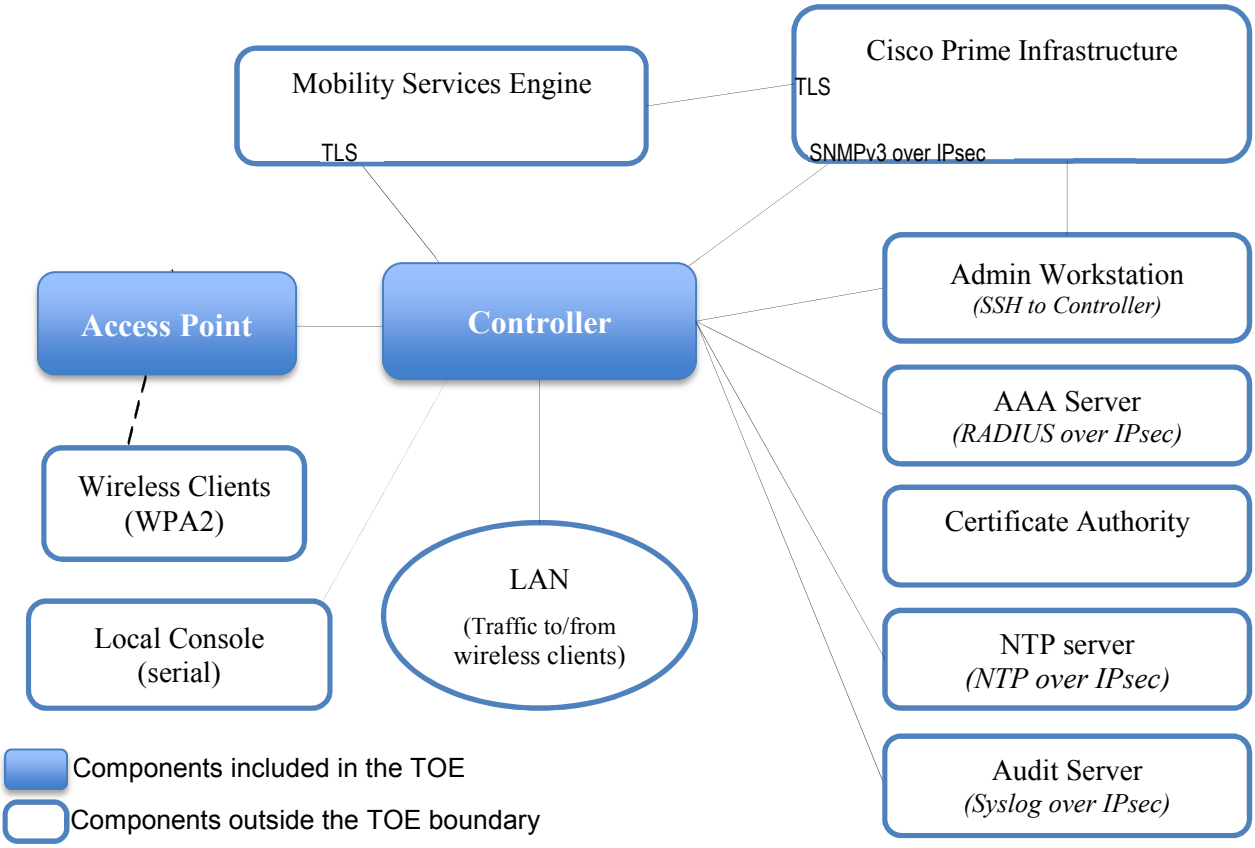
Core hardware features of the Cisco CA controllers and APs include:

- 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 Cisco IOS or IOS XE 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 router 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.

Cisco IOS XE and IOS are Cisco-developed highly configurable proprietary operating systems that provide for efficient and effective routing and switching. Although IOS XE and IOS perform many networking functions, this TOE only addresses the functions that provide for the security of the TOE itself as described in Section 1.7 Logical Scope of the TOE below, which, for example, does not include routing and switching functionality.

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

Figure 1: Sample TOE Deployment



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 specified in section 1.5 below and includes the Cisco IOS XE software running on the controllers, and IOS software running on the access points. The image "bundle" installed to controllers includes the controller's IOS XE software image and 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 interactively using a local console connection (CLI), or remotely over SSH (CLI). 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 WLAN controller and Access Point models as follows: Cisco Catalyst 3650, 3850, and WLC 5760 with APs 1532/e/i, 1572eac/ic/ec, 1600i/e, 1700i, 2600i/e, 2700i/e, 3500i/e, 3600i/e with 3000M add-on module, 3700i/e/p, and 1552e. 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 Converged Access 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 4 below:

Table 4 Hardware Models and Specifications

Hardware Platform	Picture and Part Numbers	Interfaces and Features
Cisco Catalyst 3650		24 or 48 Gigabit Ethernet ports as indicated in the part numbers. Support for up to 25 access points and 1000 wireless clients on each switching entity (switch or stack) All models include: • RJ-45 serial console port. All models support: • Stacking using proprietary cabling. • Uplink modules (1Gbps to 10Gbps). • Redundant power supplies.

Hardware Platform	Picture and Part Numbers	Interfaces and Features
Cisco Catalyst 3850 Customers need to purchase the IP Base software model or the IP Services software model in order to use the Catalyst 3850 Series Switch as a wireless controller.	 With IP Base Software • WS-C3850-24T-S • WS-C3850-48T-S • WS-C3850-24P-S • WS-C3850-48P-S • WS-C3850-24F-S With IP Services Software: • WS-C3850-24T-E • WS-C3850-48T-E • WS-C3850-24P-E • WS-C3850-48P-E • WS-C3850-48F-E	24 or 48 Gigabit Ethernet ports as indicated in the part numbers. Support for up to50 access points and 2000 wireless clients. "T" models do not provide PoE (Power over Ethernet) "P" and "F" models provide PoE. "F" models have larger power supplies to support enabling more PoE ports. All models include: • RJ-45 serial console port. All models support: • Stacking using proprietary cabling. • Uplink modules (1Gbps to 10Gbps). • Redundant power supplies.
Cisco WLAN Controller 5760	 • AIR-CT5760-25-K9 • AIR-CT5760-50-K9 • AIR-CT5760-100-K9 • AIR-CT5760-250-K9 • AIR-CT5760-500-K9 • AIR-CT5760-1k-K9 • AIR-CT5760-HA-K9	6 10 Gigabit Ethernet ports (SFP+). Support for 25 to 1000 access points (limited by licensing) as indicated in the part number, and up to 12,000 wireless clients per controller. Management port: Gigabit Ethernet (RJ45) Console Ports: RS232 and mini-USB (when one is connected, the other is disabled).

