Cisco Wireless Local Area Network (WLAN) Access System with Integrated Wireless Intrusion Prevention System (wIPS) Security Target

Version: 1.1
March 2013

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE). The evaluated solution is the Cisco Unified Wireless Network (WLAN) & Wireless Intrusion Prevention System (wIPS) release 7.0.230.0, including: Cisco Aironet 3502i, 3502e, 1262, 1252, 1142 AGN access points, 1242, 1131 AG access points, and 1524, 1522 AG outdoor mesh access points; Cisco Wireless LAN Controller 5508; Cisco Wireless LAN Controllers 4402, 4404 and; Cisco Wireless Integrated Services Module (WiSM), and WiSM2. 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.

Table of Contents

List of Tables

1 Security Target Introduction

This section presents Security Target (ST) identification information and an overview of the ST. The structure and content of this ST complies with the requirements specified in the Common Criteria (CC), Part 1, Annex A, and Part 3, Chapter 4.

1.1 ST & TOE Identification

This section provides information needed to identify and control this ST and its TOE. This ST targets Evaluation Assurance Level EAL4 augmented with ALC_FLR.2.

ST Title	Cisco Wireless Local Area Network (WLAN) Access System with Integrated Wireless Intrusion Prevention System (wIPS) Security Target
ST Version	1.1
Publication Date	March 2013

Vendor / Developer	Cisco Systems, Inc.
TOE Identification	Cisco Unified Wireless Network (WLAN)& Wireless Intrusion Prevention System (wIPS) release 7.0.230.0
CC Identification	Common Criteria for Information Technology Security Evaluation, version 3.1, Revision 3, July 2009
Common Criteria Conformance Claim	The ST is compliant with the Common Criteria (CC) version 3.1 Revision 3. The ST is EAL4 Augmented with ALC_FLR.2, Part 2 extended, and Part 3 conformant.
Protection Profile Conformance	This ST claims compliance to the US Government Wireless Local Area Network (WLAN) Access System for Basic Robustness Environments, version 1.1, 25, July 2007 (pp_wlan_as_br_v1.1).
Security Target Evaluation Status	Final
Keywords	Wireless, WLAN, Access Point, AP, wIPS

1.2 Security Target Overview

The TOE consists of hardware and software used to provide a Cisco Unified Wireless Network & Wireless Intrusion Prevention System TOE, hereafter referred to as the TOE, WLAN TOE or WLAN Access System TOE. The TOE is composed of multiple hardware and software products including the Cisco Aironet 3502i, 3502e, 1262, 1252, 1142 AGN access points, 1242, 1131 AG access points, and 1524, 1522 AG outdoor mesh access points; Cisco Wireless LAN Controller 5508; Cisco Wireless LAN Controllers 4402 and 4404; Cisco Wireless Integrated Services Module (WiSM), and WiSM2. Separately, these products are components of the WLAN TOE. Collectively they encompass the entire WLAN TOE. WLAN TOE components are listed below.

1. The Access Point, hereafter referred to as the AP:
    - Cisco Aironet 1131 AG Series Access Point
    - Cisco Aironet 1142 AGN Series Access Point
    - Cisco Aironet 1242 AG Series Access Point
    - Cisco Aironet 1252 AGN Series Access Point
    - Cisco Aironet 1262 AGN Series Access Point
    - Cisco Aironet 1522 AG Series Access Point
    - Cisco Aironet 1524 AG Series Access Point
    - Cisco Aironet 3502e AGN Series Access Point
    - Cisco Aironet 3502i AGN Series Access Point

2. The Controller, hereafter referred to as the Controller or the WLC (or WiSM when distinction is necessary between the WLC appliances and the Wireless Services Module):
    - Cisco 4400 Series Wireless LAN Controllers
    - Cisco 5508 Series Wireless LAN Controllers
    - The Wireless Integrated Services Module (WiSM), and WiSM2 hereafter both referred to as the WiSM.
3. The WLAN software. The end user downloads from Cisco.com a WLAN Controller image bundle that includes AP images (images of IOS 12.4(23c)JA4 for each AP model) that each AP downloads directly from its Controller. Those WLAN image bundlesthat are part of the TOE are:
    - Cisco Unified Wireless Network Software Release 7.0 for Cisco 5500 Series Wireless LAN Controllers.
        a. AIR-CT5500-K9-7-0-230-0.aes
    - Cisco Unified Wireless Network Software Release 7.0 for Cisco 4400 Series (4402 and 4404) Wireless LAN Controllers.
        a. AIR-WLC4400-K9-7-0-230-0.aes
        b. Boot Software 7.0 for Cisco 4400 Series Controllers: AIR-WLC4400-K9-7-0-230-0-ER.aes
    - Cisco Unified Wireless Network Software Release 7.0 for Catalyst 6500 Series Wireless Services Module (WiSM and WiSM2).
        a. SWISMK9-7-0-230-0.aes
        b. AIR-WISM2-K9-7-0-230-0.aes
        c. Boot Software Release 7.0 for Catalyst 6500 Series WiSMs: SWISMK9-7-0-230-0-ER.aes

This ST is based on the US Government Wireless Local Area Network (WLAN) Access System for Basic Robustness Environments, version 1.1, July 25, 2007 (pp_wlan_as_br_v1.1) and describes Cisco product features that satisfy the security functional and assurance requirements identified in the PP.

1.3 References

The following documentation was used to prepare this ST:

[CC_PART1]	Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, dated July 2009, version 3.1, Revision 3, CCMB-2009-07-003
[CC_PART2]	Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components, dated July 2009, version 3.1, Revision 3, CCMB-2009-07-002
[CC_PART3]	Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, dated July 2009, version 3.1, Revision 3,CCMB-2009-07-003

[CEM]	Common Methodology for Information Technology Security Evaluation - Evaluation Methodology, dated July 2009, version 3.1, Revision 3, CCMB-2009-07-004
[WLANPP]	US Government Wireless Local Area Network (WLAN) Access System for Basic Robustness Environments, version 1.1, July 25, 2007 (pp_wlan_as_br_v1.1)

1.4 Acronyms, Abbreviations & Terms

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

Table 1Acronyms, Abbreviations & Definitions

Acronyms & Abbreviations	Definition
AAA	Authentication, Authorization, and Accounting
ACS	Cisco Secure Access Control Server
AES	Advanced Encryption Standard
AP	Access Point
CC	Common Criteria for Information Technology Security Evaluation
CCM	Counter with CBC-MAC (Cipher Block Chaining Message Authentication Code)
CCMP	CCM mode Protocol
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology for Information Technology Security
CAPWAP	Control and Provisioning of Wireless Access Points
CLI	Command Line Interface
CM	Configuration Management
CPU	Central Processing Unit
DDR	Double Data Rate
DHCP	Dynamic Host Configuration Protocol
EAL	Evaluation Assurance Level

EAP	Extensible Authentication Protocol
EAP-TLS	Extensible Authentication Protocol-Transport Layer Security
EAPOL	EAP over LAN
ECC	Error Correction Coding
FSP	Functional Specification
GUI	Graphical User Interface
HLD	High Level Design
HTTPS	Secure Hypertext Transfer Protocol
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
ISE	Cisco Identity Services Engine
IT	Information Technology
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LEAP	Lightweight Extensible Authentication Protocol [EAP Cisco Wireless authentication type]
MAC	Message Authentication Code
Mbps	Megabits per second
MIB	Management Information Base (for SNMPv3)
MSE	Cisco Mobility Services Engine
NAS	Network Access Server
NCS	Cisco Prime Network Control System
NIAP	National Information Assurance Partnership
NIC	Network Interface Card
NMSP	Network Mobility Services Protocol
OS	Operating System
PAC	ProtectedAccess Credentials

PEAP	Protected Extensible Authentication Protocol
PEAP (EAP-GTC)	PEAP (Extensible Authentication Protocol-Generic Token Card)
PEAP (EAP-MSCHAP V2)	PEAP (Extensible Authentication Protocol-Microsoft Challenge Authentication Protocol version 2)
PKI	Public Key Infrastructure
PMK	Pairwise Master Keys
PP	Protection Profile
PSK	Pre-shared key
PSPF	Public Secure Protocol Format
RADIUS	Remote Authentication Dial-In User Service
RF	Radio Frequency
RFID	Radio-Frequency Identification
RSSI	Received Signal Strength Indication
SAR	Security Assurance Requirement
SDRAM	Synchronous Dynamic Random Access Memory
SFP	Security Function Policy
SFR	Security Functional Requirement
SNMPv3	Simple Network Management Protocol version 3
SOF	Strength of Function
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Socket Layer
ST	Security Target
TDofA	Time Difference of Arrival
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function

TSP	TOE Security Policy
Wi-Fi	Wireless Fidelity
WIDS	Wireless Intrusion Detection System
wIPS	Wireless Intrusion Prevention System
WiSM	Wireless Services Module
WLAN	Wireless LAN
WLC	Cisco Wireless LAN Controller
WCS	Cisco Wireless Control System
WPA2	Wi-Fi Protected Access 2

The following terms are used in this Security Target:

Table 2Terms & Definitions

Terms	Definitions
802.1X	The IEEE 802.1X standard provides a framework for many authentication types and the link layer.
AAA Client	Provides authentication, authorization and accounting. Also known as a NAS
ACS/ISE Host	The IT Environment that includes the hardware and operating system that hosts the ACS and/or ISE software.
CARS	The Operating System that runs on the ACS Host is a CentOS Linux distribution operating system, as configured for use by the ACS software.
EAP	Stands for the extensible authentication protocol (EAP). EAP is a protocol that supports the communication of other authentication protocols. EAP uses its own start and end messages which allows it to then support any number of third-party messages between supplicants and an authentication server.
EAP-FAST	Stands for EAP-flexible authentication secure tunneling (EAP-FAST). This method provides an encrypted tunnel to distribute pre-shared keys known as protected access credential (PAC) keys.
EAP-GTC	EAP-GTC (Generic Token Card), which is described in RFC 2284, is used for authenticating token card credentials across the network. EAP-GTC is typically used inside a TLS tunnel created by TTLS or PEAP to provide server authentication in wireless environments.

EAP-MSCHAP V2	EAP-MS-CHAP-V2 (Microsoft Challenge-Handshake Authentication Protocol version 2) is a mutual authentication method that supports password-based user or computer authentication. EAP-MS-CHAP-V2 is typically used inside a TLS tunnel created by TTLS or PEAP.
EAP-TLS	EAP-TLS (RFC 2716) stands for Extensible Authentication Protocol-Translation Layer Security. It uses the TLS protocol (RFC 2246) authentication hand shaking implementation for 802.1x authentication. TLS provides a way to use certificates for both user and server authentication and for dynamic session key generation and protection of the authentication session.
Management Frame Protection	A wireless technology enabling one access point to validate a neighboring Access Point's management frames.
PEAP	Protected Extensible Authentication Protocol, Protected EAP, is a method to securely transmit authentication information, including passwords, over wired or wireless networks. PEAP uses server-side public key certificates to authenticate the server. It then creates an encrypted SSL/TLS tunnel between the client and the authentication server. The ensuing exchange of authentication information to authenticate the client is then encrypted and user credentials are safe from eavesdropping.
WPA2	Wi-Fi Protected Access

2 TOE Description

This section provides an overview of the Cisco Unified Wireless Network & Wireless Intrusion Prevention System. This chapter also defines the physical and logical boundaries; summarizes the security functions; and describes the evaluated configuration.

2.1 TOE Product Type

The Target of Evaluation (TOE) is a Wireless LAN access system (WLAN) with an integrated Wireless Intrusion Prevention System (wIPS). The Wireless LAN access system defined in this ST comprises multiple products operating together to provide secure wireless access to a wired and wireless network. The Wireless Intrusion Prevention System defined in this ST are the wIPS capabilities defined in this ST including IDS signature detection, rogue AP and client detection and containment, and 802.11 management frame protection (MFP). This TOE as identified above is the Cisco Unified Wireless Network & Wireless Intrusion Prevention System TOE which provides end-to-end wireless encryption, centralized WLAN management, Authentication, Authorization, and Accounting (AAA) policy enforcement, and basic Wireless Intrusion Prevention System (wIPS) with support foradvanced WiPS and location tracking when used with the Cisco Mobility Services Engine (MSE). Note that the TOE does not claim conformance to an IDS/IPS Protection Profile, the wIPSfunctionality described in this ST includes detection of wireless intrusion attempts, generation of audit data related to those events, delivery of that audit data to external components (WCS or

NCS,MSE, and syslog server) in the environment for analysis and review, and denial of traffic flow and/or containment of rogue access points and clients consistent with applied wIPS policies. The AP performs analysis of wireless traffic in the course of generating wIPS data – the wIPS event log items represent events sent from the wIPS system to the MSE. Responses to the wIPS data from the WCS or NCSare sent via SNMPv3 and from MSE are sent via NMSP to the Controller, and wIPS policy updates are pushed from the Controller to APs where wIPS policies are enforced. The TOE relies on the WCS or NCS and MSE components in the IT environment to support the wIPS functionality by defining wIPS policies, and for location tracking by correlating wireless signal metrics measured by multiple APs.

2.2 TOE Overview

The TOE is a system of products administratively configured to interoperate to provide a WLAN. The TOE allows mobile, wireless clients to be roaming hosts on the wireless network, and to connect to the wired network using access points (APs). The TOE has Access Point TOE components (Cisco Aironet3502i, 3502e, 1262, 1252, 1142 AGN access points, 1242, 1131 AG access points, and 1524, 1522 AG outdoor mesh access points), Controller TOE components (Cisco Wireless LAN Controllers 4402 and 4404,Cisco Wireless LAN Controller 5508,and the Cisco WiSM (Cisco Wireless Services Module) and WiSM2.

Note that although there are several TOE components, when the TOE is operational there is only one component that providesadministrative interfaces authenticated by the TOE: the Controller, so there is one administrator role on the TOE.

2.3 TOE Physical Boundary

The TOE physical boundary defines all hardware and software that is required to support the TOE's logical boundary and the TOE's security functions. The TOE's support of the logical boundary and security functions is divided into functional components (TOE components) which are described in this section.

Hardware and software not included in the TOE's physical boundary and relied on by the TOE and therefore supplied by the IT Environment is described in the IT Environmental Dependencies section of this document. Security functionality included in the TOE's physical boundary but not identified in the TOE's logical boundary or claimed as TOE security functions is identified in the TOE Component Communication Methods.

Table 3 below identifies the required components in the evaluated configuration and identifies whether or not they are within the TOE boundary. This is followed by a sample network arrangement of the TOE and detailed subsections on each TOE component.