Hardware Platform	Picture and Part Numbers	Interfaces and Features
1532e/i 'e' = external antenna 'i' = integrated antenna	 External Antenna: • AIR-CAP1532E- x -K9 • AIR-AP1532E-UXK9 Internal Antenna: • AIR-CAP1532I-x-K9 • AIR-AP1532I-UXK9	10/100/1000BASE-T autosensing (RJ-45) Management console port (RJ-45) 1530e: 2x2 MIMO with 2 spatial streams (2.4 GHz) and 2x2 MIMO with 2 spatial streams (5 GHz) 1530i: 3x3 MIMO with 3 spatial streams (2.4 GHz) and 2x3 MIMO with 2 spatial streams (5 GHz) Data Rates Supported: • 802.11a: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps • 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps 802.11n data rates (2.4 GHz1 and 5 GHz): 6.5 to 300 Mbps

Hardware Platform	Picture and Part Numbers	Interfaces and Features
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	 Cisco Aironet 1552E/1552EU • AIR-CAP1552E-A-K9 • AIR-CAP1552E-*-K9 • AIR-CAP1552EU-A-K9 • AIR-CAP1552EU-*-K9 Cisco Aironet 1552C/1552CU Access Point with DOCSIS 3.0 Cable Modem • AIR-CAP1552C-A-K9 • AIR-CAP1552C-*K9 • AIR-CAP1552CU-A-K9 • AIR-CAP1552CU-*K9 Cisco Aironet 1552H Hazardous Location Access Point • AIR-CAP1552H-A-K9 • AIR-CAP1552H-*-K9 Cisco Aironet 1552I Integrated Antenna Access Point • AIR-CAP1552I-A-K9 • AIR-CAP1552I-*-K9	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): • 2.4 GHz, gain 4.0 dBi, horizontal beamwidth 360° • 5 GHz, gain 4.0 dBi, horizontal beamwidth 360° Data Rates Supported: • 802.11a: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps • 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps • 802.11n data rates (2.4 GHz1 and 5 GHz): 6.5 to 300 Mbps

Hardware Platform	Picture and Part Numbers	Interfaces and Features
1572/eac/ic/ec 'e'= external antenna 'ac'=AC power 'i'=internal antenna 'c'=cable backhaul/power-over-cable	 Cisco Aironet 1572 External Antenna, AC Power • AIR-AP1572EAC-x-K9 Cisco Aironet 1572EC External Antenna,PoC • AIR-AP1572EC1-x-K9 • AIR-AP1572EC2-x-K9 • AIR-AP1572EC3-x-K9 • AIR-AP1572EC4-x-K9 Cisco Aironet 1572 Internal Antenna, PoC • AIR-AP1572IC1-x-K9 • AIR-AP1572IC2-x-K9 • AIR-AP1572IC3-x-K9 • AIR-AP1572IC4-x-K9	10/100/1000BASE-T autosensing (RJ-45) Management console port (RJ-45) Fiber SFP Cisco Aironet 1572 External Antenna, (AC Power or PoC): Four (4) N-type female external antenna connectors that can be configured as a 2.4/5 GHz dual-band port or two (2) 2.4 GHz plus two (2) 5-GHz ports. The antenna options include single or dual-band and omnidirectional or directional. Cisco Aironet 1572 Internal Antenna, PoC: Combines four (4) dual-band, integrated antennas under a common radome. These antennas are omnidirectional with associated gains of 4 dBi and 6 dBi on the 2.4 GHz and 5 GHz bands, respectively.

Hardware Platform	Picture and Part Numbers	Interfaces and Features
1600e and 1600i 'e' = external antenna 'i' = internal antenna	 AIR-CAP1602I-x-K9 (quantity = 1) AIR-CAP1602I-xK910 (qty. 10) AIR-SAP1602I-x-K9 (qty. 1) AIR-SAP1602I-xK9-5 (qty. 5) AIR-CAP1602E-x-K9 (quantity = 1) AIR-CAP1602E-xK910 (qty. 10) AIR-SAP1602E-x-K9 (qty. 1) AIR-SAP1602E-xK9-5 (qty. 5)	10/100/1000BASE-T autosensing (RJ-45) Management console port (RJ-45) Antenna: • 2.4 GHz, gain 4.0 dBi, horizontal beamwidth 360° • 5 GHz, gain 4.0 dBi, horizontal beamwidth 360° Data Rates Supported: • 802.11a: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps • 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps • 802.11n data rates (2.4 GHz[1] and 5 GHz): 6.5 to **300 Mbps**

Hardware Platform	Picture and Part Numbers	Interfaces and Features
Cisco Aironet 1700i Access Point: Indoor environments, with internal antennas	 AIR-CAP1702I-x-K9 (quantity=1) AIR-CAP1702I-xK910 (quantity=10)	10/100/1000BASE-T autosensing (RJ-45) Management console port (RJ-45) Antenna: • 2.4 GHz, gain 4 dBi, internal omni, horizontal beamwidth 360° • 5 GHz, gain 4 dBi, internal omni, horizontal beamwidth 360° Data Rates Supported: • 802.11a: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps • 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps 802.11n data rates (2.4 GHz[1]): 6.5 to 144 Mbps 802.11n data rates (5 GHz): 6.5 to 866 Mbps

Hardware Platform	Picture and Part Numbers	Interfaces and Features
2600e and 2600i 'e' = external antenna 'i' = internal antenna	 AIR-CAP2602I-x-K9 (quantity = 1) AIR-CAP2602I-xK910 (qty. 10) AIR-SAP2602I-x-K9 (qty. 1) AIR-SAP2602I-xK9-5 (qty. 5) AIR-CAP2602E-x-K9 (quantity = 1) AIR-CAP2602E-xK910 (qty. 10) AIR-SAP2602E-x-K9 (qty. 1) AIR-SAP2602E-xK9-5 (qty. 5)	10/100/1000BASE-T autosensing (RJ-45) Management console port (RJ-45) Antenna: • 2.4 GHz, gain 4.0 dBi, horizontal beamwidth 360° • 5 GHz, gain 4.0 dBi, horizontal beamwidth 360° Data Rates Supported: • 802.11a: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps • 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps • 802.11n data rates (2.4 GHz1 and 5 GHz): 6.5 to **450 Mbps**
2700e and 2700i 'e' = external antenna 'i' = internal antenna	 AIR-CAP2702I- x-K9 (quantity = 1) AIR-CAP2702I- xK910 (quantity = 10) AIR-CAP2702E- x-K9 (quantity = 1) AIR-CAP2702E- xK910 (quantity = 10)	Dual-band 2.4 GHz and 5 GHz access points (APs) with 802.11ac Wave 1 support on the integrated 5-GHz radio. Management console port (RJ-45) Antenna: • 2.4 GHz, gain 4.0 dBi, internal omni, horizontal beamwidth 360° • 5 GHz, gain 6.0 dBi, internal omni, horizontal beamwidth 360° Data Rates Supported: • 802.11a: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps • 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps 802.11n data rates (2.4 GHz1 and 5 GHz): 6.5 to **1300 Mbps**

Hardware Platform	Picture and Part Numbers	Interfaces and Features
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: • 2.4 GHz, gain 4.0 dBi, horizontal beamwidth 360° • 5 GHz, gain 4.0 dBi, horizontal beamwidth 360° Data Rates Supported: • 802.11a: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps • 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps • 802.11n data rates (2.4 GHz[1] and 5 GHz): 6.5 to **300 Mbps**
3600e and 3600i 'e' = external antenna 'i' = internal antenna *Optional IEEE 802.11ac Adaptive Radio Module to increase wireless data throughput rates, range, and capacity.* *AIR-RM3000AC-x-K9* *AIR-RM3000MACxK910(qty. 10)* *Optional Cisco AIR-RM3000M Monitor Module helps avoid RF interference to obtain better coverage and performance on the wireless network.* *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: • 2.4 GHz, gain 4.0 dBi, horizontal beamwidth 360° • 5 GHz, gain 4.0 dBi, horizontal beamwidth 360° Data Rates Supported: • 802.11a: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps • 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps • 802.11n data rates (2.4 GHz1 and 5 GHz): 6.5 to **450 Mbps**

Hardware Platform	Picture and Part Numbers	Interfaces and Features
3700e, 3700i and 3700p 'e' = external antenna '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)	Dual-band 2.4 GHz and 5 GHz access points (APs) with 802.11ac Wave 1 support on the integrated 5-GHz radio. 10/100/1000BASE-T autosensing (RJ-45) Management console port (RJ-45) Antenna: • 2.4 GHz, gain 4.0 dBi, horizontal beamwidth 360° • 5 GHz, gain 4.0 dBi, horizontal beamwidth 360° Data Rates Supported: • 802.11a: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps • 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps • 802.11n data rates (2.4 GHz1 and 5 GHz): 6.5 to 450 Mbps 802.11ac module (5 GHz) : 6.5 to 1300 Mbps

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 Converged Access (Cisco CA) provides extensive auditing capabilities. The TOE (the Cisco CA in its certified configuration) can audit security-relevant events (as listed under FAU_GEN.1) related to cryptographic functionality, identification and authentication, and administrative actions. 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 local logging buffer (circular) with a configurable size limit. Audit messages can also be transmitted up over an encrypted channel to an external audit server.

1.6.2 Cryptographic Support

The TOE provides cryptography in support of IPsec connections to tunnel communications with AAA servers, syslog servers, and NTP servers, SSHv2 for secure remote administration via CLI. The TOE can also use the X.509v3 certificates for authenticating sessions, and can act as a certification authority to sign and issue certificates to other devices.

This cryptography implemented by the Cisco Converged Access components has been validated for conformance to the requirements of FIPS 140-2 Level 2. See the table below for certificate number references.

Table 5 FIPS Certificate Number References

	AES Algorithm	HMAC Algorithm	RSA Algorithm	SHS Algorithm	DRBG Algorithm
3650 (CMVP #2341)	#2817, #2685, and #2879	#1764, #1672, and #1815	#1471	#2361, #2256, and #2420	#481, #435
3850 (CMVP #2341)	#2817, #2685, and #2879	#1764, #1672, and #1815	#1471	#2361, #2256, and #2420	#481, #435
5760 (CMVP #2363)	#2817, #2685, and #2879	#1764, #1672, and #1815	#1471	#2361, #2256, and #2420	#481, #435
1532 APs (CMVP#2421)	#2817, #2450	#1764	#1471	#2361	#481
1552 APs (CMVP#2421)	#2235, #2817	#1764	#1471	#2361	#481
1572 APs (CMVP#2421)	#2334, #2901	#1836	#1529	#2441	#534

	AES Algorithm	HMAC Algorithm	RSA Algorithm	SHS Algorithm	DRBG Algorithm
1600 APs (CMVP#2421)	#2846, #2901	#1836	#1529	#2441	#534
1700 APs (CMVP#2421)	#2901, #2334	#1836	#1529	#2441	#534
2600 APs (CMVP#2421)	#2334, #2901	#1836	#1529	#2441	#534
2700 APs (CMVP#2421)	#2334	#1836	#1529	#2441	#534
3500 APs (CMVP#2421)	#2235, #2901	#1764	#1471	#2361	#481
3600 APs (CMVP#2421)	#2334, #2901	#1836	#1529	#2441	#534
3700 APs (CMVP#2421)	#2334, #2901	#1836	#1529	#2441	#534

The cryptographic services provided by the TOE are listed in Table 6.

Table 6 TOE Provided Cryptography

Cryptographic Method	Use within the TOE
Internet Key Exchange	Used to establish initial IPsec session.
Secure Shell Establishment	Used to establish initial SSH session.
RSA Signature Services	Used in IPsec session establishment. Used in SSH session establishment. Used in X.509 certificate signing.
SP 800-90 RBG	Used in IPsec session establishment. Used in SSH session establishment.
SHS	Used to provide IPsec traffic integrity verification Used to provide SSH traffic integrity verification
AES	Used to encrypt IPsec session traffic. Used to encrypt SSH session traffic.

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.

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, or remotely to CLI over SSH. 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 connections the TOE support password-based authentication of administrators against either a local user database or remote RADIUS or TACACS+ server, and administrators connecting via SSH have the option to use SSH key (RSA) authentication.

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.

In addition to authentication of administrators and wireless clients, the TOE also performs device-level authentication of the remote IPsec peers. Device-level authentication allows the TOE to establish a mutually-authenticated secure channel with a trusted peer. The IKE authentication for the IPsec communication channels used to secure AAA, audit, NTP, and SNMPv3 traffic.

1.6.5 Security Management

Through the CLI 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 can have read-write access, or can be assigned to lesser sets of privileges that can be custom-defined. For the Cisco CA TOE, 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.

Thus, “authorized administrator” accounts include accounts defined in IOS XE with the “username” command (regardless of the privilege level assigned to the username).

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 Cisco IOS XE and IOS are not 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. The APs and Controllers will detect and drop (not forward) replayed packets received at network interfaces (including wireless radio interfaces).

Each component (controller and AP) of the TOE 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. If using an external NTP server, NTP communications will be secured at the TOE with IPsec.

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 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 DTLS (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, syslog, and NTP servers are secured using IPsec.

Remote administrators can establish trusted communication paths to controllers using SSHv2 (for CLI access). 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.

1.7 Excluded Functionality

The following functionality is excluded from the evaluation.

Table 7 Excluded Functionality

Excluded Functionality	Exclusion Rationale
Non-FIPS 140-2 mode of operation on the	This mode of operation includes non-FIPS allowed operations.

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 3, dated: July 2009. 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 8 below:

Table 8 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
- TD0020: Update of Requirements for IKE Authentication

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 1.0 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 9 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 10 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.
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.

Threat	Description of Threat
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 11 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 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 12 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.
O.SYSTEM_MONITORING	The TOE will provide the capability to generate audit data and

TOE Objective	Objective Description
	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 13 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 3, dated: July 2009* 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 PP itself, the formatting used in the PP 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 PP.

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 14 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)
	FCS_COP.1(4)	Cryptographic Operation (Keyed-Hash Message

Class Name	Component Identification	Component Name
		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_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 WLANPP

5.3.1 Security audit (FAU)

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 15].

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*information specified in column three of* Table 15].

Table 15 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-Data Integrity.	Cryptographic mode of operation, name/identifier of object being hashed.

Requirement	Auditable Events	Additional Audit Record Contents
FCS_COP.1(5)	Failure of WPA2 encryption of 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_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 of the reply attack. Identity (e.g., source IP address) of the source of the replay attack.
FPT_STM.1	None.	

Requirement	Auditable Events	Additional Audit Record Contents
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.

5.3.1.3 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) administrator identity;

b) event type;

c) success of auditable security events;

d) failure of auditable security events; and

e) [*no other attributes*].

5.3.1.4 FAU_STG.1 Protected Audit Trail Storage (Local Storage)

FAU_STG.1.1 Refinement: The TSF shall protect [***a configurable circular logging buffer size of 4096-2147483647 bytes***] 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.

5.3.1.5 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 [IPsec] protocol.

5.3.1.6 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 logging buffer about the logging host failure, and/or send an SNMP trap*] 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**.

5.3.2.5 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.

5.3.2.6 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]

5.3.2.7 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"]

5.3.2.8 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, SHA-384, SHA-512] and message digest sizes [160, 256, 384, 512] bits** that meet the following: FIPS Pub 180-3, "Secure Hash Standard."

5.3.2.9 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, SHA-256, SHA-384, SHA-512], key size [***160, 256, 384, 512 bits***] **and message digest size of** [160, 256, 384, 512]

bits that meet the following: **FIPS PUB 198-1, "The Keyed-Hash Message Authentication Code", and FIPS PUB 180-3, "Secure Hash Standard".**

5.3.2.10 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.**

5.3.2.11 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.