Table 3Required Number & Versions

Component Name	Required Quantity	Model Number and Versions	Part of TOE
AP	**One or more**	Cisco Aironet 1131 AG Series Access Points Cisco Aironet 1142AGN Series Access Points Cisco Aironet 1242 AG Series Access Points Cisco Aironet 1252 AGN Series Access Points Cisco Aironet 1262 AGN Series Access Points Cisco Aironet 1522 AG Series Access Points Cisco Aironet 1524 AG Series Access Points Cisco Aironet 3502e AGN Series Access Points or Cisco Aironet 3502i AGN Series Access Points each running IOSversion 12.4(23c)JA4 (downloaded to the AP from the Controller) and includingthe Cisco FIPS kit part number AIRLAP-FIPSKIT	**Yes**
4400 Controller *or* *5508 Controller* *or* *WiSM* *or* *WiSM2*	**One or more**	Cisco 4400 Series Wireless LAN Controller running software version 7.0.230.0; and the Cisco FIPS kit part number AIRWLC4400FIPSKIT; Cisco 5508 Series Wireless LAN Controller running software version 7.0.230.0; and the Cisco FIPS kit part number AIR-CT5508FIPSKIT; or *Cisco Wireless Integrated Service Module (WiSM) or WiSM2 w/software version 7.0.230.0, and Cisco FIPS kit as appropriate for the 6500 chassis.*	**Yes**
6500 Chassis and Supervisor 720	**One or more (with WiSM or WiSM2 only)**	*6500 Catalyst chassis; and the* Cisco FIPS kit part number CVPN6500FIPS/KIT. *720 Supervisor w/software IOS versions* 12.2(18)SXF2 *or* 12.2(18)SXF5	**No**
Cisco ACS or ISE	**One or more**	Cisco Secure Access Control Server (ACS) version 5.3 or lateron any of the following platforms: Cisco 1120 Secure ACS appliance Cisco 1121 Secure ACS appliance Virtual appliances running VMware version ESX 3.5 or 4.0 Or Cisco Identity Services Engine (ISE) version 1.1 or later on any supported hardware or virtual appliance.	**No**
Syslog server	**One or more**	Any syslog server that supports receiving syslog over TLS, and meets pre-filtering requirements specified in FAU_SEL.1(2), including: Kiwi Syslog Daemon version 9.2 or later, or Syslog-ng version 2.0 or later.	**No**
Wireless Client	**One or more**	No specific version requirements	**No**
Cisco MSE	**One**	Release 5.1.30.0 (or greater)	**No**
Cisco WCS or NCS	**One**	WCS release 5.1.64.0 (or greater) NCS release 1.0 (or greater)	**No**
Certificate Authority	**One**	This CA does not need to be dedicated for use by the TOE, nor managed by the TOE administrators, it only needs to be available to generate certificates for use with the syslog server (for syslog over TLS), and when using EAP-TLS, or EAP-FAST.	**No**
LDAP Server or Active Directory Server	**None or One**	If ISE is being used as the RADIUS server to authenticate Controller Management Users, an LDAP, AD, or additional RADIUS server (such as ACS) is also required.	**No**

Figure 1 depicts a sample TOE configuration, highlighting the physical boundary. The shaded portions define the components in the physical boundary. The un-shaded portions define the components supplied by the IT Environment.

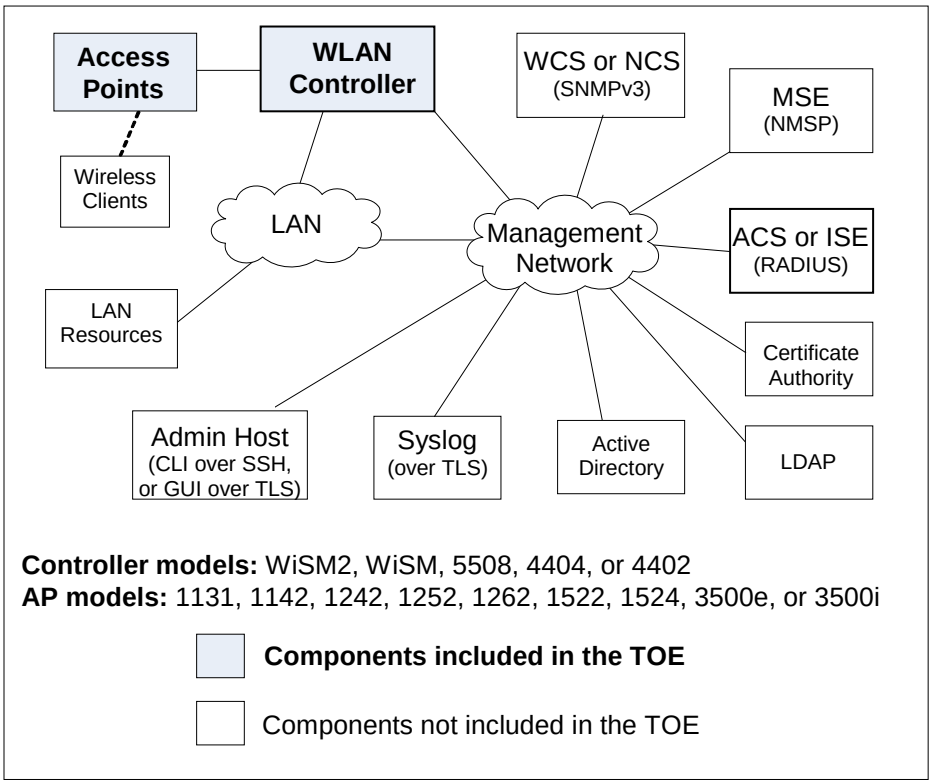


Figure 1Sample Deployment Topology

The following subsections describe the TOE components in detail.

2.3.1 Access Point (AP) TOE Component

The following Access Point models:

- Cisco Aironet 1131 AG Series Access Points
- Cisco Aironet 1142 AG Series Access Points
- Cisco Aironet 1242 AG Series Access Points
- Cisco Aironet 1252 AG Series Access Points
- Cisco Aironet 1262 AG Series Access Points
- Cisco Aironet 1520 AG Series Access Points
- Cisco Aironet 3500 AG Series Access Points

Hereafter referred to as Access Points or APs, the APs provides the connection point between wireless client hosts and the wired network. Once authenticated as trusted nodes on the wired infrastructure, the APs provide encryption service on the wireless network between themselves and the wireless client. The APs also communicate directly with the Controller for management purposes.

The physical boundary of the APs includes FIPS Kits that cover the physical interfaces of the APs to make them FIPS compliant. The FIPS Kits are part of the physical boundary of the AP. The FIPS Kits for the APs are the Cisco product number AIRLAP-FIPSKIT.

The AP TOE components have an RF interface, an Ethernet interface, and a serial console interface. All three of these interfaces are controlled by the software executing on the AP.

The seven Access Point series included in the TOE physical boundary vary by the antenna support they offer; however the differences do not affect the security functionality of the TOE.

The serial or console interface to the AP is not included in the evaluated configuration. This interface cannot be used for administration or configuration of the AP when the AP is in its evaluated configuration, fully managed by a Controller. All administration and configuration of the AP TOE component occurs through the Controller TOE component.

The Ethernet interface of the AP is a wired interface that connects the AP to the Controller. The Ethernet interface is used as a management interface to the AP and also as the communication channel for those successfully authenticated wireless users to communicate with the wired network controlled by the TOE and the other successfully authenticated wireless users. Wired communications between the APs and Controllers (or WiSM) is carried out using the Control and Provisioning of Wireless Access Points (CAPWAP). Control and Provisioning of Wireless Access Points (CAPWAP) is an IETF network protocol draft supported by the APs and controllers that aids in centralized management and security of the controllers and APs. Specifically, CAPWAP supports traffic handling, authentication, encryption and policy enforcement. CAPWAP is the underlying protocol selected by the IETF Control and Provisioning of Wireless Access Points (CAPWAP) Working Group. CAPWAP has also been validated by NIST for FIPS 140-2 Level 2 certification. CAPWAP allows the APs and Controllers to carry out secure control and bridging communications over a FIPS 140-2 validated assured channel using DTLS with AES-CBC encryption. On the 5508 Controller and 1131, 1142, 1242, 1252, 1262, 3502E, and 3502I series access points a secondary DTLS tunnel is supported for protection of client data as part of CAPWAP. Note that all TOE devices have a separate tunnel for client data traffic as part of CAPWAP, but only the devices above support DTLS protection of this tunnel.

- Wireless communications between clients and APs is carried out using the IEEE 802.11 protocol standardgoverning communication transmission for wireless devices. For this evaluation the APs use one or more of the following: 802.11a, 802.11b, 802.11g and 802.11n for wireless communication. The wireless security protocol that is to be used with the APs is WPA2, which is the Wi-Fi Alliance interoperable specification based on IEEE 802.11i security standard (described below).

The following table provides details for each of the Access Points models included in the TOE.

Table 4Cisco Access Point Model, Hardware Configuration, and Part Number

TOE Configuration	Hardware Configuration	Part Numbers

Cisco Aironet 1131 AG Series Access Point 	The Cisco Aironet 1131 AG Series IEEE 802.11a/b/g Access Point is a fixed-configuration dual-band Access Point. The Cisco 1131 AG Series IEEE 802.11a/b/g Access Point provides two radios each with diversity antennas that provide omni-directional coverage. The TOE's physical boundary includes the listed Cisco Aironet 1131 AG Series Access Points which are considered hardware components of the TOE. This module is within the TOE boundary.	AIR-LAP1131AG-A-K9 AIR-LAP1131AG-C-K9 AIR-LAP1131AG-E-K9 AIR-LAP1131AG-I-K9 AIR-LAP1131AG-K-K9 AIR-LAP1131AG-N-K9 AIR-LAP1131AG-P-K9 AIR-LAP1131AG-Q-K9 AIR-LAP1131AG-S-K9 AIR-LAP1131AG-T-K9
Cisco Aironet 1142 AG Series Access Point 	The Cisco Aironet 1142 AG Series IEEE 802.11a/b/g/n Access Point is a fixed-configuration dual-band Access Point. The Cisco 1142 AG Series IEEE 802.11a/b/g /n Access Point provides two radios each with diversity antennas that provide omni-directional coverage. The TOE's physical boundary includes the listed Cisco Aironet 1142 AG Series Access Points which are considered hardware components of the TOE. This module is within the TOE boundary.	AIR-LAP1142N-A-K9 AIR-LAP1142N-C-K9 AIR-LAP1142N-E-K9 AIR-LAP1142N-P-K9 AIR-LAP1142N-K-K9 AIR-LAP1142N-N-K9 AIR-LAP1142N-S-K9 AIR-LAP1142N-T-K9 AIR-LAP1142N-I-K9
Cisco Aironet 1242 AG Series Access Point 	The Cisco Aironet 1242 AG Series IEEE 802.11a/b/g Access Point is a fixed-configuration dual-band Access Point. The Cisco 1242 AG Series IEEE 802.11a/b/g Access Point provides two radios each with diversity antennas that provide omni-directional coverage. The TOE's physical boundary includes the listed Cisco Aironet 1242 AG Series Access Points which are considered hardware components of the TOE. This module is within the TOE boundary.	AIR-LAP1242AG-A-K9 AIR-LAP1242AG-C-K9 AIR-LAP1242AG-E-K9 AIR-LAP1242AG-I-K9 AIR-LAP1242AG-K-K9 AIR-LAP1242AG-N-K9 AIR-LAP1242AG-P-K9 AIR-LAP1242AG-Q-K9 AIR-LAP1242AG-S-K9 AIR-LAP1242AG-T-K9

Cisco Aironet 1252 AG Series Access Point 	The Cisco Aironet 1252 AG Series IEEE 802.11a/b/g/n Access Point is a fixed-configuration dual-band Access Point. The Cisco 1252 AG Series IEEE 802.11a/b/g /n Access Point provides two radios each with diversity antennas that provide omni-directional coverage. The TOE's physical boundary includes the listed Cisco Aironet 1252 AG Series Access Points which are considered hardware components of the TOE. This module is within the TOE boundary.	AIR-LAP1252AG-A-K9 AIR-LAP1252AG-C-K9 AIR-LAP1252AG-E-K9 AIR-LAP1252AG-I-K9 AIR-LAP1252AG-K-K9 AIR-LAP1252AG-N-K9 AIR-LAP1252AG-P-K9 AIR-LAP1252AG-S-K9 AIR-LAP1252AG-T-K9
Cisco Aironet 1262 AG Series Access Point 	The Cisco Aironet 1262 AG Series IEEE 802.11a/b/g/n Access Point is a fixed-configuration dual-band Access Point. The Cisco 1262 AG Series IEEE 802.11a/b/g /n Access Point provides two radios each with diversity antennas that provide omni-directional coverage. The TOE's physical boundary includes the listed Cisco Aironet 1262 AG Series Access Points which are considered hardware components of the TOE. This module is within the TOE boundary.	AIR-LAP1262N-A-K9 AIR-LAP1262N-C-K9 AIR-LAP1262N-E-K9 AIR-LAP1262N-I-K9 AIR-LAP1262N-K-K9 AIR-LAP1262N-N-K9 AIR-LAP1262N-Q-K9 AIR-LAP1262N-S-K9 AIR-LAP1262N-T-K9

Cisco Aironet 1520 AG Series Access Point 	The Cisco Aironet 1520 AG Series IEEE 802.11a/b/g Access Point is a fixed-configuration dual-band Access Point. The Cisco 1520 AG Series IEEE 802.11a/b/g Access Point provides two radios each with diversity antennas that provide omni-directional coverage. The Cisco Aironet 1520 AG Series is comprised of two models, the Cisco Aironet 1522 and the Cisco Aironet 1524. The TOE's physical boundary includes the listed Cisco Aironet 1520 AG Series Access Points which are considered hardware components of the TOE. This module is within the TOE boundary.	AIR-LAP1522AG-A-K9 AIR-LAP1522AG-C-K9 AIR-LAP1522AG-E-K9 AIR-LAP1522AG-K-K9 AIR-LAP1522AG-N-K9 AIR-LAP1522AG-M-K9 AIR-LAP1522AG-P-K9 AIR-LAP1522AG-S-K9 AIR-LAP1522AG-T-K9 AIR-LAP1522CV-A-K9 AIR-LAP1522PC-A-K9 AIR-LAP1522PC-N-K9 AIR-LAP1522HZ-A-K9 AIR-LAP1522HZ-C-K9 AIR-LAP1522HZ-N-K9 AIR-LAP1522HZ-E-K9 AIR-LAP1522HZ-S-K9 AIR-LAP1524PS-A-K9 AIR-LAP1524SB-A-K9 AIR-LAP1524SB-C-K9 AIR-LAP1524SB-M-K9 AIR-LAP1524SB-N-K9
Cisco Aironet 3500 AG Series Access Point 	The Cisco Aironet 3500 AG Series IEEE 802.11a/b/g/n Access Point is a fixed-configuration dual-band Access Point. The Cisco 3500 AG Series IEEE 802.11a/b/g /n Access Point provides two radios each with diversity antennas that provide omni-directional coverage. The 3500 series is made up of two models, the Cisco Aironet 3502E and the Cisco Aironet 3502I. The "E" designation refers to "External" antennas while the "I" designation refers to an "Internal" antenna configuration. The TOE's physical boundary includes the listed Cisco Aironet 3500 AG Series Access Points which are considered hardware components of the TOE. This module is within the TOE boundary.	AIR-CAP3502I-A-K9 AIR-CAP3502I-C-K9 AIR-CAP3502I-E-K9 AIR-CAP3502I-I-K9 AIR-CAP3502I-K-K9 AIR-CAP3502I-N-K9 AIR-CAP3502I-Q-K9 AIR-CAP3502I-S-K9 AIR-CAP3502I-T-K9 AIR-CAP3502E-A-K9 AIR-CAP3502E-C-K9 AIR-CAP3502E-E-K9 AIR-CAP3502E-I-K9 AIR-CAP3502E-K-K9 AIR-CAP3502E-N-K9 AIR-CAP3502E-Q-K9 AIR-CAP3502E-S-K9 AIR-CAP3502E-T-K9

2.3.2 Wireless LAN Controller TOE Component

The Wireless LAN Controller TOE components (herein referred to as Controller) are management devices for one or more APs and the wireless LANs that are implemented on the APs. The Controller communicates with the AP TOE components, and other external components including admin workstation, ACS/ISE servers, syslog server, WCS or NCS, and MSE through its network interface. The Controllers provide WLAN security, monitoring, quality of service and radio resource management services for APs over redundant Gigabit Ethernet network interfaces.

The Controllers provide security management services for APs include managing access control lists (ACLs) for wireless devices, defining the authentication policies and authorization and accounting servers that are to be used by the TOE, defining the encryption types and security policies that the APs are to enforce, and managing the radio resource management capabilities.

The Controllers provide monitoring management services to monitor the state of APs, the state of wireless devices associated with the APs, along with the security events detected by the APs which include wireless intrusion prevention signature detection, rogue device detection, 802.11 management frame protection and the containment of rogue access points and rogue wireless clients.

- The Controllers have a web based and a command line interface for administration. Both are included in the evaluated configuration of the TOE. Changes that affect APs are pushed out to the APs immediately using CAPWAP management plane messages.
- AES RADIUS key wrap is used to protect the 802.11i PMK distributed from ACS/ISE to the Controller after a successful wireless user authentication. The Controller ensures that this management interface between the Controller and the ACS/ISE is invoked and succeeds before allowing any other mediate security function dealing with authentication or accounting to proceed.
- The Controller interfaces with the APs for management communication. The Controller ensures that the management interface functions are invoked and succeed before allowing any further management functions to be carried out between the Controller and the APs.

Controllers enforce protection of audit events being logged by transmitting syslog over TLS to the Syslog server.

The following table provides details for each of the Wireless LAN Controllers included in the TOE.

Table 5Cisco Wireless LAN Controllers, Hardware Configuration, and Part Numbers

TOE Configuration	Hardware Configuration	Part Numbers
Cisco 4400 Series Wireless LAN Controller 	The Cisco 4400 Wireless LAN Controller is a series of wireless LAN controllers that is available in two models: the 4402 Cisco 4400 Series Wireless LAN Controller and the 4404 Cisco 4400 Series Wireless LAN Controller. The two models differ in the number of redundant Gigabit Ethernet connections they provide: The 4402 Cisco 4400 Series Wireless LAN Controller provides one set of two redundant Gigabit Ethernet connections. The 4404 Cisco 4400 Series Wireless LAN Controller provides two sets of redundant Gigabit Ethernet connections. Within the Cisco 4400 models are products that vary in the number of access points they support and the regulatory domains they support. The Cisco 4402 Wireless LAN Controller supports either 12, 25 or 50 access points while the Cisco 4404 Wireless LAN Controller supports 100 access points. Part of the physical boundary of the 4400 series controllers are FIPS Kits that change the physical interfaces of the 4400 series controllers to make them FIPS compliant. The FIPS Kits are part of the physical boundary of the 4400 series controllers. The FIPS Kits for the 4400 series controllers are the Cisco product number AIRWLC4400-FIPSKIT.This module is within the TOE boundary.	AIR-WLC4402-12-K9 AIR-WLC4402-25-K9 AIR-WLC4402-50-K9 AIR-WLC4404-100-K9
Cisco 5500 Series Wireless LAN Controller 	The Cisco 5500 Series Wireless LAN Controller functionally is the same as the 4400 series Controller. Whereas the 4400 series supported up to 100 access points the Cisco 5500 series supports up to 500 access points. The Cisco 5508 Wireless LAN Controller supports 12, 25, 50, 100, 250 or 500 access points. FIPS Kit AIR-CT5508FIPSKIT=.	AIR-CT5508-12-K9 AIR-CT5508-25-K9 AIR-CT5508-50-K9 AIR-CT5508-100-K9 AIR-CT5508-250-K9 AIR-CT5508-500-K9

Catalyst 6500 Wireless Integrated Service Module (WiSM) and WiSM2 	The WiSM and WiSM2 functionally is the same as the 4400 or 5500 series Controllers. The WiSM and WiSM2 are hardware modules that plug into a Catalyst 6500 switch chassis. Each WiSM blade supports up to 300 Access Points. The Supervisor 720 provides routing and switching to support network connectivity to the management interface of the WiSM and WiSM2. The WiSM and WiSM2 controllerssupport the following 5 chassis configurations: 6503, 6504, 6506, 6509 and 6513. The chassis vary in the number of slots they provide, but this difference does not affect the security functionality claimed by the TOE. Up to four WiSM or WiSM2 blades with support for 1200 APs can be managed by a single 6509 or 6513 Catalyst chassis with a Supervisor 720. A fifth WiSM or WiSM2 blade can be installed in the Catalyst 6509 or 6513 chassis for redundant failover of another WiSM or WiSM2 within the same chassis. The chassis is not included in the TOE physical boundary, nor is the Sup720. Though the 6500 chassis is not part of the physical TOE boundary, the evaluated configuration requires that the Catalyst 6500 be installed with its FIPS Kit, Cisco product number CVPN6500FIPS/KIT.	WS-SVC-WISM-1-K9 WS-SVC-WISM2-1-K9 WS-SVC-WISM2-3-K9 WS-SVC-WISM2-5-K9

2.4 TOE Logical Boundary

This section identifies the security functions provided by the TSF.

- Administration (FMT)
- Audit (FAU)
- Encryption (FCS)
- Identification and Authentication (FIA)
- Information Flow Control (FDP)
- Self Protection (FPT)
- Wireless Intrusion Prevention System (IPS)

2.4.1 Administration (FMT)

The TOE's Administration security functions provides security capabilities that guarantees Controller administrators are required to identify and authenticate to the TOE or to a RADIUS server configured for use by the TOE before any administrative actions can be performed. Syslog administrators identify and authenticate to the Syslog Host OS prior to managing syslog settings or reviewing audit data stored there. RADIUS server administrators authenticate to ISE or ACS prior to administrating the RADIUS server. NCS/WCS and MSE administrators authenticate to NCS/WCS and MSE respectively before configuring NCS/WCS and MSE. The Syslog Host OS, RADIUS server, NCS/WCS and MSE are outside the TOE scope of control, so authentication of their administrators is also outside the scope of control. The TOE only allows administration of TOE components to occur from the wired network. The TOE's management security capability provides administrator support

functionality that enables a human user to configure and manage TOE components.Management functions include configuration of cryptographic keys, encryption settings, audit settings, authentication credentials, and the use of authentication servers.

The SFRs covered by this security function are FMT_MOF.1(1), FMT_MOF.1(2), FMT_MOF.1(3), FMT_MSA.2, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), FMT_SMF.1(1), FMT_SMF.1(2), FMT_SMF.1(3), FMT_SMR.1(1), FTA_SSL.3

2.4.2 Audit (FAU)

The TOE's Audit security function supports audit record generation and selective audit record generation functionality. All components of the TOE work to implement an auditing capability of security relevant events that happen under the control of the TOE. Audit records are generated by the APs, and Controllers of the TOE, and the ACS/ISE of the TOE IT Environment. The TOE's audit data viewing capability provides administrator support functionality that enables administrators to view audit records and selective view audit records along with allowing them to selectively choose what events they want audited.

Audit generation by the TOE (viewable via the controller or the remote syslog server):

- The TOE generates audit records of administrator actions related to the management of TSF data and configuration data. Controller administrator actions are audited by means of TACACS+ Accounting messages sent from the Controller to the ACS/ISE. In the evaluated configuration, ACS/ISE will be configured to send these messages to the syslog server as well.
- The TOE generates wIPS audit records based on signatures distributed by the MSE, by monitoring and analyzing wireless network traffic and generating events/alerts for potential intrusions. The TOE includes Denial of Service Security Penetration Attack Wireless Intrusion Prevention Signatures which it uses to detect unauthorized or threatening WLAN activity. This information is generated by the APs, and forwarded through the Controller to the MSE over a TLS protected interface.

Audit generation by the TOE IT Environment (viewable via the ACS/ISE):

- Wireless users authentication attempts (successful and failed) and ACS/ISE administrative audit events are sent from the ACS/ISE to the Syslog storage for pre-selection, storage and review. Other ACS/ISE audit activities (the management of user accounts controlled by the ACS/ISE, the encryption policies controlled by the ACS/ISE for wireless users, and the changing of auditing capabilities controlled by the ACS/ISE) may be written into ACS/ISE persistent storage for a time before being sent to the Syslog server. Post selection filtering can be done on any audit records stored on the Syslog server.

The SFRs covered by this security function are FAU_GEN.1(1), FAU_GEN.2, FAU_SEL.1(1), FPT_STM_(EXT).1

2.4.3 Encryption (FCS)

The TOE's wireless network encryption security function ensures that when an administrator has configured encryption, all network packet data payloads are encrypted with the scheme defined by the administrator for flows of information occurring in the RF domain. This allows for the TOE to provide end-to-end encryption capabilities between wireless clients, trusted APs and trusted nodes that reside within the TOE.The TOE also uses encryption to protect communication between TOE components, remote administration and communication with

external components such as the time server use for Controller clock updates. The APs, and Controllers all use FIPS 140-2 validated cryptomodules, see the TSS for details.

The SFRs covered by this security function are FCS_BCM_(EXT).1, FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM.2, FCS_CKM_(EXT).2, FCS_CKM.4, FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4), FCS_COP_(EXT).1

2.4.4 Identification & Authentication (FIA)

The TOE's Identification and Authentication security function provides I&A support of all wireless client hosts (WPA2 with preshared keys or WPA2 with 802.1X) connecting to the trusted wired network from the wireless network along with providing I&A for all administrators (username/password over HTTPS) prior to accessing TOE functionality. Additionally the TOE components authenticate each other via certificates used inCAPWAP, and Controllers authenticate environmental components with username and password (SNMPv3), with shared secrets (RADIUS with AES key wrap), and certificates (syslog over TLS, and NMSP to/from MSE).

The SFRs covered by this security function are FIA_AFL.1(1), FIA_ATD.1(1), FIA_ATD.1(2), FIA_UAU.1, FIA_UAU_(EXT).5(1), FIA_UID.2, FIA_USB.1(1), FIA_USB.1(2), FTA_TAB.1, FTP_ITT.1, FTP_ITC_(EXT).1, FTP_TRP.1

2.4.5 Information Flow Control (FDP)

The TOE's Information Flow Control security function provides control of information by enforcing the wireless encryption scheme that has been administratively configured. This encryption policy determines whether the APs and Controllers will encrypt and decrypt communications with wireless clients.

The SFR covered by this security function is FDP_PUD_(EXT).1

2.4.6 Self Protection (FPT)

The TOE controls actions carried out by a user by controlling a user session and the actions carried out during a user session. By maintaining and controlling a user session a user has with the TOE the TOE protects itself from the actions of unauthorized users.The hardware components of the TOE perform TSF tests during initial start-up of the component. These include the cryptographic module testing on the APs and Controllers. The APs and Controllers also perform an integrity check on the configuration files upon initial start up. The results for these tests are reported at the console upon boot up. The Controller and APs execute FIPS 140-2 power on self tests and conditional tests to ensure the proper operation of the cryptographic functionality.

The SFRs covered by this security function are FDP_RIP.1(1), FPT_ITT.1, FPT_TST_(EXT).1, FPT_TST.1(1), FPT_TST.1(2)

2.4.7 Wireless Intrusion Prevention System (IPS)

The wIPS functionality of the TOE provides IDS signature detection, generation of audit messages related to IDS signature detection, measurement and collection of wireless signal strength for us in wireless device location tracking (requires deployment of multiple APs and an MSE), as well as IPS functionality including containment of rogue wireless devices through transmission of targeted de-authentication attacks to prevent rogue devices from connecting to other wireless devices. The APs of the TOE support Adaptive wIPS functions,

which requires integration with MSE and NCS or WCS, but Adaptive wIPS is beyond the logical scope of this evaluation, so is not discussed further in this ST.

2.5 IT Environment Dependencies

The following section defines the IT Environment components relied upon by the TOE and not included in the physical boundary and therefore supplied by the IT Environment. The following section details the IT Environment supplied components and the dependencies on them from TOE components.

2.5.1 Wireless Client Hosts

All wireless client hosts connecting to the wired network from the wireless network are excluded from the TOE's physical boundary.

2.5.2 Administrator Management Hosts

The Controllerssupport remote access from a workstation via HTTPS or SSH (authenticated via RADIUS). Additionally, the controllers support serial access from a workstation, but that functionality is not permitted in the TOE evaluated configuration and would be authenticated to the local Management User database on the Controller. Administrator Management Hosts (HTTPS and SSH clients) are not included in the TOE's physical boundary.

2.5.3 Cisco Secure Access Control Server (ACS) and Cisco Identity Services Engine (ISE)

The Cisco Secure ACS version 5.x (hereafter referred to as the ACS) and Cisco Identity Services Engine (ISE) are different generations of products that provide centralized authentication, authorization and accounting. The ACS/ISE centralizes access control and accounting and enables ACS/ISE administrators the ability to configure user accounts from a centralized source. User account information includes support for wireless client hosts attempting to access the wired LAN and Controller administrator accounts for access to Controllers.

- Cisco Secure ACS is available in several platform configurations. Cisco Secure ACS version 5.x software is provided on either the Cisco 1120 Secure ACS 5.x Appliance or the Cisco 1121 Secure ACS 5.x Appliance. Additionally, Cisco Secure ACS version 5.2 software is available as a virtual appliance running VMware version ESX 3.5 or 4.0.
- Cisco ISE is available as a physical appliance on the 3300 series models (3315, 3355, and 3395, for small, medium, and large deployments respectively), and the Cisco Identity Services Engine virtual appliances supported on VMware ESX/ESXi 4.x, which should be run on hardware that equals or exceeds the characteristics of the physical appliances.
    - When ISE is used as the RADIUS server for Controller(s), the wireless client accounts can be defined within ISE, but ISE must be configured to defer (proxy) authentication of Controller administrators (Management Users) to a separate (second-tier) authentication server that is able to enforce lockout after failed login attempts. Those second-tier authentication servers could include Active Directory, LDAP, or an ACS server.

The Controller can be configured to require the APs to use the Controller's internal database of wireless user accounts, or to use either ACS or ISE to perform RADIUS authentication,

authorization, and accounting of wireless clients that connect to the TOE. When RADIUS is ued, the Controller is configured into ACS or ISE as a RADIUS client which enables APs to pass secure wireless user authentication requests through the Controller to a AAA server. IEEE 802.1X (which is part of IEEE 802.11i security) is used by the TOE to manage secure authentication of wireless clients into the TOE.

- APs enforce the 802.1X port access control, Controllers manage the 802.1X state machine and the AAA server terminates the 802.1X client authentication and resulting 802.11i key derivation.
- With 802.1X port access control, APs disallow all wireless packets transmitted from wireless hosts from entering the trusted wired network except for 802.1X EAP packets. APs forward 802.1X EAP packets to the Controller which passes them to the AAA server. Upon the completion of a successful 802.1X authentication session between a wireless client and the AAA server, access is granted to the trusted wired network.

The RADIUS protocol is used to communicate the 802.1X authentication information between the Controller and ACS/ISE. ACS/ISE verifies the username and password using the user databases it is configured to query, such as the local ACS/ISE user database, or a RADIUS store. ACS/ISE returns a success or failure response via the Controller to the AP, which permits or denies user access based on the response it receives. When the user authenticates successfully, ACS/ISE sends a set of authorization attributes to the AP. If RADIUS accounting is also configured the AP then begins forwarding wireless user accounting information to ACS/ISE for logging.

When the user has successfully authenticated, a set of session attributes can be sent to the AAA client to provide additional security and control of privileges, otherwise known as authorization. These attributes might include the IP address pool, access control lists (ACLs), or type of connection.