5.3.2.12 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 [IKEv2 as defined in RFCs 5996 (with mandatory support for NAT traversal as specified in section 2.23), 4307, and [no other RFCs for hash functions]] for connections to the Authentication Server and [Syslog Server, NTP Server, and SNMPv3 management service].

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 [IKEv2 lifetimes can be configured by an administrator based on number of packets or length of time].

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 mod p) using the random bit generator specified in FCS_RBG_EXT.1, and having a length of at least [*320 (for DH Group 14), 256 (for DH Group 24), 256 (for DH Group 19), 384 (for DH Group 20), 424 (for DH Group 15), and 480 (bits for DH Group 16)*] 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^[*128 bits of security for DH Groups 14, 24, and 19; and 192 bits of security for DH Groups 20, 15, and 16*].

FCS_IPSEC_EXT.1.7 The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP) and [24 (2048-bit MODP with 256-bit POS), 19 (256-bit Random ECP), 20 (384-bit Random ECP), 15 (3072 bit MODP), and 16 (4096-bit MODP)].

FCS_IPSEC_EXT.1.8 The TSF shall ensure that all IKE protocols perform peer authentication using [rDSA] that use X.509v3 certificates that conform to RFC 4945 and [no other method].

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 [IKEv2 IKE_SA] connection is greater than or equal to the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [IKEv2 CHILD_SA] connection. `

5.3.2.13 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.

5.3.2.14 FCS_SSH_EXT.1 Explicit: SSH

FCS_SSH_EXT.1.1 The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, and 4254.

FCS_SSH_EXT.1.2 The TSF shall ensure that the SSH connection be rekeyed after no more than 2^28 packets have been transmitted using that key.

FCS_SSH_EXT.1.3 The TSF shall ensure that the SSH protocol implements a timeout period for authentication as defined in RFC 4252 of [*a configurable timeout period of no more than 120 seconds*], and provide a limit to the number of failed authentication attempts a client may perform in a single session to [*a configurable maximum number of attempts of no more than 5*] attempts.

FCS_SSH_EXT.1.4 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, password-based.

FCS_SSH_EXT.1.5 The TSF shall ensure that, as described in RFC 4253, packets greater than [*65,535 bytes*] bytes in an SSH transport connection are dropped.

FCS_SSH_EXT.1.6 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms: AES-CBC-128, AES-CBC-256-CBC, [*no other encryption algorithms*].

FCS_SSH_EXT.1.7 The TSF shall ensure that the SSH transport implementation uses SSH_RSA and [no other public key algorithms] as its public key algorithm(s).

FCS_SSH_EXT.1.8 The TSF shall ensure that the data integrity algorithm used in the SSH transport connection is hmac-sha1 and [hmac-sha1-96, hmac-md5, hmac-md5-96].
FCS_SSH_EXT.1.9 The TSF shall ensure that diffie-hellman-group14-sha1 is the only allowed key exchange method used for the SSH protocol.

5.3.2.15 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 1.2 (RFC 5246)] 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.

5.3.4 Identification and authentication (FIA)

5.3.4.1 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 [*action to unlock the account*] is taken by a local Authorized Administrator].

5.3.4.2 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: [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”,];
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

5.3.4.3 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.

5.3.4.4 FIA_UAU_EXT.5 Password-based Authentication Mechanism

FIA_UAU_EXT.5.1 The TSF shall provide a local password-based authentication mechanism, [RADIUS, and TACACS+] 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].

5.3.4.5 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)].

5.3.4.6 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.

5.3.4.7 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.

.

5.3.4.8 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.

5.3.5 Security management (FMT)

5.3.5.1 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**.

5.3.5.2 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*.

5.3.5.3 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**.

5.3.5.4 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*.

5.3.5.5 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 this PP.*

5.3.5.6 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.

Application note: For the Cisco CA TOE, 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. Thus, "authorized administrator" accounts include accounts defined in IOS XE with the "username" command (regardless of the privilege level assigned to the username).

5.3.6 Protection of the TSF (FPT)

5.3.6.1 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**.

5.3.6.1 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**].

5.3.6.2 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.

5.3.6.3 FPT_STM.1 Reliable time stamps

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

5.3.6.4 FPT_TST_EXT.1: 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.

FPT_TST_EXT.1.2 The TSF shall provide the capability to verify the integrity of stored TSF executable code when it is loaded for execution through the use of the TSF-provided cryptographic service specified in FCS_COP.1(2).

5.3.6.5 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.

5.3.7 Resource Allocation (FRU)

5.3.7.1 FRU_RSA.1 Maximum Quotas

FRU_RSA.1.1 The TSF shall enforce maximum quotas of the following resources: [*SSH services supporting the administrative command line interface*], [and *no other resources*] that [subjects] can use [simultaneously].

5.3.8 TOE Access (FTA)

5.3.8.1 FTA_SSL_EXT.1 TSF-initiated Session Locking

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

- terminate the session]

after a Authorized Administrator specified time period of inactivity.

5.3.8.2 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**.

5.3.8.3 FTA_SSL.4 User-initiated Termination

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

5.3.8.4 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.

5.3.8.5 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 [SSH, TLS, TLS/HTTPS]** 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.

> **Application note:** PI is able to initiate communication to the Cisco CA TOE using an IPsec trusted channel.

FTP_ ITC.1.3 The TSF shall initiate communication via the trusted channel for [*connections with RADIUS and TACACS+ servers (over IPsec), syslog servers (over IPsec), Cisco Mobility Services Engine (over TLS), and NTP servers (over IPsec), remote file servers (over TLS/HTTPS, or SSH (SCP), PI using SNMPv3 traps over IPsec (for sending alert messages)*].

5.3.1.2 FTP_TRP.1 Trusted Path

FTP_TRP.1.1 Refinement: The TSF shall **use** [**SSH**] 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 PP

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 PP which are derived from Common Criteria Version 3.1, Revision 3. The assurance requirements are summarized in the table below.

Table 16: 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
TESTS	ATE_IND.1	Independent testing - conformance
VULNERABILITY ASSESSMENT	AVA_VAN.1	Vulnerability analysis
LIFE CYCLE SUPPORT	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM coverage

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 17 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.
ATE_IND.1	Cisco provides the TOE for testing.
AVA_VAN.1	Cisco provides the TOE for testing.
ALC_CMC.1	The Configuration Management (CM) document(s) describes how the consumer (end-user) of

Component	How requirement will be met
ALC_CMS.1	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.