ACS or ISEcan also be used for authentication, authorization and accounting for administrators of the TOE (Management Users only, not SNMPv3 Users). When ISE is used as a directly-accessible (first-tier) RADIUS server for any Controller(s), ISE must be configured to defer (proxy) authentication and authorization requests for those accounts to a separate (second-tier) authentication server that is able to enforce lockout after failed login attempts. Those second-tier authentication servers could include Active Directory, LDAP, or an ACS server. The Controller's Management Users can be configured through ACS for authentication and authorization using RADIUS, and controller TACACS+ accounting can be used by ACS/ISE for logging actions performed by Management Users on the Controller.

- The network communication interface between ACS/ISE and the Controller is controlled and protected with the use of the RADIUS protocol for non-crypto client related communications and AES RADIUS key wrap for FIPS compliant transfer of the 802.11i PMK to the controller.
- The ACS/ISE controls and mediates all actions that occur through these interfaces and make sure that the enforcement functions (those dealing with access control of the interfaces) are invoked and succeed before allowing any other mediated action to occur with any of its other security functions. Through these mediations and access controls of the interfaces of the ACS/ISE the ACS/ISE achieves non-bypassability.

2.5.4 Cisco Wireless Control System (WCS) and Network Control System (NCS)

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.

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).

2.5.5 Cisco Mobility Services Engine (MSE)

The Cisco Mobility Services Engine (MSE) is an appliance supporting a suite of mobility services programs. It supports the TOE's wIPS functionality by sending wIPS profiles to Controllers for further distribution to APs and receiving wIPS data from the Controllers.

2.5.6 Syslog Server

The syslog server can be one of any syslog server that supports receiving syslog over TLS, and is capable of filtering audit messages upon receipt. Two compatible software syslog daemons are Kiwi Syslog and Syslog-ng. Use of a syslog server can provide centralized location for storage of audit data forwarded from the WLAN Controller (and optionally from other IT Environment components) and support filtering of the audit data.

2.6 Security Functionality Not Included in the TOE's Logical Boundary

The following section defines functionality included in the TOE's physical boundary but not included in the TOE's logical boundary or claimed in the TOE's security functionality.

2.6.1 Identification & Authentication

ACS supports many different I&A protocols, and only a subset are included within the TOE. Table 7 lists the I&A methods included in the TOE's physical boundary (AAA Client and AAA Server implementation) and identifies which are not supported in the evaluated configuration. The I&A methods omitted are not deemed secure enough to use in the evaluated configuration.

Table 6ACS/ISE I&A Methods Included in the TOE Physical Boundary

	I&A Wireless Agent Host	Administrative Hosts
ASCII/PAP	Not supported	Not supported
CHAP	Not supported	Supported
MS-CHAP	Not supported	Not supported
LEAP	Not supported	Not supported
EAP-MD5	Not supported	Supported

EAP-TLS	Supported	Not supported
EAP-MSCHAPv2	Supported	Not supported
EAP-GCT	Supported	Not supported
EAP-FAST	Supported	Not supported
WPA2-PSK	Supported	Not supported
HTTPS	Not supported	Supported

2.6.1.1 Controller Functionality Excluded from the Logical Boundary

Controller TACACS+ authentication and authorization are not included in the Logical Boundary of the TOE. Controller TACACS+ accounting is allowed in the evaluated configuration but would be redundant to syslog messages generated by the Controller.

2.7 TOE Evaluated Configuration

The TOE's evaluated configuration requires one or more Controllersplus one or more of APs.

Additionally, the following list itemizes the evaluated configuration requirements:

1) The ACS or ISE is installed and configured to support authentication for all installed Controllers.
2) The Syslog server supporting syslog over TLS is operational on a Syslog Host.
3) The Controllers are configured with SNMPv3 enabled and SNMPv1 and SNMPv2 disabled.
4) AES RADIUS key wrapis enabled between the Controllers and ACS or ISE.
5) Telnet is disabled on the Controllers.
6) RADIUS is used for authentication of wireless clients.
7) RADIUS is used for authentication and authorization of the Controlleradministrator.
8) TACACS+ is used for accounting of Controlleradministrator actions on the Controller.
9) All APs are CAPWAP APs.
10) A TFTP client is included locally on the Controller for downloading image bundle updates.FTP shall not be used.
11) A separate NTP server is included in the IT environment for use with the ACS, MSE, WCS or NCS, and the syslog components.
12) Wireless administration is disabled on the TOE.

2.8 TOE Component Communication Methods

The evaluated configuration of the TOE consists of several components that work together to provide the TOE functionality described in this ST. Table 8 details the secure communication methods used between TOE components:

Table 7TOE Component Communication Methods

To/From a TOE Component	Communication Method
Between Controller and ACS	RADIUS withAES Key Wrap
Between Controller and APs	CAPWAP
Between Controllers	EoIP tunnels using SSL
Between APs	Authenticated AP to AP wireless neighbor messages (AES encrypted)

3 Conformance Claims

3.1 Protection Profile Reference

This ST claims conformance to the US Government Wireless Local Area Network (WLAN) Access System Protection Profile (PP) For Basic Robustness Environments, version 1.1, July 25, 2007 (pp_wlan_as_br_v1.1)

3.2 Protection Profile Refinements

This ST makes the following refinements to the PP referenced above:

1) The term “FIPS 140-1/2” was replaced with the term “FIPS 140-2” to reflect the validation scheme under which all TOE cryptomodules were evaluated,
2) The Table associated with FAU_GEN.1(1) was refined in the following ways:
    1. to indicate iteration numbers for FIA_ATD.1, and FIA_USB.1;
    2. to add additional rows added via refinement for FCS_BCM_(EXT).1, FCS_CKM.2, FCS_COP.1(1), FCS_COP.1(2), FMT_SMF.1(1), FMT_SMF.1(2), FMT_SMF.1(3), FPT_ITT.1, FTP_TST_(EXT).2 and FTA_TAB.1;
    3. to change the FIA_UID.1 row to FIA_UID.2;
    4. to remove FMT_REV.1; and
    5. to correct typos FDP_PUD.1_(EXT) to FDP_PUD_(EXT).1 and 2nd FCS_CKM.1(1) to FCS_CKM.1(2)
3) FCS_BCM_(EXT).1.2 was deleted to bring the ST in conformance with current cryptography policy as exemplified in the common management requirements PP (draft).
4) FCS_CKM.1.1(2) changed 128 bit symmetric strength to 2048 bit modulus (to match FCS_COP.1(2)).
5) FCS_COP.1(3) was refined to include support for SHA-1 for compatibility with existing protocols (DTLS/TLS,SNMPv3).

6) FDP_PUD_(EXT).1 was updated to remove the word “authenticated” from both bullets as the encryption happens prior to authentication and FCS_COP_(EXT).2 was changed to FCS_COP.1(1).

7) FIA_AFL.1.2(2) was refined to replace “TSF” with “TOE IT Environment”.

8) FIA_USB.1 was refined to include the word “administrator” prior to user, to specify that this is for the administrative TOE users. Also, the iteration identifier of (1) was added to it, because a second iteration was added for wireless users.

9) FMT_MOF.1(1) was refined to specify administrators “with read-write permission.”

10) FMT_MOF.1(2) was refined to specify administrators “with read-write permission.”

11) FMT_MOF.1(3) was refined: to specify administrators “with read-write permission,” and to remove the bullet about setting an authentication failure limit because that function is enforced by and configured on the RADIUS server in the IT Environment.

12) FMT_MOF.1(4) on the IT Environment was refined to add all the available selections from CC Part 2 “disable, enable, modify the behaviour of”. Without all those abilities, the “security administrator of the authorized IT entity” wouldn’t be able to do what’s defined in the iterations of FMT_MTD.1 on the IT Environment.

13) FPT_TST.1(1) and FPT_TST.1(2) were modified to change the role from cryptographic administrator to administrator.

14) FTP_TRP.1 was refined to change the two mentions of “wireless users” to “wireless client devices” as the path is not truly to the user.

15) The wording of the rationale to support mapping OE.MANAGE to T.TSF_COMPROMISE was adjusted to reflect proper focus on the IT Environment and functions. Wording was changed from, “…the administrator can view security relevant audit events,” to, “…the TOE operational environment limits access to management functions to the administrator.”

16) The wording of rationale to support mapping of O.DOCUMENTED_DESIGN to T.POOR_DESIGN was updated to reference ADV_TDS instead of ADV_RCR to be consistent with CC v3.1.

17) The wording of O.TIME_STAMPS was changed to reflect the fact that the TOE has its own hardware clock and it’s that hardware clock that’s used when applying timestamps to audit records, while the clock itself can be updated by an administrator, or an administratively-defined source of automated clock updates.

3.3 Protection Profile Additions

3.3.1 TOE Security Problem Definition Additions

- The TOE for this ST contains functionality for Wireless IPS (wIPS) specific audit events. These are captured in a threat, policy, objective and explicitly stated SFR. This ST claims conformance to the PP listed above with the following additions for the wIPS functionality:

T.WIRELESS_INTRUSION	Rogue APs and malicious wireless clients may attempt to subvert the wireless network.

P.WIRELESS_LOCATION_POLICY	In concordance with the DOD 8100.2 Wireless LAN Policy, the TOE will supportlocation tracking for all 802.11 devices transmitting within the RF environment.
O.WIPS_FUNCTIONS	The TOE will provide the capability to identify wIPS events, create records based on the observed actions from specific IT System resources; and deny unauthorized traffic and contain rogue access points and clients.

- The TOE evaluated configuration requires that wireless clients that are configured to allow storage of TOE authentication credentials be physically and/or technologically protected such that an unauthorized user cannot attempt to use the stored credentials.

T.CLIENT_INSECURE	An unauthorised user may attempt to gain access to an authorised client with saved credentials and attempt to subvert the wireless network.
OE.CLIENT_PROTECT	Wireless clients and/or their hosts will be configured to not allow unauthorized access to networking services of the wireless client or to stored TOE authentication credentials.
A.CLIENT_PROTECT	Wireless clients and/or their hosts are configured to not allow unauthorized access to networking services of the wireless client or to stored TOE authentication credentials.

3.3.2 TOE Security Functional Requirement Additions

The SFRs that were added to the set in the Protection Profile for the TOE are listed in this section.

TheIPS_SDC_(EXT).1, IPS_ANL_(EXT).1, and IPS_RCT_(EXT).1SFRswere added to cover the O.WIPS_FUNCTIONS.

The FIA_USB.1(2) SFR was added to cover the user subject binding for wireless clients.

FPT_ITT.1 was added to describe the protection of TSF data in transmission between the Controller and APs.

IPS_ANL_(EXT).1 was added to cover the wIPS event analysis function of the AP component, which functions as a precursor to wIPS audit generation (as referenced from the Table of auditable events in FAU_GEN.1(1)),and wIPS reaction (IPS_RCT_(EXT).1). The format for this SFR was drawn from, but not claiming conformance to, the Intrusion Detection System System For Basic Robustness Environments, Version 1.7, July 25, 2007.

IPS_RCT_(EXT).1 was added to cover the wIPS reaction functions of the TOE to drop traffic or de-authenticate unauthorized wireless access points and clients. The format for this SFR was drawn from, but not claiming conformance to, the Intrusion Detection System System For Basic Robustness Environments, Version 1.7, July 25, 2007.

4 Security Problem Definition

This section 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. Policies are identified as P.policy with "policy" specifying a unique name.

The Security Problem Definition described below is consistent with that of the PP except as noted above in the listing of TOE Security Problem Definition Additions.

4.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's IT 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. The assumptions are identical to the assumptions itemized in [WLANPP].

Table 8TOE Assumptions

Name	Assumption
A.NO_EVIL	Administrators are non-hostile, appropriately trained and follow all administrator guidance.
A.NO_GENERAL_PURPOSE	There are no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on 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.TOE_NO_BYPASS	Wireless clients are configured so that information cannot flow between a wireless client and any other wireless client or host networked to the TOE without passing through the TOE.
A.CLIENT_PROTECT	Wireless clients and/or their hosts are configured to not allow unauthorized access to networking services of the wireless client or to stored TOE authentication credentials.

4.2 Threats

Table 10 lists the threats addressed by the TOE and the IT Environment. The threats are identical to the threats identified in [WLANPP]. For the threats below, attackers are assumed to be of low attack potential.

Table 9Threats

Threat Name	Threat Definition
T.ACCIDENTAL_ADMIN_ERROR	An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.
T.ACCIDENTAL_ CRYPTO_COMPROMISE	A user or process may cause key, data or executable code associated with the cryptographic functionality to be inappropriately accessed (viewed, modified, or deleted), thus compromising the cryptographic mechanisms and the data protected by those mechanisms.
T.MASQUERADE	A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.
T.POOR_DESIGN	Unintentional errors in requirements specification or design of the TOE may occur, leading to flaws that may be exploited by a casually mischievous user or program.
T.POOR_IMPLEMENTATION	Unintentional errors in implementation of the TOE design may occur, leading to flaws that may be exploited by a casually mischievous user or program.
T.POOR_TEST	The developer or tester performs insufficient tests to demonstrate that all TOE security functions operate correctly (including in a fielded TOE) may occur, resulting in incorrect TOE behavior being undiscovered leading to flaws that may be exploited by a mischievous user or program.
T.RESIDUAL_DATA	A user or process may gain unauthorized access to data through reallocation of TOE resources from one user or process to another.
T.TSF_COMPROMISE	A user or process may cause, through an unsophisticated attack, TSF data, or executable code to be inappropriately accessed (viewed, modified, or deleted).
T.UNATTENDED_SESSION	A user may gain unauthorized access to an unattended session.
T.UNAUTHORIZED_ACCESS	A user may gain access to services (either on the TOE or by sending data through the TOE) for which they are not authorized according to the TOE security policy.
T.UNAUTH_ADMIN_ACCESS	An unauthorized user or process may gain access to an administrative account.

T.WIRELESS_INTRUSION	Rogue APs and malicious wireless clients may attempt to subvert the wireless network.
T.CLIENT_INSECURE	An unauthorised user may attempt to gain access to an authorised client with saved credentials and attempt to subvert the wireless network.

4.3 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. Table 11 identifies the organizational security policies applicable to the WLAN.

Table 10Organizational Security Policies

Policy Name	Policy Definition
P.ACCESS_BANNER	The TOE shall display an initial banner for administrator logins describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.
P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE.
P.CRYPTOGRAPHY	The TOE shall provide cryptographic functions for its own use, including encryption/decryption operations.
P.CRYPTOGRAPHY_VALIDATED	Only NIST FIPS validated cryptography (methods and implementations) are acceptable for key management (i.e.; generation, access, distribution, destruction, handling, and storage of keys) and cryptographic services (i.e., encryption, decryption, signature, hashing, key exchange, and random number generation services).
P.ENCRYPTED_CHANNEL	The TOE shall provide the capability to encrypt/decrypt wireless network traffic between the TOE and those wireless clients that are authorized to join the network.
P.NO_AD_HOC_NET WORKS	In concordance with the DOD Wireless Policy, there will be no ad hoc 802.11 or 802.15 networks allowed.
P.WIRELESS_LOCATION_POLICY	In concordance with the DOD 8100.2 Wireless LAN Policy, the TOE will supportlocation tracking for all 802.11 devices transmitting within the RF environment.

5 Security Objectives

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

Objectives of the TOE are identified 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.