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 18 How TOE Satisfies the SFRs

TOE SFRs	How the SFR is Met
FAU_GEN.1	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 15. 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.
FAU_GEN.2	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.
FAU_SEL.1	The TOE supports pre-selection (enabling and disabling) of audit messages based on administrator identity, event type, and success or failure. Authorized administrators can specify event types to be enabled or disabled in terms of standard syslog severity levels, and can have different levels defined for the local logging buffer vs. the remote syslog server. All messages contain a facility code, a severity level, a mnemonic code and a message text. The standard syslog severity levels are: • Emergencies = Severity level 0 • Alerts = Severity level 1 • Critical = Severity level 2 • Errors = Severity level 3 • Warnings = Severity level 4 • Notifications = Severity level 5 • Informational = Severity level 6 • Debugging = Severity level 7
FAU_STG.1	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) are able to clear the local logging buffer. **AP Logging** 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

TOE SFRs	How the SFR is Met
	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. **Controller Logging** Controllers may send audit logs to up to three syslog servers that may be configured to receive messages at or below a selected severity level: • Emergencies = Severity level 0 • Alerts = Severity level 1 • Critical = Severity level 2 • Errors = Severity level 3 • Warnings = Severity level 4 • Notifications = Severity level 5 • Informational = Severity level 6 • Debugging = Severity level 7 All system messages have a facility code, a severity level, a mnemonic code and a message text. The logging buffer size can be configured from a range of 4096 (default) to 4,294,967,295 bytes. It is noted to not make the buffer size too large because the TOE could run out of memory for other tasks. Use the show memory privileged EXEC command to view the free processor memory on the TOE. However, this value is the maximum available, and the buffer size should not be set to this amount. The administrator can also configure a 'configuration logger' to keep track of configuration changes made with the command-line interface (CLI). The administrator can configure the size of the configuration log from 1 to 1000 entries (the default is 100). The log buffer is circular, so newer messages overwrite older messages after the buffer is full. Administrators are instructed to monitor the log buffer using the show logging privileged EXEC command to view the audit records. The first message displayed is the oldest message in the buffer. There are other associated commands to clear the buffer, to set the logging level, etc.
FAU_STG_EXT.1 FAU_STG_EXT.3	The TOE is configured to export syslog records to one or more external syslog servers, and protects communications with an external syslog server via IPsec. Audit messages are transmitted to all configured syslog servers at the same time messages are written to other configurable destinations such as the local logging buffer, or the console. 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 TCP syslog connection to a syslog server fails, or cannot be established, a message about the failure will (if configured) be written to the local logging buffer and/or to the console. The syslog daemon on the TOE maintains a small amount of messages is 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.
FCS_CKM.1(1) FCS_CKM.2(1)	The TOE implements a FIPS-approved Deterministic Random Bit Generator 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

TOE SFRs	How the SFR is Met
FCS_CKM.2(2) FCS_COP.1(5) FIA_8021X_EXT.1	elliptic-curve-based key establishment schemes. Cisco assures their components are in conformance with the FIPS 140-2 standard. Each TOE component has been validated in accordance with FIPS 140-2. Details on certificate numbers can be found in table 5.The TOE operates as the 'authenticator' as part of the 802.1X authentication exchange between wireless clients (the 'supplicants') 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. The use of 802.1X results in three communication paths used during the authentication 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). 1. The TOE establishes an EAP over LAN (EAPOL) connection with the wireless client as specified in 802.1X-2007. 2. The TOE establishes a RADIUS protocol connection (tunneled in IPsec) with the RADIUS server. 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. 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)). 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.
FCS_CKM.1(2)	The TOE implements a random number generator for RSA key establishment schemes (conformant to NIST SP 800-56B). The key pair generation portions of "The RSA Validation System" for FIPS 186-2 were used as a guide in testing the FCS_CKM.1 during the FIPS validation. The TOE can create a RSA public-private key pair that can be used to generate a Certificate Signing Request (CSR). Through use of Simple Certificate Enrollment Protocol (SCEP), the TOE can: send the CSR to a Certificate Authority (CA) for the CA to generate a certificate; and receive its certificate (including X.509v3) from the CA. Integrity of the CSR and certificate during transit are assured through use of digitally signatures (encrypting the hash of the TOE's public key contained in the CSR and certificate). The TOE can store and distribute the certificate to external entities including Registration Authorities (RA). The IOS XE Software supports embedded PKI client functions that provide secure mechanisms for distributing, managing, and revoking certificates. In addition, the IOS XE Software includes an embedded certificate server, allowing the router to act as a certification authority on the network.
FCS_CKM_EXT.4	The TOE meets all requirements specified in FIPS 140-2 for destruction of 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 section 7.1 Key Zeroization.
FCS_COP.1(1)	The TOE provides symmetric encryption and decryption capabilities using AES in CBC

TOE SFRs	How the SFR is Met
	mode (128, 256, and 192 bits) as described in NIST SP 800-38A. AES is implemented in the following protocols: IPsec, SSH, TLS, TLS/HTTPS, and DTLS. The relevant FIPS certificate numbers are listed in Table 5 FIPS Certificate Number References.
FCS_COP.1(2)	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 FIPS certificate numbers are listed in Table 5 FIPS Certificate Number References.
FCS_COP.1(3)	The TOE provides cryptographic hashing services using SHA-1, SHA-256, SHA-384, and SHA-512 as specified in FIPS Pub 180-3 "Secure Hash Standard." For IKE (ISAKMP) hashing, administrators can select any of SHA-1, SHA-256, SHA-384, and/or SHA-512 (with message digest sizes of 160, 256, 384, and 512 bits respectively) to be used with remote IPsec endpoints. Both SHA-1 and SHA-256 hashing are used for verification of software image integrity. The relevant FIPS certificate numbers are listed in Table 5 FIPS Certificate Number References.
FCS_COP.1(4)	The TOE uses HMAC-SHA1 message authentication as part of the RADIUS Key Wrap functionality. For IPsec SA authentication integrity options administrators can select any of esp-sha-hmac (HMAC-SHA-1), esp-sha256-hmac, esp-sha384-hmac, or esp-sha512-hmac (with message digest sizes of 160, 256, 384, and 512 bits respectively) to be part of the IPsec SA transform-set to be used with remote IPsec endpoints. The relevant FIPS certificate numbers are listed in Table 5 FIPS Certificate Number References.
FCS_HTTPS_EXT.1 FCS_TLS_EXT.1	The TOE implements TLS/HTTPS for copy commands (initiated only via the CLI by authorized administrators) to remote file servers over TLS/HTTPS where HTTPS is implemented conformant to RFC 2818 and TLSv1.0 is implemented conformant to RFC 2346. TLS is used to authenticate and encrypt NMSP sessions between wireless controllers and MSE. All four mandatory TLS ciphersuites as defined in FCS_TLS_EXT.1 are supported.
FCS_IPSEC_EXT.1	The TOE implements IPsec to provide both certificates and pre-shared key-based authentication and encryption services to prevent unauthorized viewing or modification of data as it travels over the external network. 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. The TOE will use IPsec to secure: connections with AAA servers (RADIUS is required for authentication of wireless clients, and TACACS+ is supported) and connections with audit servers (syslog servers). IPsec Internet Key Exchange (IKE, 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 with X.509v3 certificates, or preshared keys. 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 g^x mod p) using a random bit generator (RBG) specified in FCS_RBG_EXT.1 to ensure the length of "x" is at least 256 bits, and uses output from the RBG to generate nonces of 1024 bits for IKEv2. The key negotiated in phase 1 enables IKE peers to communicate securely in phase 2. During Phase 2 IKE establishes the IPsec SA. IKE maintains a trusted channel, referred to as a Security Association (SA), between IPsec peers that is also used to manage IPsec connections, including: • The negotiation of mutually acceptable IPsec options between peers (including peer authentication parameters, either signature based or pre-shared key based);

TOE SFRs	How the SFR is Met
	• The establishment of additional Security Associations to protect packets flows using Encapsulating Security Payload (ESP); and • The agreement of secure bulk data encryption AES keys for use with ESP. 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. The TOE supports IKEv2 session establishment. As part of this support, the TOE can be configured to only use main mode using the 'crypto isakmp aggressive-mode disable' command. The TOE will be configured to not allow "confidentiality only" ESP mode by ensuring the IKE Policies configured include ESP-encryption. The TOE supports configuration lifetimes of both Phase 1 SAs and Phase 2 SAs through using the "lifetime" command. The default time value for Phase 1 SAs is 24 hours. The default time value for Phase 2 SAs is 1 hour, but it is configurable to 8 hours. The TOE supports configuring the maximum amount of traffic that is allowed to flow for a given IPsec SA using the following command, 'crypto ipsec security-association lifetime'. The default amount is 2560KB, which is the minimum configurable value. The maximum configurable value is 4GB. The TOE supports Diffie-Hellman Group 14 (2048-bit keys), 19 (256-bit Random ECP), 24 (2048-bit MODP with 256-bit POS), 20 (384-bit Random ECP), 15 (3072 bit MODP), and 16 (4096-bit MODP) in support of IKE Key Establishment. These keys are generated using the AES-CTR Deterministic Random Bit Generator (DRBG), as specified in SP 800-90, and the following corresponding key sizes (in bits) are used: 320 (for DH Group 14), 256 (for DH Group 19), 256 (for DH Group 24), 384 (for DH Group 20), 424 (for DH Group 15), and 480 (bits for DH Group 16) bits. Peer authentication uses rDSA (RSA), and can be configured to use pre-shared keys. Pre-shared keys 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 applied to the TOE by the TOE administrator in coordination with the administrator of the remote IPsec endpoint (e.g. AAA server, syslog server, NTP server, or VPN Gateway located between the TOE and those remote servers). Preshared keys can be configured using the 'crypto isakmp key' key command as instructed in the administrator guidance and may be proposed by each of the peers negotiating the IKE establishment. 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. IPsec provides secure tunnels between two peers, such as two routers and remote VPN clients. An authorized administrator defines which packets are considered sensitive and should be sent through these secure tunnels. When the IPsec peer recognizes a sensitive packet, the peer sets up the appropriate secure tunnel and sends the packet through the tunnel to the remote peer. More accurately, these tunnels are sets of security associations (SAs) that are established between two IPsec peers or between the TOE and remote VPN client. The SAs define the protocols and algorithms to be applied to sensitive packets and specify the keying material to be used. SAs are unidirectional and are established per security protocol (AH or ESP). In the evaluated configuration only ESP will be configured for use. The security policy database (SPD) is configured via the crypto map which combines all components required to set up IPsec security associations (SA), including IPsec rules, transform sets, remote peers, and other parameters that might be necessary to define an

TOE SFRs	How the SFR is Met
	IPsec SA. A crypto map entry is a named series of CLI commands. A crypto map may contain multiple entries, each with a different access list. The crypto map entries are searched in a sequence - the TOE attempts to match the packet to the access list (ACL) specified in that entry. When a packet matches a permit entry in a particular access list, the method of security in the corresponding crypto map is applied. If the "crypto map" type is "ipsec-isakmp", IPsec is triggered. The traffic permitted by the ACL associated with the crypto map would then flow through the IPsec tunnel and be classified as "PROTECTED". Traffic that is not permitted by the ACL applied to the crypto map, but is permitted by ACLs applied to the ingress and egress interface is allowed to BYPASS the tunnel. Traffic that is not permitted by the crypto map's ACL and is also not permitted by other non-crypto ACLs applied to ingress and egress interfaces would be DISCARDED. If there is no SA that the IPsec can use to protect this traffic to the peer, IPsec uses IKE to negotiate with the remote peer to set up the necessary IPsec SAs on behalf of the data flow. The negotiation uses information specified in the crypto map entry as well as the data flow information from the specific access list entry.
FCS_RBG_EXT.1	The TOE implements a NIST-approved AES-CTR Deterministic Random Bit Generator (DRBG), as specified in SP 800-90. Note: The details that are proprietary will be provided in a separate entropy document.
FCS_SSH_EXT.1	The TOE implementation of SSHv2 supports the following: • Compliance with RFCs 4251, 4252, 4253, and 4254; • Ensuring that the SSH connection is re-keyed prior to transmission of 2^28 packets; • A configurable time-out period of no more than 120 seconds during which a new session request must provide a password; • A configurable limit of no more than 5 re-attempts to enter a valid password to authenticate a new SSH session; • Use of the SSH_RSA public key algorithm for authentication. • Local password-based authentication for administrative users accessing the TOE through SSHv2, and optionally supports deferring authentication to a remote AAA server. • Dropping packets greater than 65535 bytes, as such packets would violate the IP packet size limitations; • Encryption algorithms AES-CBC-128, and AES-CBC-256 to ensure confidentiality of the session; • Hashing algorithms hmac-sha1, hmac-sha1-96, hmac-md5, and hmac-md5-96 to ensure the integrity of the session; • Enforcement of DH Group 14 (diffie-hellman-group-14-sha1) as the only allowed key exchange method.
FDP_RIP.2	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.
FIA_AFL.1	The TOE 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. 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 a an authorized (authenticated and sufficiently privileged) administrator unlocks the account. The ability for the TOE to enforce this requirement is only applicable when accounts are

TOE SFRs	How the SFR is Met
	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.
FIA_PMG_EXT.1	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: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")". Minimum password length is settable by the Authorized Administrator, and can be configured for minimum password lengths of 15 characters.
FIA_UIA_EXT.1	The TOE requires all users to be successfully identified and authenticated before allowing any TSF mediated actions to be performed. Administrative access to the TOE is facilitated through the TOE's CLI interface, 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), 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), the TOE displays a customizable login banner, which can contain an advisory notice and consent warning message regarding unauthorized use of the TOE.
FIA_UAU_EXT.5	The TOE provides a local password based authentication mechanism as well as RADIUS and TACACS+ authentication. Local, RADIUS and TACACS+ can be configured for use to authenticate CLI accounts. The TOE can be 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. The process for authentication is the same for administrative access whether administration is occurring via a directly connected console cable or remotely via SSH. 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. The TOE does not provide a reason for failure in the cases of a login failure.
FIA_UAU.6	When an authorized administrator changes their own password (only an option via CLI interactive interface), the TOE requires the administrator to re-enter the old/current password prior to changing the password.
FIA_UAU.7	When a user enters their password at the CLI, the TOE displays only '*' (asterisk) characters so that the password is obscured, and the TOE does not echo any characters back to remote clients as the characters are entered.
FIA_X509_EXT.1	The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for IPsec and DTLS connections. Public key infrastructure (PKI) credentials, such as Rivest, Shamir, and Adelman (RSA) keys and certificates can be stored in a specific location on the TOE, such as NVRAM and flash memory or on a USB eToken 64 KB smart card. The certificates themselves provide protection in that they are digitally signed. If a certificate is modified in any way, it would be invalidated. The digital signature verifications process would show that the certificate had been tampered with when the hash value would be invalid. The physical security of the TOE (A.Physical) protects the TOE and the certificates from being tampered with or deleted. In addition, the TOE identification and authentication security functions protect an unauthorized user from gaining access to the TOE. USB tokens provide for secure configuration distribution of the digital certificates and private keys. RSA operations such as on-token key generation, signing, and authentication, and the storage of Virtual Private Network (VPN) credentials for