5.1 Security Objectives for the TOE

Table 12identifies 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 11Security Objectives for the TOE

Name	TOE Security Objective
O.ADMIN_GUIDANCE	The TOE will provide administrators with the necessary information for secure management.
O.AUDIT_GENERATION	The TOE will provide the capability to detect and create records of security-relevant events associated with users.
O.CONFIGURATION_IDENTIFICATION	The configuration of the TOE is fully identified in a manner that will allow implementation errors to be identified, corrected with the TOE being redistributed promptly.
O.CORRECT_TSF_OPERATION	The TOE will provide the capability to verify the correct operation of the TSF.
O.CRYPTOGRAPHY	The TOE shall provide cryptographic functions to maintain the confidentiality and allow for detection of modification of user data that is transmitted between physically separated portions of the TOE, or outside of the TOE.
O.CRYPTOGRAPHY_VALIDATED	The TOE will use NIST FIPS 140-2 validated cryptomodules for cryptographic services implementing NIST-approved security functions and random number generation services used by cryptographic functions.
O.DISPLAY_BANNER	The TOE will display an advisory warning prior to establishing an administrator session regarding use of the TOE prior to permitting the use of any TOE services that requires authentication.

O.DOCUMENTED_DESIGN	The design of the TOE is adequately and accurately documented.
O.WIPS_FUNCTIONS	The TOE will provide the capability to identify wIPS events, create records based on the observed actions from specific IT System resources, and deny unauthorized traffic and contain rogue access points and clients.
O.MANAGE	The TOE will provide functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
O.MEDIATE	The TOE must mediate the flow of information to and from wireless clients communicating via the TOE RF Transmitter/Receiver in accordance with its security policy.
O.PARTIAL_FUNCTIONAL_TESTING	The TOE will undergo some security functional testing that demonstrates the TSF satisfies some of its security functional requirements.
O.RESIDUAL_INFORMATION	The TOE will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated.
O.SELF_PROTECTION	The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure through its own interfaces.
O.TIME_STAMPS	The TOE shall obtain reliable clock updates from the IT Environment and retain the capability for the administrator to set the time used for timestamps.
O.TOE_ACCESS	The TOE will provide mechanisms that control a user's logical access to the TOE.
O.VULNERABILITY_ANALYSIS	The TOE will undergo some vulnerability analysis to demonstrate the design and implementation of the TOE does not contain any obvious flaws.

5.2 Security Objectives for the Environment

The assumptions identified above are incorporated as security objectives for the environment. They levy additional requirements on the environment, which are largely satisfied through procedural or administrative measures. Table 13 identifies the security objectives for the environment.

Table 12Security Objectives for the Environment

Name	IT Environment Security Objective

OE.AUDIT_PROTECTION	The IT Environment will provide the capability to protect audit information and the authentication credentials.
OE.AUDIT_REVIEW	The IT Environment will provide the capability to selectively view audit information.
OE.MANAGE	The TOE IT environment will augment the TOE functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
OE.NO_EVIL	Sites using the TOE shall ensure that administrators are non-hostile, appropriately trained and follow all administrator guidance.
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the TOE.
OE.PHYSICAL	The environment provides physical security, commensurate with the value of the TOE and the data it contains.
OE.PROTECT_MGMT_COMMS	The IT environment shall protect the transport of audit records to the audit server, remote network management, and authentication server communications with the TOE and time service in a manner that is commensurate with the risks posed to the network.
OE.RESIDUAL_INFORMATION	The TOE IT Environment will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated.
OE.SELF_PROTECTION	The IT environment will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure through its own interfaces.
OE.TOE_ACCESS	The IT environment will provide mechanisms that support the TOE in providing user's logical access to the TOE.
OE.TOE_NO_BYPASS	Wireless clients are configured so that information cannot flow between a wireless client and any other wireless client or host networked to the TOE without passing through the TOE.
OE.TIME_STAMPS	The TOE IT environment shall provide reliable time stamps and the capability for the administrator to set the time used for these time stamps.
OE.CLIENT_PROTECT	Wireless clients and/or their hosts will be configured to not allow unauthorized access to networking services of the wireless client or to stored TOE authentication credentials.

6 Security Requirements

This section identifies the Security Functional Requirements for the TOE and for the IT Environment. The Security Functional Requirements included in this section are derived verbatim from Part 2 of the *Common Criteria for Information Technology Security Evaluation*, version 3.1 revision 3.

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.

- Assignments: indicated by showing the value in square brackets [Assignment_value].
- Selections: indicated by *italicized text*.
- Assignments within selections: indicated in italics within the [*greater brackets*].
- Refinements: indicated in **bold text** with the addition of details and bold text with strikethrough (**~~refinement~~**) when details are deleted.

Multiple Security Functional Requirement instances (iterations) are identified by the Security Functional Requirement component identification followed by the instance number in parenthesis (e.g.,FCS_CKM.1(1)) and the Security Functional Requirement element name followed by the instance number in parenthesis (e.g., FCS_CKM.1.1(1)).

Operations already completed within the Protection Profile (US Government Wireless Local Area Network (WLAN) Access System Protection Profile for Basic Robustness Environments, July 25 2007, version 1.1) will not be repeated here in the Security Target. Please see the PP for these details. Therefore, the SFR operations from CC Part 2 that have already been completed in the PP will not show the font conventions in the bullet list above.

Extended SFRs are identified by having a label 'Extended component SFR for the TOE' after the requirement name for TOE SFRs.

The TOE security requirements described below are consistent with those of the WLAN PP except as noted in the listing of TOE Security Functional Requirement Additions in section 3 above.

6.1 TOE Security Functional Requirements

This section identifies the Security Functional Requirements for the TOE. The TOE Security Functional Requirements that appear Table 13 are described in more detail in the following subsections.

Table 13TOE Security Functional Requirements

Functional Component	
FAU_GEN.1**(1)**	Audit data generation
FAU_GEN.2~~(1)~~	User identity association
FAU_SEL.1(1)	Selective audit
FCS_BCM_(EXT).1	Extended: Baseline Cryptographic Module
FCS_CKM.1(1)	Symmetric Cryptographic Key Generation

FCS_CKM.1(2)	Asymmetric Cryptographic key generation
FCS_CKM.2	Cryptographic Key Distribution
FCS_CKM_(EXT).2	Extended: Cryptographic Key Handling and Storage
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1(1)	Cryptographic Operation (symmetric-encryption)
FCS_COP.1(2)	Cryptographic Operation (cryptographic-signatures)
FCS_COP.1(3)	Cryptographic Operation (hashing)
FCS_COP.1(4)	Cryptographic Operation (cryptographic key agreement)
FCS_COP_(EXT).1	Extended: Random Number Generation
FDP_PUD_(EXT).1	Extended: Protection of User Data
FDP_RIP.1(1)	Subset residual information protection
FIA_AFL.1(1)	Administrator Authentication failure handling
FIA_ATD.1(1)	Administrator attribute definition
FIA_ATD.1(2)	User attribute definition
FIA_UAU.1	Timing of local authentication
FIA_UAU_(EXT).5(1)	Extended: Multiple authentication mechanisms
FIA_UID.2	User identification before any action
FIA_USB.1**(1)**	User-subject binding **(Administrator)**
FIA_USB.1(2)	**User-subject binding (Wireless User)**
FMT_MOF.1(1)	Management of cryptographic security functions behavior
FMT_MOF.1(2)	Management of audit security functions behavior
FMT_MOF.1(3)	Management of authentication security functions behavior
FMT_MSA.2	Secure security attributes
FMT_MTD.1(1)	Management of Audit pre-selection data
FMT_MTD.1(2)	Management of Authentication data (Administrator)
FMT_MTD.1(3)	Management of Authentication data (User)

FMT_SMF.1(1)	Specification of Management Functions (Cryptographic Function)
FMT_SMF.1(2)	Specification of Management Functions (TOE Audit Record Generation)
FMT_SMF.1(3)	Specification of Management Functions (Cryptographic Key Data)
FMT_SMR.1(1)	Security roles
FPT_ITT.1	**Basic internal TSF data transfer protection**
FPT_STM_(EXT).1	Extended: Reliable time stamps
FPT_TST_(EXT).1	Extended: TSF Testing
FPT_TST.1(1)	TSF Testing (for cryptography)
FPT_TST.1(2)	TSF Testing (for key generation components)
FTA_SSL.3	TSF-initiated termination
FTA_TAB.1	Default TOE access banners
FTP_ITC_(EXT).1	Extended: Inter-TSF trusted channel
FTP_TRP.1	Trusted Path
IPS_SDC_(EXT).1	**wIPS Data Collection**
IPS_ANL_(EXT).1	**wIPS Analysis**
IPS_RCT_(EXT).1	**wIPS Reaction**

6.1.1 FAU_GEN.1(1) Audit Data Generation

FAU_GEN.1.1(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 minimum level of audit; and

c. [additional auditable events shown in column 2 of **Table 14**].

Table 14SFR Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1**(1)**	None	None
FAU_GEN.2	None	None

FAU_SEL.1**(1)**	All modifications to the audit configuration that occur while the audit collection functions are operating.	The identity of the Administrator performing the function.
FCS_BCM_(EXT).1	**None**	**None**
FCS_CKM.1(1)	Generation of a key.	The identity of the Administrator performing the function.
FCS_CKM.1(~~1~~**2**)	Generation of a key.	The identity of the Administrator performing the function.
FCS_CKM.2	**Success and Failure of key distribution.**	**None**
FCS_CKM_(EXT).2	Error(s) detected during cryptographic key transfer	If available the authentication credentials of subjects with which the invalid key is shared.
FCS_CKM.4	Destruction of a cryptographic key	If available the identity of the Administrator performing the function
FCS_COP.1(1),(2),(3),(4)	None	None
FCS_COP_(EXT).1	None	None
FDP_PUD~~.1_(EXT)~~ **_(EXT).1**	Enabling or disabling TOE encryption of wireless traffic	The identity of the administrator performing the function.
FDP_RIP.1**(1)**	None	None
FIA_AFL.1(1)	The reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g., disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g., re-enabling of a terminal	None
FIA_ATD.1**(1),(2)**	None	None
FIA_UAU.1	Use of the authentication mechanism (success or failure)	User identity - the TOE SHALL NOT record invalid passwords in the audit log.
FIA_UAU_(EXT).5(1)	Failure to receive a response from the remote authentication server	Identification of the Authentication server that did not reply

FIA_UID.2	~~None~~ **Unsuccessful use of the user identification mechanism,**	~~None~~ **user identity provided**
FIA_USB.1**(1),(2)**	Unsuccessful binding of user security attributes to a subject	None
FMT_MOF.1(1)	Changing the TOE encryption algorithm including the selection not to encrypt communications	Encryption algorithm selected (or none)
FMT_MOF.1(2)	Start or Stop of audit record generation	None
FMT_MOF.1(3)	Changes to the TOE remote authentication settings; Changes to the threshold of failed authentication attempts; Changes to the session lock timeframe	The identity of the administrator performing the function.
FMT_MSA.2	All offered and rejected values for security attributes	None
FMT_MTD.1(1)	Changing the TOE audit pre-selection data	None
FMT_MTD.1(2) FMT_MTD.1(3)	Changing the TOE authentication credentials	None – the TOE SHALL NOT record authentication credentials in the audit log.
FMT_SMF.1(1)	**Use of the (cryptographic) management functions**	**None**
FMT_SMF.1(2)	**Use of the (audit record generation) management functions**	**None**
FMT_SMF.1(3)	**Use of the (crypto key data) management functions**	**None**
~~**FMT_REV.1**~~	~~**Unsuccessful revocation of security attributes.**~~	~~**None**~~
FMT_SMR.1(1)	Modifications to the group of users that are part of a role	None
FPT_ITT.1	**The detection of modification of TSF data**	**None**
FPT_STM_(EXT).1	Changes to the time	None
FPT_TST_(EXT).1	Execution of the self test	Success or Failure of test
FPT_TST.1**(1)**	Execution of the self test	Success or Failure of test

FPT_TST.~~2~~**1(2)**	Execution of the self test	Success or Failure of test
FTA_SSL.3	TSF Initiated Termination	Termination of an interactive session by the session locking mechanism.
FTA_TAB.1	**None**	**None**
FTP_ITC_(EXT).1	Initiation/Closure of a trusted channel; **Failure of the trusted channel functions.**	Identification of the remote entity with which the channel was attempted/created; Success or failure of the event**;** **Identification of the initiator and target of failed trusted channel functions.**
FTP_TRP.1	Initiation of a trusted channel **Failures of the trusted path functions.**	Identification of the remote entity with which the channel was attempted/created; Success or failure of the event**;** **Identification of the user associated with all trusted path failures, if available.**

FAU_GEN.1.2(1) 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 (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the ~~**PP/**~~ST, information specified in column three of **Table 14.**

6.1.2 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.

Application note: Actions of Management Usersand SNMPv3 Usersare identified in audit messages by their username though Management Users are human users, and SNMPv3 Users are remote entities such as NCS, WCS, or MSE servers.

6.1.3 FAU_SEL.1(1) Selective Audit

FAU_SEL.1.1(1) The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

a) event type.

6.1.4 FCS_BCM_(EXT).1 Extended: Baseline Cryptographic Module

FCS_BCM_(EXT).1.1 All FIPS-approved cryptographic functions implemented by the TOE shall be implemented in a crypto-module that is FIPS 140-2 validated, and perform the specified cryptographic

functions in a FIPS-approved mode of operation. The FIPS 140-2 validation shall include an algorithm validation certificate for all FIPS-approved cryptographic functions implemented by the TOE.

~~**FCS_BCM_(EXT).1.2 All cryptographic modules implemented in the TOE [As a combination of hardware and software shall have a minimum overall rating of FIPS PUB 140-2, Level 1 and also meet FIPS PUB 140-2, Level 3 for the following: Cryptographic Module Ports and Interfaces; Roles, Services and Authentication; Cryptographic Key Management; and Design Assurance.]**~~

6.1.5 FCS_CKM.1(1) Cryptographic Key Generation (for symmetric keys)

FCS_CKM.1.1(1) The TSF shall generate symmetric cryptographic keys using a FIPS-Approved Random Number Generator as specified in FCS_COP_(EXT).1, and provide integrity protection to generated symmetric keys in accordance with NIST SP 800-57 "Recommendation for Key Management" Section 6.1.

6.1.6 FCS_CKM.1(2) Cryptographic Key Generation (for asymmetric keys)

FCS_CKM.1.1(2) The TSF shall generate asymmetric cryptographic keys in accordance with the mathematical specifications of the FIPS-approved or NIST-recommended standard [FIPS 186-3], using a domain parameter generator and**[**a FIPS-Approved Random Number Generator as specified in FCS_COP_(EXT).1] in a cryptographic key generation scheme that meets the following:

- The TSF shall provide integrity protection and assurance of domain parameter and public key validity to generated asymmetric keys in accordance with NIST SP 800-57 "Recommendation for Key Management" Section 6.1.
- Generated key strength shall ~~**be equivalent to, or greater than, a symmetric key strength of 128 bits using conservative estimates.**~~**2048 bits or higher**.

6.1.7 FCS_CKM.2 Cryptographic Key Distribution

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method *Automated (Electronic) Method* that meets the following:

a) NIST Special Publication 800-57, "Recommendation for Key Management" Section 8.1.5

b) NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"

6.1.8 FCS_CKM_(EXT).2 Extended: Cryptographic Key Handling & Storage

FCS_CKM_(EXT).2.1 The TSF shall perform a key error detection check on each transfer of key (internal, intermediate transfers).

FCS_CKM_(EXT).2.2 The TSF shall store persistent secret and private keys when not in use in encrypted form or using split knowledge procedures.

FCS_CKM_(EXT).2.3 The TSF shall destroy non-persistent cryptographic keys after a cryptographic administrator-defined period of time of inactivity.

FCS_CKM_(EXT).2.4 The TSF shall prevent archiving of expired (private) signature keys.