TOE SFRs	How the SFR is Met
	deployment can be implemented using the USB tokens. Both OSP and CRL are configurable and may be used for certificate revocation. Checking is also done for the basicConstraints extension and the cA flag to determine whether they are present and set to TRUE. If they are not, the certificate is not accepted.
FMT_MOF.1	The TOE provides the ability for Authorized Administrators to access TSF data, such as audit data, configuration data, and security attributes. Each predefined and administratively configured privilege level has a default set of permissions granting access to the TSF data, though with some privilege levels, the access is limited. The TOE performs role-based authorization, using TOE platform authorization mechanisms, to grant access to the semi-privileged and privileged levels. For the purposes of this evaluation, all administrative accounts are presumed to have full administrative access to the CLI, which for IOS-XE is privilege level 15; and semi-privileged accounts refer to any account operating at a privilege level that has a subset of the level 15 privileges. Privilege levels 0 and 1 are defined by default and are customizable, while levels 2-14 are undefined by default (inheriting permissions of level 1) and are also customizable. The term "Authorized Administrator" is used in this ST to refer to any user which has been assigned to a privilege level that is permitted to perform the relevant action; therefore has the appropriate privileges to perform the requested functions. Therefore, semi-privileged administrators with only a subset of privileges can also modify TOE data based on if granted the privilege.
FMT_SMF.1	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, IOS XE 'username' accounts with privilege level less than 15 may have restricted management capabilities. Authorized administrators can connect to the TOE to perform management functions via CLI (console or SSH) and can perform specific management capabilities including, but not limited to: • Local and remote administration of the TOE and the services provided by the TOE; • Initiate updates of the TOE software, including certificate-based image integrity verification; • Configure the cryptographic functionality; • Configure an advisory notice and consent warning message to be displayed at login prior to gaining access to administrative functions. • Configure audit generation functions described earlier in this table for FAU_SEL.1(1). • 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. • Configure (enable/disable/define/re-define) authentication servers used by the Controller. • Define the length of time that an administrative session can remain inactive before the session is terminated, and can configure serial console, SSH with separate timeout limits.
FMT_MTD.1(1) FMT_MTD.1(2) FMT_MTD.1(3)	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 (Controller CLI) are able to modify their own passwords. Though some authorized administrators will have 'full' access to the TOE, even those

TOE SFRs	How the SFR is Met
	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 file by enabling "service password-encryption". 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, including username passwords, authentication key passwords, the privileged command password, console and virtual terminal line access passwords, and Border Gateway Protocol neighbor passwords. Once passwords are stored in their hashed form in the configuration file, they can no longer be viewed in plaintext on the TOE. Pre-shared keys used for IPsec can be stored in AES-encrypted form by setting a master encryption key with the "key config-key password-encrypt" command, and enabling "password encryption aes". Once configured, the master key is used to encrypt any existing or new keys in the router configuration. For security reasons, neither the removal of the master key, nor the removal of the "password encryption aes" command decrypts the passwords in the router configuration, so once encrypted the encrypted keys no longer be viewed in plaintext on the TOE. After these services are enabled, passwords and pre-shared keys can continue to be entered in plaintext form via the CLI, and even when command logging is enabled via the "log config" command, the plaintext form of the passwords will be replaced by "*****" in syslog messages when the "hidekeys" option has also been enabled. 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.
FMT_SMR.1	Once the TOE is operational (after APs have been configured to be managed by a Controller), there is only one administrative role in the TOE, which is the administrator. The Controller Administrator is responsible for management and configuration of the Controller and AP TOE components. 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. A "user" (as defined in CC) is an "external entity -human or IT entity possibly interacting with the TOE from outside of the TOE boundary." The Cisco WLAN Controller administrator accounts are able to access interactive administrative CLI interface on the local console or via SSH. Though Cisco CA supports local authentication of wireless clients, the TOE (Cisco CA in the certified configuration) requires wireless clients to be authenticated through the TOE to a RADIUS server. Thus, the TOE does not maintain roles for wireless clients/users, though the TOE does maintain clear distinction between authenticated wireless clients and authenticated administrators, and wireless clients have no ability to interact with administrative functions or administrative interfaces. Though Cisco CA does support use of an Access Point administrator, the ability to for an administrative user to authenticate directly to an AP (via its local console interface or otherwise) is disabled in the certified configuration. The Console port on the APs is not used during configuration or in the TOEs evaluated configuration and is covered with a tamper evident label once the FIPS Kit is installed.
FPT_FLS.1	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 information flow. There are no failures that circumvent this protection.

TOE SFRs	How the SFR is Met
FPT_ITT.1	When TSF data is transferred between parts of the TOE (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 DTLS (Data TLS, RFC 4347 based on TLS1.1, RFC 4346). The TOE implementation of DTLS supports the same encryption (AES-256) and hashing (SHA-256) options as the WLANPP requires for TLS, and ensures that DTLS 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.
FPT_RPL.1	The TOE detects and drops replay packets for all secure protocols enabled in the certified configuration (IPsec, SSH, TLS, and TLS/HTTPS, as well as DTLS).
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. This This date and time is used as the time stamp that is applied to TOE generated audit records and used to track inactivity of administrative sessions.
FPT_TST_EXT.1	The hardware components of the TOE perform TSF tests during initial start-up of the component. These include the cryptographic module testing on the Catalysts, APs, and Controllers. The APs and Controllers also perform a SHA-1 integrity check on the configuration files upon initial start-up. The calculated checksum is compared to the digitally-signed checksum stored within the image. If the calculated value does not match the digitally-signed value, or if the verification of the digital signature fails the software will not be loaded. The results for these tests are reported at the console upon boot up. As a FIPS 140-2 validated product, 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). 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: • AES Known Answer Test • RSA Signature Known Answer Test (both signature/verification) • RNG Known Answer Test • Diffie Hellman test • HMAC Known Answer Test • SHA-1/256/512 Known Answer Test • Software Integrity Test The Software Integrity Test is run automatically whenever the IOS system images 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.

TOE SFRs	How the SFR is Met
	Cryptographic administrators can initiate the tests by methods specified in the relevant FIPS 140-2 Security Policies. In addition, the Controller administrator may initiate cryptographic self tests via special control packets sent to the crypto processing components and configure periodic self-tests. The capability to verify integrity of stored code can only be performed through the Controller CLI, thus can only be performed by administrator accounts. The capability to verify integrity of TSF data related to key generation can only be performed through the Controller CLI, thus can only be performed by Management User accounts.
FPT_TUD_EXT.1	Authorized administrators can query the software version running on each TOE component, and can initiate updates to (replacements of) software images. When software updates (new controller image bundles) are made available by Cisco, an administrator can obtain, verify the integrity of, and install those updates. The updates can be downloaded from the software.Cisco.com. 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.
FRU_RSA.1	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 for SSH. The switch supports up to five simultaneous secure SSH sessions. This includes the establishment of subject sessions. Meaning if a SSH session is set up between two devices, this would also be considered one of the 5 simultaneous SSH sessions. Administrators have the option to protect these system resources in a number of ways including: • Limiting the number of VTY lines that will support SSH by controller which of the VTY lines are enabled for "transport input ssh"; • Limiting the number of minutes a session may remain open (separate from inactivity timeouts) by setting an "absolute-timeout" value on VTY lines from 0 (zero = no absolute timeout) to 10,000 minutes; • Limiting the number of new SSH sessions that can concurrently be in an authentication state by setting a value for "ip ssh maxstartups" to a value from 2-128; • Limiting the duration of each session authentication state by adjusting the value for "ip ssh time-out" from 1-120 seconds; • Limiting the number of authentication re-tries that may be attempted during a session authentication state by adjusting the value for "ip ssh authentication-retries" to a value from 0-5.
FTA_SSL_EXT.1 FTA_SSL.3	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.
FTA_SSL.4	Administrators are able to initiate termination (logout) of their own authenticated interactive sessions (CLI).
FTA_TAB.1	Authorized administrators define a custom login banner that will be displayed to users of the TOE who connect locally to the Controller CLI via serial console or remotely to the Controller CLI over SSH.
FTA_TSE.1	Authorized administrators can configure the TOE to deny establishment of connections