6.1.9 FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a cryptographic key zeroization method that meets the following:

a) Key zeroization requirements of FIPS PUB 140-2, “Security Requirements for Cryptographic Modules”

b) Zeroization of all plaintext cryptographic keys and all other critical cryptographic security parameters shall be immediate and complete.

c) The TSF shall zeroize each intermediate storage area for plaintext key/critical cryptographic security parameter (i.e., any storage, such as memory buffers, that is included in the path of such data) upon the transfer of the key/critical cryptographic security parameter to another location.

d) For non-volatile memories other than EEPROM and Flash, the zeroization shall be executed by overwriting three or more times using a different alternating data pattern each time.

e) For volatile memory and non-volatile EEPROM and Flash memories, the zeroization shall be executed by a single direct overwrite consisting of a pseudo random pattern, followed by a read-verify.

6.1.10 FCS_COP.1(1) Cryptographic Operation (Data Encryption/Decryption)

FCS_COP.1.1(1) The cryptomodule**s** shall perform encryption and decryption using the FIPS-approved security function AES algorithm operating in [ECB, CBC, CCMP, CMAC and Key Wrap modes] and cryptographic key size of *128 bits*.

6.1.11 FCS_COP.1(2) Cryptographic Operation (Cryptographic Signatures)

FCS_COP.1.1(2) The TSF shall perform cryptographic signature services using the FIPS-approved security function**s**
Digital Signature Algorithm (DSA) with a key size (modulus) of [2048 bits],

RSA Digital Signature Algorithm (rDSA) with a key size (modulus) of [2048 bits]

that meets NIST Special Publication 800-57, "Recommendation for Key Management."

6.1.12 FCS_COP.1(3) Cryptographic Operation (Hashing)

FCS_COP.1.1(3) The TSF shall perform cryptographic hashing services using the FIPS-approved security function Secure Hash Algorithm and message digest size of ***160 bits or*** *256 bits*.

6.1.13 FCS_COP.1(4) Cryptographic Operation (Cryptographic Key Agreement)

FCS_COP.1.1(4) The TSF shall perform cryptographic key agreement services using the FIPS-approved security function as specified in NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" *[Diffie-Hellman] and cryptographic key sizes (modulus) of [2048 bits]* that meets NIST Special Publication 800-57, "Recommendation for Key Management."

6.1.14 FCS_COP_(EXT).1 Extended: Random Number Generation

FCS_COP_(EXT).1 The TSF shall perform all random number generation (RNG) services in accordance with a FIPS-approved RNG [X9.31 or FIPS 186-2]seeded by *entropy gathered during startup via an entropy gathering process.*

FCS_COP_(EXT).1.2 The TSF shall defend against tampering of the random number generation (RNG)/ pseudorandom number generation (PRNG) sources.

6.1.15 FDP_PUD_(EXT).1 Extended: Protection of User Data

FDP_PUD_(EXT).1.1 When the administrator has enabled encryption**of wireless client data during transmission**, the TSF shall:

- encrypt authenticated user data transmitted to a wireless client from the radio interface of the wireless access system using the cryptographic algorithm(s) specified in ~~**FCS_COP_(EXT).2**~~**FCS_COP.1(1)**;
- decrypt authenticated user data received from a wireless client by the radio interface of the wireless access system using the cryptographic algorithm(s) specified in ~~**FCS_COP_(EXT).2**~~**FCS_COP.1(1)**.

Application Note This requirement helps support carrying out end to end security for this wireless solution. User data is protected in transit from wireless client to the trusted boundary of the access points (the APs) where it then is decrypted and enters the protected wired network.

6.1.16 FDP_RIP.1(1) Subset Residual Information Protection

FDP_RIP.1.1(1) The TSF shall ensure that any previous information content of a resource is made unavailable upon *the allocation of the resource to* the following objects: network packet objects.

6.1.17 FIA_AFL.1(1) Administrator Authentication Failure Handling

FIA_AFL.1.1(1) The TSF shall **defer authentication of remote administrators to a RADIUS server for the IT Environment to**detect when an administrator configurable positive integer within the range [1 to 10] of unsuccessful authentication attempts occur related to remote administrators logging on to the WLAN access system.

FIA_AFL.1.2(1) When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall prevent remote login by administrators **by continuing to defer authentication of remote administrators to a RADIUS server**until an action is taken by a local Administrator **or a RADIUS administrator**.

Application note: Authentication of Management Users is deferred to a RADIUS server for authentication failure handling. This requirement is not applicable to administrative authentication at the SNMPv3 interface of the Controller.

6.1.18 FIA_ATD.1(1) Administrator Attribute Definition

FIA_ATD.1.1(1) The TSF shall maintain the following minimum list of security attributes belonging to individual administrators: password, [username, access mode].

Application note: An “access mode” of ReadOnly, or ReadWrite is assigned to each SNMPv3 User account. SNMPv3 User accounts are the only administrative accounts stored and used locally in

the Controller, attributes for Management Users are stored in the RADIUS server.

6.1.19 FIA_ATD.1(2) User Attribute Definition

FIA_ATD.1.1(2) The TSF shall maintain the following minimum list of security attributes belonging to individual remotely authenticated users: [

- Using EAP-TLS: client's device certificate
- Using EAP-FAST without client certificate: username and password
- Using EAP-FAST with client certificate: client's device certificate
- Using EAP-FAST with EAP-GTC: username and PAC (Protected Access Credentials)
- Using EAP-MSCHAPv2 without client certificate: username and password
- Using EAP-MSCHAPv2 with client certificate: client's device certificate
- Using WPA2-PSK: Passphrase (ASCII or Hex)]

6.1.20 FIA_UAU.1 Timing of Local Authentication

FIA_UAU.1.1 The TSF shall allow [login attempts] on behalf ofusers to be performed before the user is authenticated.

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

6.1.21 FIA_UAU_(EXT).5(1)Extended: Multiple Authentication Mechanisms

FIA_UAU_(EXT).5.1(1) The TSF shall provide local authentication, and a remote authentication mechanism to perform user authentication.

FIA_UAU_(EXT).5.2(1) The TSF shall, at the option of the administrator, invoke the remote authentication mechanism for administrators and wireless LAN users.

Application note: Local authentication mechanisms are used for all authentication of SNMPv3 Users, and optionally for authentication of wireless users. Remote authentication is used for all authentication of Management Users connecting to the SSH CLI or the TLS GUI, and optionally for authentication of wireless users.

6.1.22 FIA_UID.2 User Identification Before any Action

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

6.1.23 FIA_USB.1(1) User-Subject Binding (Administrator)

FIA_USB.1.1(1) The TSF shall associate the following **administrator** user security attributes with subjects acting on the behalf of that user: [username, session ID, access mode].

FIA_USB.1.2(1) The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [**the username role will be bound to the administrative session upon successful authentication with the TOE**].

FIA_USB.1.3(1) The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [**none**].

Application note: An “access mode” such as ReadOnly, and ReadWrite is assigned to each administrative user account (Management User account or SNMPv3 User account).

6.1.24 FIA_USB.1(2) User-Subject Binding (Wireless User)

FIA_USB.1.1(2) The TSF shall associate the following **wireless**user security attributes with subjects acting on the behalf of that user: [host MAC address].

FIA_USB.1.2(2) The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [a wireless user will have their MAC address associated with their session after successful authentication with the TOE].

FIA_USB.1.3(2) The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [none].

6.1.25 FMT_MOF.1(1) Management of Cryptographic Security Functions Behavior

FMT_MOF.1.1(1) The TSF shall restrict the ability to modify the behavior of the cryptographic functions

- Crypto: load a key
- Crypto: delete/zeroize a key
- Crypto: set a key lifetime
- Crypto: set the cryptographic algorithm
- Crypto: set the TOE to encrypt or not to encrypt wireless transmissions
- Crypto: execute self tests of TOE hardware and the cryptographic functions

to administrators**with read-write permission**.

6.1.26 FMT_MOF.1(2) Management of Audit Security Functions Behavior

FMT_MOF.1.1 (2) The TSF shall restrict the ability to enable, disable, and modify the behaviorof the functions

- Audit: pre-selection of the events which trigger an audit record,
- Audit: start and stop of the audit function

to administrators**with read-write permission**.

6.1.27 FMT_MOF.1(3) Management of Authentication Security Functions Behavior

FMT_MOF.1.1(3) The TSF shall restrict the ability to modify the behavior of the Authenticationfunctions

- Auth: allow or disallow the use of an authentication server
- ~~**Auth: set the number of authentication failures that must occur before the TOE takes action to disallow future logins**~~
- Auth: set the length of time a session may remain inactive before it is terminated

to administrators**with read-write permissions**.

Application note: The TOE must be configured to defer all authentication of Management Users to the RADIUS server, though the administrator can allow or disallow use of the RADIUS server for wireless users, and can add or remove secondary, tertiary (up to 17 total) RADIUS

servers.Authentication failure limits are managed by the RADIUS server administrator. Inactivity timeouts only apply to interactive interfaces (CLI and GUI), not to programmatic interfaces (SNMPv3 and NMSP).

6.1.28 FMT_MSA.2 Secure Security Attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

6.1.29 FMT_MTD.1(1) Management of Audit Pre-selection Data

FMT_MTD.1.1(1) The TSF shall restrict the ability to query, modify, clear,createthe set of rules used to pre-select audit events to the administrator.

6.1.30 FMT_MTD.1(2) Management of Authentication Data (Administrator)

FMT_MTD.1.1(2) The TSF shall restrict the ability to query, modify, delete, clear, create the authentication credentials and user identification credentialsto administrators.

6.1.31 FMT_MTD.1(3) Management of Authentication Data (User)

FMT_MTD.1.1(3) The TSF shallrestrict the ability to modify the user authentication credentials to TOE users.

6.1.32 FMT_SMF.1(1) Specification of Management Functions (Cryptographic Function)

FMT_SMF.1.1(1) The TSF shall be capable of performing the following security management functions: query and set the encryption/decryption of network packets **(via FCS_COP.1(1))** in conformance with the administrator**'**s configuration of the TOE.

6.1.33 FMT_SMF.1(2) Specification of Management Functions (TOE Audit Record Generation)

FMT_SMF.1.1(2) The TSF shall be capable of performing the following security management functions: query, enable or disable Security Audit.

6.1.34 FMT_SMF.1(3) Specification of Management Functions (Cryptographic Key Data)

FMT_SMF.1.1(3) The TSF shall be capable of performing the following security management functions: query, set, modify, and delete the cryptographic keys and key data in support of FDP_PUD_(EXT) and enable/disable verification of cryptographic key testing.

6.1.35 FMT_SMR.1(1) Security Roles

FMT_SMR.1.1(1) The TSF shall maintain the roles administrator, wireless user.

FMT_SMR.1.2(1) The TSF shall be able to associate users with roles.

Application note: TOE administratorsinclude Management Users, and SNMPv3 Users, and each administrartive

account has an “access mode” such as ReadOnly, and ReadWrite.

6.1.36 FPT_ITT.1 Basic Internal TSF Data Transfer Protection

FPT_ITT.1 The TSF shall protect TSF data from *modification***and***disclosure* when it is transmitted between separate parts of the TOE.

6.1.37 FPT_STM_(EXT).1 Extended: Reliable Time Stamps

FPT_STM_(EXT).1.1 The TSF shall be able to provide reliable time stamps, synchronized via an external time source, for its own use.

6.1.38 FPT_TST_(EXT).1 Extended: TSF Testing

FPT_TST_(EXT).1.1 The TSF shall run a suite of self tests during the initial start-up and also either periodically during normal operation or at the request of an authorized administrator to demonstrate the correct operation of the TSF.

FPT_TST_(EXT).1.2 The TSF shall provide authorized administrators with the capability to verify the integrity of stored TSF executable code through the use of the TSF-provided cryptographic services.

6.1.39 FPT_TST.1(1) TST Testing (for cryptography)

FPT_TST.1.1(1) The TSF shall run a suite of self tests in accordance with FIPS PUB 140-2 and Appendix C of **the PP** during initial start-up (on power on), at the request of the ~~**cryptographic**~~ administrator (on demand), under various conditions defined in section 4.9.1 of FIPS 140-2, and periodically (at least once a day) to demonstrate the correct operation of the following cryptographic functions:

a) key error detection;

b) cryptographic algorithms;

c) RNG/PRNG

FPT_TST.1.2(1) The TSF shall provide authorized ~~**cryptographic**~~administrators with the capability to verify the integrity of TSF data related to the cryptography by using TSF-provided cryptographic functions.

FPT_TST.1.3(1) The TSF shall provide authorized ~~**cryptographic**~~administrators with the capability to verify the integrity of stored TSF executable code related to the cryptography by using TSF-provided cryptographic functions.

6.1.40 FPT_TST.1(2) TSF Testing (for key generation components)

FPT_TST.1.1(2) The TSF shall perform self tests immediately after generation of a key to demonstrate the correct operation of each key generation component. If any of these tests fails, that generated key shall not be used, the cryptographic module shall react as required by FIPS PUB 140-2 for failing a self-test, and this event will be audited.

FPT_TST.1.2(2) The TSF shall provide authorized ~~**cryptographic**~~administrators with the capability to verify the integrity of TSF data related to the key generation by using TSF-provided cryptographic functions.

FPT_TST.1.3(2) The TSF shall provide authorized ~~**cryptographic**~~administrators with the capability to verify

the integrity of stored TSF executable code related to the key generation by using TSF-provided cryptographic functions.

6.1.41 FTA_SSL.3 TSF-Initiated Termination

FTA_SSL.3.1 The TSF shall terminate a local interactive or wireless session after an administrator configurable time interval of user inactivity.

Application note: For administrative sessions (not wireless sessions), the "local interactive" session is understood here to mean the 'interactive' (CLI or GUI) session that is established with and maintained 'locally' on the controller (via SSH or TLS).

6.1.42 FTA_TAB.1 Default TOE Access Banners

FTA_TAB.1.1 Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorized use of the TOE.

Application note: This SFR applies only to interactive administrative interfaces (the Controller CLI, and the Controller GUI), and does not apply to the SNMPv3 interface.

6.1.43 FTP_ITC_(EXT).1 Extended: Inter-TSF Trusted Channel

FTP_ITC_(EXT).1.1 The TOE shall provide an encrypted communication channel between itself and entities in TOE IT Environment that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC_(EXT).1.2 The TSF shall permit the TSF, or the IT Environment entities to initiate communication via the trusted channel.

FTP_ITC_(EXT).1.3 The TSF shall initiate communication via the trusted channel for all authentication functions, remote logging, time,*[remote administration, communications with MSE, communications with WCS or NCS]*.

6.1.44 FTP_TRP.1 Trusted Path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and wireless ~~**users**~~**client devices** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification, replay or disclosure.

FTP_TRP.1.2 The TSF shall permit wireless client devices to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for wireless~~**user**~~**client** authentication, [**none**].

6.1.45 IPS_SDC_(EXT).1 Extended: wIPS Data Collection

IPS_SDC_(EXT).1.1 The TSF shall be able to collect the following information from wireless networks:

a) wireless network traffic.

IPS_SDC_(EXT).1.2 The TSF shall be able to collect and record the following information, and transmit the information to the MSE for further analysis and reporting:

a) date and time of the event;

b) identity of the source and destination of the traffic;

c) AP identity;

d) wireless signal strength; and

e) the wireless network traffic details indicative of the following advanced wIPS events:

    a. DoS Attack Detection including:

        i. Association flood
        ii. Association table overflow
        iii. Authentication flood
        iv. EAPOL-Start attack
        v. PS-Poll flood
        vi. CTS Flood
        vii. Queensland University of Technology Exploit
        viii. RF jamming attack
        ix. RTS flood
        x. Virtual carrier attack
        xi. Authentication-failure attack
        xii. Deauthentication broadcast attack
        xiii. Deauthentication flood attack
        xiv. Disassociation broadcast attack
        xv. Disassociation flood attack
        xvi. EAPOL-logoff attack
        xvii. FATA-jack tool detected
        xviii. Premature EAP-failure attack
        xix. Premature EAP-success attack

    b. Security Penetration Attack Detection including:

        i. Airsnarf attack
        ii. ChopChop Attack
        iii. Day-zero attack by WLAN security anomaly
        iv. Day-zero attack by device security anomaly
        v. Device probing for access points
        vi. Dictionary attack on EAP methods
        vii. EAP attack against 802.1x authentication
        viii. Fake access points detected
        ix. Fake DHCP server detected
        x. Fast WEP crack detected
        xi. Fragmentation Attack
        xii. Hotspotter tool detected
        xiii. Malformed 802.11 packets detected

xiv. Man in the middle attack detected

xv. NetStumbler detected

xvi. PSPF violation

xvii. ASLEAP attack detected

xviii. Honey pot access point detected

xix. Soft access point or Host access point detected

xx. Spoofed MAC address detected

xxi. Suspicious after-hours traffic

xxii. Unauthorized association by vendor list

xxiii. Unauthorized association detected

xxiv. Wellenreiter detected

c. A violation in the authentication policy of a network

d. A violation in the encryption policy of a network

e. Events related to detection of authorized wireless devices

Application Note This IPS Data Collection SFR (IPS_SDC) is distinct from the wIPS Analysis SFR (IPS_ANL) in that this SFR lists the wireless network events for which the MSE performs data correlation, analysis, and generation of audit records of detected events based on that analysis. Identity of the data source is used for detection of rogue APs and rogue clients, and to allow correlation to an active list of malicious source addresses. Signal strength measurements are included in analysis data to support location tracking by the MSE through correlation of data from multiple APs.

6.1.46 IPS_ANL_(EXT).1 Extended: wIPS Analysis

IPS_ANL_(EXT).1.1 The TSF shall perform the following analysis functions(s) on all wireless data received:

a) signature check;

b) integrity check; and

c) measurement of signal strength.

IPS_ANL_(EXT).1.2 The TSF shall record within each analytical result at least the following information:

a) date and time of the event;

b) identity of the source and destination of the traffic;

c) AP identity; and

d) Basic wIPS events detected:

a. DoS Attack Detection including:

i. Association flood

ii. Authentication flood

iii. Unauthenticated Association

iv. Deauthentication broadcast attack

v. Deauthentication flood attack

vi. Disassociation broadcast attack

vii. Disassociation flood attack

b. Security Penetration Attack Detection including:

i. NetStumbler detected

ii. Wellenreiter detected

c. Events related to detection of ad-hoc 802.11 devices

d. Events related to detection of rogue clients

e. Spoofed 802.11 Management Frames

Application Note This wIPS Analysis SFR (IPS_ANL) is distinct from the IPS Data Collection SFR (IPS_SDC)in that this SFR lists the wireless network events for which the AP performs analysis, and generation of audit records of detected events based on that analysis.

6.1.47 IPS_RCT_(EXT).1 Extended: wIPS Reaction

IPS_RCT_(EXT).1.1 The TSF shall be able to take one or more appropriate actions listed below when an IPS policy violation is detected:

a) Drop traffic that matches signatures listed in IPS_ANL_(EXT).1.1; and/or

b) Drop traffic that fails integrity checks described in FDP_PUD_(EXT).1; and/or

c) Drop traffic that fails authentication checks; and/or

d) Drop traffic that matches an entry in the active list of malicious source addresses; and/or

e) Launch a de-authentication attack (rogue containment) against one or more rogue APs and associated clients, and generate an audit record of the rogue containment with the following audit message details:

a. date and time of the event;

b. identity of the rogue target; and

c. AP identity.

6.2 Security Requirements for the IT Environment

6.2.1 FAU_GEN.1(2) Audit Data Generation

FAU_GEN.1.1(2) The TOE IT Environment 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 minimum level of audit; and

c. [additional auditable events shown in column 2 of **Table 15**].

Table 15TOE IT Environment Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1**(2)**	None	None
FAU_SAR.1	None	None

FAU_SAR.2	Unsuccessful attempt to read the audit records	The identity of the user attempting to perform the action
FAU_SAR.3	None	None
FAU_STG.1	None	None
FAU_STG.3	Any actions taken when the audit limits are exceeded.	None
FAU_SEL.1(2)	**All modifications to the audit configuration that occur while the audit collection functions are operating.**	**The identity of the Administrator performing the function.**
FDP_RIP.1(2)	None	None
FIA_AFL.1**(2)**	The reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g., disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g., re-enabling of a terminal	None
FIA_ATD.1**(3)**	None	None
FIA_UAU_(EXT).5**(2)**	Failure to receive a response from the remote authentication server	Identification of the Authentication server that did not reply
FIA_UID.1	None	None
FMT_MTD.1(4)	Changes to the time data	None
FMT_MTD.1(5)	Changing the TOE audit pre-selection data	None
FMT_SMR.1(2)	Modifications to the group of users that are part of a role	None
FPT_STM.1**(2)**	Setting time/date	Identity of the administrator that performed the action
FTP_ITC_(EXT).1	Initiation/Closure of a trusted channel	Identification of the remote entity with which the channel was attempted/created; Success or failure of the event.

FAU_GEN.1.2(2) The TOE IT Environment shall record within each audit record at least the following information:

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

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

6.2.2 FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TOE IT environment shall provide only the[administrator]with the capability to read [all audit data] from the audit records.

FAU_SAR.1.2 The TOE IT environment TSF shall provide the audit records in a manner suitable for the **administrator** to interpret the information.

6.2.3 FAU_SAR.2 Restricted Audit Review

FAU_SAR.2.1 The TOE IT environment shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

6.2.4 FAU_SAR.3 Selectable Audit Review

FAU_SAR.3.1 The TOE IT environment shall provide the ability to perform [*searches*] of audit data based on event type, date, time, and/or [**message contents**].

6.2.5 FAU_STG.1 Protected audit trail storage

FAU_STG.1.1 The TOE IT environment shall protect the stored audit records from unauthorized deletion.

FAU_STG.1.2 The TOE IT environment shall be able to prevent unauthorized modifications to the audit records in the audit trail.

6.2.6 FAU_STG.3 Action in case of possible audit data loss

FAU_STG.3.1 The TOE IT environment shall [immediately alert the administrator by displaying a message at the local console,[*none*] if the audit trail exceeds an administrator-settable percentage of storage capacity.

6.2.7 FAU_SEL.1(2) Selective Audit

FAU_SEL.1.1(2) The **TOE IT environment**shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

a) *user identity*;

b) [device interface, wireless client identity].

6.2.8 FDP_RIP.1(2) Subset Residual Information Protection

FDP_RIP.1.1(2) The **TOE IT Environment** shall ensure that any previous information content of a resource is made unavailable upon the allocation of the resource to the following objects: network packet objects.

6.2.9 FIA_AFL.1(2) Remote User Authentication failure handling

FIA_AFL.1.1(2) The TOE IT Environment shalldetect when an administrator configurable positive integer within [**a non-zero positive integer**] of unsuccessful authentication attempts occur related to [remote users logging on to the WLAN access system].

FIA_AFL.1.2 (2) When the defined number of unsuccessful authentication attempts has been met or surpassed, the **TOE IT Environment**shall prevent the remote user from authenticating until action is taken by an administrator.

6.2.10 FIA_ATD.1(3) User attribute definition

FIA_ATD.1.1(3) The**TOE IT environment** shall maintain the following minimum list of security attributes belonging to individual remotely authenticated users: [**user ID, password, host MAC address, X.509 certificates (for EAP-TLS), PAC (for EAP-FAST), smart card token (for EAP-GCT), 802.11i session encryption keys**].

6.2.11 FIA_UAU_(EXT).5(2) Remote authentication mechanisms

FIA_UAU_(EXT).5.1(2) The TOE IT Environment shall provide a remote authentication mechanism to provide TOE remote user authentication.

FIA_UAU_(EXT).5.2(2) The TOE IT Environment shall authenticate any user's claimed identity according to the [**AAA authentication policies defined on the Controller**].

6.2.12 FIA_UID.1 Timing of identification

FIA_UID.1.1 The TOE IT environment shall allow [**no mediated actions**] on behalf of the TOE remote user to be performed before the user is identified.

FIA_UID.1.2 The TOE IT environment shall require each TOE remote user to identify itself before allowing any other IT environment or TSF-mediated actions on behalf of that TOE remote user.

6.2.13 FMT_MOF.1(4) Management of Security Functions Behavior

FMT_MOF.1.1(4) The TOE IT environment shall restrict the ability to determine the behavior of ***disable, enable, modify the behaviour of***the functions: [

- Audit,
- Remote Authentication
- Time service]

to [the administrator].

6.2.14 FMT_MTD.1(4) Management of time data

FMT_MTD.1.1(4) The TOE IT environment shall restrict the ability to [set] the [time and date used to form the time stamps in FPT_STM.1] to [the Security Administrator or authorized IT entity].

6.2.15 FMT_MTD.1(5) Management of Audit Pre-selection Data

FMT_MTD.1.1(5) The **TOE IT environment** shall restrict the ability to *query, modify, clear,create*the *set of rules used to pre-select audit events* to [the administrator].

6.2.16 FMT_SMR.1(2) Security roles

FMT_SMR.1.1(2) The TOE IT environment shall maintain the roles [administrator].

FMT_SMR.1.2(2) The TOE IT environment shall be able to associate users with roles.

6.2.17 FTP_ITC_(EXT).1(2) Inter-TSF trusted channel

FTP_ITC_(EXT).1.1(2) The TOE IT environment shall provide an encrypted communication channel between itself and the TOE that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC_(EXT).1.2(2) The TOE IT Environment shall permit the TSF, or the TOE IT Environment entities to initiate communication via the trusted channel.

FTP_ITC_(EXT).1.3(2) The TOE IT environment shall initiate communication via the trusted channel for [all authentication functions, remote logging, time, [***remote configuration from WCS/NCS to Controllers***].

6.2.18 FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The TOE IT environment shall be able to provide reliable time and date stamps for the TOE and its own use.

6.3 TOE Security Assurance Requirements

The TOE security assurance requirements summarized in **Table 16:** TOE Assurance Requirements identify the management and evaluative activities required to address the threats and policies identified in section 3 of this ST. This ST complies with assurance level EAL4 augmented with ALC_FLR.2. EAL4 was chosen because it permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices. EAL4 provides the developers and users a moderate to high level of independently assured security in conventional commercial TOEs.EAL 4 is augmented by ALC_FLR.2 to help ensure that the customers can report the flaws and the flaws can be systematically corrected.

Table 16TOE Assurance Requirements

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design

AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_FLR.2 Flaw reporting procedures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.2 Testing: security enforcing modules
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis

7 TOE Summary Specification

This section identifies and describes the security functions implemented by the TOE and the assurance measures applied to ensure their correct implementation.

7.1 TOE Security Functional Requirements Measures

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

Table 17TOE Security Functions

TOE SFRs	How the SFR is met
FAU_GEN.1(1)	All components of the TOE work to implement an auditing capability of security relevant events that happen under the control of the TOE. Audit records are generated by the TOE for all of the events that are listed in FAU_GEN.1(1) as they occur on the respective AP and Controller components. During installation the administrator must configure the Controller to communicate with the syslog server via TLS for remote storage of TOE-generated audit records. Audit events generated by the TOE contain the following fields: a timestamp, an associated user identity, event type, and whether it was a success or failure. The timestamp that is used is based on a local timestamp on each TOE component, which relies on a time server in the environment for synchronization. **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. **AP Logging** Access points log all system messages (with a severity level less than or equal to notifications, i.e. 0-5) to the access point event log. The event log can contain up to 1024 lines of messages, with up to 128 characters per line. When the event log becomes filled, the oldest message is removed to accommodate a new event message. The event log is saved in a file on the access point flash, which ensures that it is saved through a reboot cycle. To minimize the number of writes to the access point flash, the contents of the event log are written to the event log file during normal reload and crash scenarios only. The AP system event log may be viewed from the controller CLI. Related TOE IT Environment SFRs: FAU_GEN.1(2):ACS/ISEgenerates those auditing records that deal with the management of user accounts controlled by the ACS/ISE, the encryption policies controlled by the ACS/ISEfor wireless users, the changing of auditing capabilities controlled by the ACS/ISE, authentication actions, and administrative actions. The ACS/ISEauditing capability is implemented in three different logging capabilities of ACS/ISE. These logging capabilities are the CSV Failed Attempts, CSV Passed Authentication, and CSV RADIUS Accounting. Within each of these logging capabilities the ACS/ISEAdministrator is able to define what is audited based on the type of event. ACS/ISEalso provides the TOE functionality that allows for administrator actions

<table>
<tr><td></td><td>through the Controller to be logged and viewed. This is accomplished using Controller TACACS+ accounting. For this, the ACS/ISEacts as an AAA server and the Controller as the AAA client. All actions performed by the Controller administrator are forwarded back to ACS/ISEin the form of Controller TACACS+ accounting logs. These logs are then viewable through the ACS/ISEinterface in the TACACS+ Administration Active CSV logs. This log, in conjunction with the Passed Authentication Active CSV log, provides the audit generation capability for the audit requirements stated in the SFR.</td></tr>
<tr><td>FAU_GEN.2</td><td>Administrator management activities include the user name of the administrator in the event logs. Wireless users cannot establish interactive user interface with the TOE and thus there are not auditable user actions other than any activity related to the wireless client, which will be audited by the AP with proper client identification (see IPS_*_EXT.1 for more details). The AP provides wireless client MAC address so the Controller can record the MAC address in syslog messages, and the ACS/ISE server in the TOE IT Environment can record the user identity as the “Caller-ID” field.
The SNMPv3 interface on the Controller is a programmatic interface, not an interactive administrative interface. Each “SNMPv3 User” account is used to authenticate a single external entity (one instance of an NCS or WCS). An SNMPv3 server is not capable of (re)authenticate administrators who have individually authenticated to an external entity prior to trigging an SNMPv3 GET or SET command to be sent from the external entity to an SNMPv3 server. Thus, Controller-generated audit records of actions performed on a Controller by an “SNMPv3 User” are actions performed by an external entity (one instance of WCS or NCS).</td></tr>
<tr><td>FAU_SEL.1(1)</td><td>The Controller supports pre-selection of audit generation based on event type, which are standard syslog severity levels 0 through 7. The severity level can be set separately for APs than for the Controller itself, and can be set separately for those messages stored in the local log, or written to the console, or transmitted via syslog. Additionally, the logging of process information (procinfo) and traceback information (traceinfo) can be enabled or disabled. 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 evaluated configuration.
Related TOE IT Environment SFRs:
FAU_SEL.1(2):
The Kiwi Syslog Daemon and the Syslog-ng software package filtering capabilities are used to support both pre- and post-selection of audit data. To satisfy pre-selection in FAU_SEL.1(2), the wireless user "passed authentications" wireless user "failed attempts" and ACS/ISE admin "Administrative Audit" logs are generated by ACS/ISE but not stored locally in ACS/ISE persistent storage. Instead these event records are forwarded by ACS/ISE directly to the syslog server for pre-filtering before being placed in persistent storage. The ability to filter passed or failed attempts, administration, password changes, and service monitoring events is selected based on the GUI setting for that event report.
All other ACS/ISE audit log files may be written into ACS/ISE persistent storage for a time before being sent to the Syslog server. Post selection filtering can be done on any audit records stored on the Syslog server.
Syslog audit log filtering will map the fields identified in FAU_SEL.1.1(2) to the following wireless user audit log fields generated by ACS/ISE.
<table>
<tr><th>FAU_SEL.1.1(2) Term</th><th>ACS/ISE Log Event Field</th></tr>
<tr><td>“user identity”</td><td>“User Name”</td></tr>
<tr><td>“event type”</td><td>“Priority” set to “Auth”</td></tr>
</table>
</td></tr>
</table>