TOE SFRs	How the SFR is Met
	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	Secure communications between the TOE and non-TOE entities (other than remote administrators and wireless clients) includes communications: • To an audit server using syslog over IPsec (for external audit storage) • To a RADIUS server over IPsec (for 802.1X authentication of wireless clients or password-based authentication of TOE administrators) • To a TACACS+ server over IPsec (for authentication of administrative accounts and/or for the auditing or accounting aspects of AAA) • To/from MSE using TLS (includes wIPS data and signatures, and location data) • From NCS or PI using SNMPv3 tunnelled in IPsec (for external management). • To NCS or PI using SNMPv3 traps over IPsec (for sending alert messages). • To/from NTP servers over IPsec. • Copy (initiated only via the CLI by authorized administrators) to remote file servers over TLS/HTTPS, or SSH (SCP). Note: The TOE is capable of being managed by an external IT entity (PI or NCS) using SNMPv3 over an IPsec tunnel provided by the TOE. SNMPv3 accounts are not considered administrative roles since SNMPv3 is not an interactive interface. TLS is used to authenticate and encrypt NMSP sessions between Controllers and MSE. The Cisco-proprietary aspects of NMSP do not impact the underlying RFC-compliant implementation of TLS. NMSP adds some application-layer features such as session keep-alive timers, and defines a format of the information that's encapsulated in the "data" portion of the packet, but all that is irrelevant/invisible to the transport-layer protocol (TCP for TLS, or UDP for DTLS), and to the presentation-layer protocol (TLS or DTLS). Note: NMSP can be encapsulated over TLS or DTLS, but only TLS is used between MSE and wireless controllers. Interconnections among wireless controllers and APs use a UDP-based protocol secured by DTLS (the UDP form of TLS) for authentication and encryption. DLTS, which is essentially TLS over UDP, is an RFC-defined protocol (http://tools.ietf.org/html/rfc4347) that references the TLS RFC (http://tools.ietf.org/html/rfc2246). The RFC for DTLS doesn't define any DTLS-specific ciphersuites, but instead references the TLS RFC for the ciphersuite definitions, so the DTLS ciphersuites are consistent with the TLS ciphersuites listed in FCS_TLS_EXT.1. The authentication and encryption aspects of TLS are implemented in accordance with the TLS RFC, with UDP-specific characteristics implemented in accordance with the "Differences from TLS" section of the DTLS RFC, http://tools.ietf.org/html/rfc4347.
FTP_TRP.1	Remote administrative communications can be established using SSH (for CLI access). SSH will use AES for encryption, and SHA for integrity. Unencrypted remote administrative connections to the TOE (such as Telnet, SNMPv1, SNMPv2) are administratively disabled.

7 ANNEX A: ADDITIONAL PROPRIETARY INFORMATION TO BE REMOVED AT THE END OF THE EVALUATION

7.1 Key Zeroization

The following table describes the key zeroization referenced by FCS_CKM_EXT.4 provided by the TOE.

Table 19: TOE Key Zeroization

Name	Description	Zeroization
Diffie-Hellman Shared Secret	The value is zeroized after it has been given back to the consuming operation. The value is overwritten by 0's.	Automatically after completion of DH exchange. Overwritten with: 0x00
Diffie Hellman private exponent	The function returns the value to the RP and then calls the function to perform the zeroization of the generated key pair (p_dh_kepair) and then calls the standard Linux free (without the poisoning). These values are automatically zeroized after generation and once the value has been provided back to the actual consumer.	Zeroized upon completion of DH exchange. Overwritten with: 0x00
skeyid	The function calls the operation ike_free_ike_sa_chunk, which performs the zeroization of the IKE structure. This structure contains all of the SA items, including the skeyid, skeyid_d, IKE Session Encryption Key and IKE Session Authentication Key. All values overwritten by 0's.	Automatically after IKE session terminated. Overwritten with: 0x00
skeyid_d	The function calls the operation ike_free_ike_sa_chunk, which performs the zeroization of the IKE structure. This structure contains all of the SA items, including the skeyid, skeyid_d, IKE Session Encryption Key and IKE Session Authentication Key. All values overwritten by 0's.	Automatically after IKE session terminated. Overwritten with: 0x00
IKE session encrypt key	The function calls the operation ike_free_ike_sa_chunk, which performs the zeroization of the IKE structure. This structure contains all of the SA items, including the skeyid, skeyid_d, IKE Session Encryption Key and IKE Session Authentication Key. All values overwritten by 0's.	Automatically after IKE session terminated. Overwritten with: 0x00
IKE session authentication key	The function calls the operation ike_free_ike_sa_chunk, which performs the zeroization of the IKE structure. This structure contains all of the SA items, including the skeyid, skeyid_d, IKE Session Encryption Key and IKE Session Authentication Key. All values overwritten by 0's.	Automatically after IKE session terminated. Overwritten with: 0x00
ISAKMP preshared	The function calls the free operation with the poisoning mechanism that overwrites the value with 0x0d.	Zeroized using the following command: # no crypto isakmp key Overwritten with: 0x0d
IKE RSA Private Key	The operation uses the free operation with the poisoning mechanism that overwrites the value with 0x0d. (This function is used by the module when zeroizing bad key pairs from RSA Key generations.)	Zeroized using the following command: # crypto key zeroize rsa Overwritten with: 0x0d

Name	Description	Zeroization
IPsec encryption key	The function zeroizes an _ike_flow structure that includes the encryption and authentication keys. The entire object is overwritten by 0's using memset.	Automatically when IPsec session terminated. Overwritten with: 0x00
IPsec authentication key	The function zeroizes an _ike_flow structure that includes the encryption and authentication keys. The entire object is overwritten by 0's using memset.	Automatically when IPsec session terminated. Overwritten with: 0x00
RADIUS secret	The function calls aaa_free_secret, which uses the poisoned free operation to zeroize the memory from the secret structure by overwriting the space with 0x0d and releasing the memory.	Zeroized using the following command: # no radius-server key Overwritten with: 0x0d
TACACS+ secret	The function calls aaa_free_secret, which uses the poisoned free operation to zeroize the memory from the secret structure by overwriting the space with 0x0d and releasing the memory.	Zeroized using the following command: # no tacacs-server key Overwritten with: 0x0d
SSH Private Key	Once the function has completed the operations requiring the RSA key object, the module over writes the entire object (no matter its contents) using memset. This overwrites the key with all 0's.	Zeroized using the following command: # crypto key zeroize rsa Overwritten with: 0x00
SSH Session Key	The results zeroized using the poisioning in free to overwrite the values with 0x00. This is called by the ssh_close function when a session is ended.	Automatically when the SSH session is terminated. Overwritten with: 0x00

ANNEX B: REFERENCES

The following documentation was used to prepare this ST:

Table 20: 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
[800-56A]	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 3, CCMB-2009-007-001
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated September 2012, version 3.1, Revision 3, CCMB-2009-007-002
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated September 2012, version 3.1, Revision 3, CCMB-2009-007-003
[CEM]	Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated September 2012, version 3.1, Revision 3, CCMB-2009-007-004
[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
[WLANPP]	Protection Profile for Wireless Local Area Network (WLAN) Access Systems, version 1.0, December, 2011