	<table><tr><td>“device interface”</td><td>Implied WLAN interface [The ACS/ISE audit logs for wireless users “Passed Authentications” and “Failed Attempts” only apply to TOE audit events generated by a wireless users WLAN interface]</td></tr><tr><td>“wireless client identity”</td><td>“Caller-ID”. [The ACS/ISE “Caller-ID” field corresponds to the wireless client machine MAC ID address]</td></tr></table> The TOE administrator has the ability to either enable or disable logging for each of these categories, based on the syslog fields. This is done on the syslog side through the graphical user interface on the Kiwi Syslog Server or the Command Line Interface on the Syslog-ng server.
FCS_BCM_(EXT).1	The APs and Controllers are FIPS PUB 140-2 validated Level 2 cryptomodules and perform cryptographic functions in FIPS approved modes of operation. The following FIPS 140-2 certificates apply: • FIPS certificate #1446 (APs 1522, and 1524) • FIPS certificate #1448 (APs 1131, 1142, 1242, 1252, 1262, 3502e and 3502i) • FIPS certificate #1909(WiSM2) • FIPS certificate #1875(WiSM) • FIPS certificate #1853 (Controllers 4402, and 4404) • FIPS certificate #1829 (Controller 5508)
FCS_CKM.1(1)	The following values are generated by FIPS 140-2 evaluated cryptographic modules. • Generated by AP: DTLS pre-master secret • Generated by Controller: TLS pre-master secret, Infrastructure MFP MIC Key, EAP-FAST Server Key and EAP-FAST PAC-Key All of these values are generated using FIPS 140-2 approved and certified RNGs. SP 800-57 compliant key integrity protection is provided by the physical protection of a certified cryptographic module.
FCS_CKM.1(2)	DSA and RSA keys are generated according to FIPS 186-3, using a FIPS approved RNG. Key validity is assured by the means of a pairwise integrity test when the keys are generated. Key integrity protection is provided by the physical protection of a certified cryptographic module.
FCS_CKM.2	Electronic key distribution methods used in the WLAN Access System include RSA key wrapping as part of the DTLS protocol that underlies CAPWAP and AES Key Wrap for distribution of the 802.11i Pairwise Temporal Key. The AES Key Wrap Key is entered via the Controller GUI rather than generated in the TOE, to comply with SP 800-57 Section 8.1.5 the source of the key should be approved by the U.S. Government for the protection of national security information. The RSA key wrap keys are generated in FIPS 140-2 validated cryptographic modules. Once in the system both types of keys are protected in accordance with section 6 of SP 800.57 (as per FCS_CKM.1(1) and FCS_CKM.1(2)). When the ACS/ISE distributes the PMK to the Controller it performs AES key wrapping on the PMK. Key wrapping protects the confidentiality and integrity of Pairwise Master Keys (PMK) under FIPS 140-2 validation when the keys are in transit. From the Controller to the AP, the PMK is protected via the FIPS 140-2 validated assured channel with AES-CBC encryption. Keys are distributed to the APs from the Controller/WiSM over a CAPWAP control session. During a CAPWAP session, the APs first authenticate to the Controller/WiSM using an RSA key pair. After a successful authentication, the CAPWAP session key generated in the

	Controller/WiSM is transported to the AP wrapped with AP's RSA key. Discrete logarithm cryptography is not used for key distribution in the TOE.
FCS_CKM_(EXT).2	All keys transmission techniques used by the TOE include integrity mechanisms to detect errors. Private keys on the AP and Controller are stored in PKCS#12 files that are AES encrypted. Private keys on the ACS/ISE are stored encrypted in NSS tokens or in an encrypted database. The Controller administrator may configure the length of time that an inactive session may exist before it is terminated, when that occurs non-persistent cryptographic keys are zeroized. The TOE does not support archiving of private keys.
FCS_CKM.4	Key destruction (zeroization) for the AP and Controller modules is a onetime operation for hardware, factory burned certificates. The Controller FIPS 140-2 Security Policy stipulates that zeroization should take place over the Controller CLI, which will take the TOE out of the evaluated configuration. Once the zeroization operation is performed for hardware certificates the TOE components will be non-communicative. Intermediate key values are zeroized by the Controller and AP, and all transient key values such as session keys are zeroized when their associated sessions are complete. For non-volatile memories other than EEPROM and Flash, the zeroization shall be executed by overwriting three or more times using a different alternating data pattern each time.
FCS_COP.1(1)	AES-128 is used within TLS and DTLS ciphersuites (for CAPWAP, HTTPS, EAP-FAST and EAP-TLS), for AES Key Wrap to distribute 802.11i PMKs, and for encryption of 802.11i keys and traffic. The APs perform FIPS 140-2 validated end-to-end AES-CCMP wireless encryption and decryption between a wireless device and the AP. End-to-end wireless encryption is implemented in the TOE through the use of EAP-TLS, EAP-FAST, EAP-MSCHAPv2, EAP-GCT, or WPA2-PSK. To carry out encryption the AP, and Controller components of the TOE, and the ACS/ISE play a role. The encryption algorithm used is AES-CCM (CCMP) mode of operation with a 128-bit key. Controllers support Cisco Access Points operating in CAPWAP mode and configured with Wi-Fi Protected Access 2 (WPA2) security. WPA2 is the approved Wi-Fi Alliance interoperable implementation of the IEEE 802.11i standard. When WPA2-PSK is used only the APs are involved with the encryption and decryption that takes place with a wireless client. WPA2 protects all wireless communications between the wireless client and other trusted networked devices on the wired network with AES-CCMP encryption. CAPWAP protects all control and bridging traffic between trusted network access points and the module with AES-CBC encryption. CAPWAP also protects all client data traffic between the Access Points and the Controller on the 5508 Controller and 1131, 1142, 1242, 1252, 1262, 3502E, and 3502I series access points. This utilizes a secondary AES-CBC (with 128 bit keys) protected DTLS tunnel For encryption implemented with EAP-TLS, EAP-MSCHAPv2, EAP-GCT, and EAP-FAST the APs, Controllers, and ACS/ISEs all play a role in the cryptographic key generation and encryption process. The TOE uses the IEEE 802.11i Pairwise key hierarchy to establish session-specific keys from the Pairwise Master Key (PMK). The PMK is generated by the ACS/ISE (Radius server) in coordination with the wireless client and encrypted with the AES key wrap protocol and passed to the Controller/WiSM. The PMK is then used to generate the session specific Pairwise Transient Key (PTK). The Controller/WiSM then passes the (PTK) to the AP. The AP uses the PTK to generate the individual session keys (Key Encryption Key (KEK), Key Confirmation Key (KCK) and Temporal Key (TK) for encrypting the wireless traffic with each wireless client that has been authenticated. The KEK is used by the EAPOL-Key frames to provide confidentiality. The KCK is used by IEEE 802.11i to provide data origin authenticity The TK, also known as the CCMP key, is the 802.11i session key for unicast communications. Cryptographic keys are stored in flash and in SDRAM for active keys.
FCS_COP.1(2)	RSA is used for authentication and key distribution in the CAPWAP, HTTPS, EAP-FAST and EAP-TLS, and for verification of software images downloaded from the controller to the AP.

	DSA is used for authentication and key distribution for SSH. All DSA and RSA keys used in the evaluated configuration will have a key size of 2048 bits.
FCS_COP.1(3)	SHA-1 is used as part of the TLS and DTLS protocols that underlie CAPWAP, HTTPS, EAP-FAST and EAP-TLS, as part of HMAC-SHA-1 for SNMPv3 authentication between the Controller and SNMPv3 applications, and key integrity protection within the 802.11i protocol. SHA-256 is also supported for digital signatures.
FCS_COP.1(4)	Diffie-Hellman is used for anonymous and authenticated TLS DHE ciphersuite options for EAP-FAST and EAP-TLS.
FCS_COP_(EXT).1	The Access Points implement FIPS 140-2 approved X9.31 RNGs, seeded with system entropy at startup. The Controllers implement the FIPS 140-2 approved FIPS 186-2 RNG, seeded with system entropy at startup. The FIPS approved RNGs are used for generation of security relevant random values (e.g. nonces, Diffie-Hellman parameters) and cryptographic keys.
FDP_PUD_(EXT).1	The administrator has control over whether or not unencrypted data will be allowed to pass through the TOE by providing the ability to enable and disable the encryption policy of the TOE. This encryption policy determines whether the APs and Controllers will encrypt and decrypt communications with wireless clients. After a wireless client has successfully authenticated to the TOE the wireless client can communicate with other wireless clients that have successfully authenticated through the TOE and with other wired clients that operate on the wired network controlled by the TOE. If the administrator has enabled encryption of wireless client user data, the TOE will encrypt user data transmitted to a wireless client from the radio interface of the wireless access system and decrypt user data received from a wireless client by the radio interface of the wireless access system. This ensures that the TOE supports end-to-end wireless encryption. The TOE allows for the detection of modification of user data while carrying out network communications on the wireless network through the use of AES operating in CCM (CCMP). This is done through this standard through the integrity protection capabilities of the algorithm. The Cipher Block Chaining Message Authentication Code (CBC-MAC) component of CCMP provides data integrity. The CBC-MAC allows for the detection of a modified packet. If a CBC-MAC indicates a packet has been modified the packet is dropped.
FDP_RIP.1(1)	Network packet objects are padded with zeroes upon allocation of network interfaces of each TOE component (AP, and WLC). Related TOE IT Environment SFRs: FDP_RIP.1(2): The ACS/ISE also ensures through their network interface drivers that any residual data from previous packets is not re-transmitted any subsequent packets. This requirement does not apply to the remote syslog server since it only receives audit records, but does not transmit audit records.
FIA_AFL.1(1)	To meet the requirement to be able to lock administrative accounts (Management Users only, not SNMPv3 Users) after failed login attempts to remote administrative interfaces (SSH or TLS), the Controller will be configured to defer authentication of SSH and TLS administrative authentication to the remote authentication server. Locked accounts on the RADIUS server can be resolved bythe RADIUS administrator unlocking administrative accounts Related TOE IT Environment SFRs: FIA_AFL.1(2): The ACS enforces the number of unsuccessful authentication attempts and will lock out user accounts after they reach the administrator-defined threshold. An ACS administrator is required to unlock a user account. When ISE is used as the directly-accessible (first-tier) RADIUS server for the Controller(s), ISE must be configured to defer authentication of Controller administrators (Management Users) to a separate (second-tier) authentication server that is able to enforce lockout after failed

	login attempts. Those second-tier authentication servers could include Active Directory, LDAP, or an ACS server.
FIA_ATD.1(1)	Controller SNMPv3 Users (administrative accounts) are defined in the Controller's local user database with their username and password. Related TOE IT Environment SFRs: FIA_ATD.1(3): The remote authentication server (ACS, and optionally AD, or LDAP servers referenced through ACS or ISE) maintains username and password for Controller administrators (Management Users) authenticating to the TOE via any remote administration method (SSH or TLS).
FIA_ATD.1(2)	Wireless users authenticating to the TOE can be authenticated to the local user database or to authentication can be deferred to a remote authentication server. When users are authenticated locally, the Controller maintains their authentication credentials listed below as appropriate for each authentication method: • EAP-TLS: client's device certificate • EAP-FAST without client certificate: username and password • EAP-FAST with client certificate: client's device certificate • EAP-FAST with EAP-GTC: username and PAC (Protected Access Credential) • EAP-MSCHAPv2 without client certificate: username and password • EAP-MSCHAPv2 with client certificate: client's device certificate • WPA2-PSK: Passphrase (ASCII or Hex)] Protected access credentials (PACs) are strong shared secrets that enable the Controller and an EAP-FAST client to authenticate each other and establish a TLS tunnel for use in EAP-FAST. PACs can be either automatically or manually provisioned from the Controller to the client. When manual PAC provisioning is enabled, the PAC file is manually generated on the controller. PACs generated off the Controller can be downloaded to the Controller by an administrator. Client certificates and CA server certificates can also be downloaded to the Controller by an administrator. Related TOE IT Environment SFRs: FIA_ATD.1(3): Wireless users who are remotely authenticated against user stores within ACS/ISE have the following authentication parameters stored within the ACS/ISE: user ID, passwords, and host MAC address are used for simple authentication (users can be disabled by their User ID, and clients can be disabled by their MAC address). X.509 certificates, PACs or smart card tokens are security attributes that may optionally be used when authenticating the user. 802.11i session encryption keys are provisioned to clients and APs from the ACS/ISE, and are used to protect wireless traffic.
FIA_UAU.1	The TOE provides GUI and CLI administrative interfaces at the Controller that both require an authenticated session to providing any administrative services. Unauthenticated users connecting via TLS will be directed to log in to the GUI, and connections via SSH or serial console require authentication to the CLI. In addition, the AP and Controller TOE components authenticate each other during set up of the communications channel. To be consisten with the application notes in the WLAN PP, this SFR is specific to accounts authenticated locally on the TOE, which can include wireless users (if configured by the Controller administrator to authenticate locally), and SNMPv3 Users. The TOE does not allow actions to be performed by any identified wireless user, or SNMPv3 User until authentication has completed successfully.

FIA_UAU_(EXT).5(1)	The Controller administrator can configure both local authentication and remote authentication. Remote authentication is required for remote administrative access to the TOE. The TOE can be configured (independently for each WLAN) to authenticate wireless users to its local wireless user database, or to defer authentication of wireless users to one or more RADIUS servers. The TOE can be configured (independently for each WLAN) to authenticate wireless users to its local wireless user database, or to defer authentication of wireless users to one or more RADIUS servers. The TOE authenticates SNMPv3 User accounts locally. Management User accounts defined within the local user database of the Controller are not used in the evaluated configuration in which all remote access by Management Users is authenticated to the RADIUS server, and the serial console port is inaccessible when the FIPS Kit is installed. Related TOE IT Environment SFRs: FIA_UAU_(EXT).5(2): The ACS/ISE is the remote authentication server for the TOE, providing administrator and wireless user authentication via RADIUS.
FIA_UID.2	No administrative or user actions are permitted on the AP or Controller without identification to AP, or WLC. All wireless users and TOE administrators (including Controller administrators authenticated via RADIUS, and SNMPv3 Users authenticated locally) are required to be successfully identified (via the configured authentication mechanisms), prior to the TOE allowing any TSF-mediated actions other than authentication attempts. Any deferring of authentication of authentication decisions (for Controller administrators or wireless users) to a RADIUS server does not interfere with the TOE controlling the sequence of identification, authentication, and access events (e.g. allowing the establishment of an encrypted session, allowing a login attempt, deferring authentication decision to RADIUS, and waiting for successful authentication to be confirmed by RADIUS, before granting further access). Related TOE IT Environment SFRs: FIA_UID.1: No administrative or user actions are permitted on ACS/ISE without identification. The syslog server relies on its host operating system to ensure identification, and authentication.
FIA_USB.1(1)	Administrative sessions (for Management Users and SNMPv3 Users) are associated with their access mode (e.g. ReadOnly or ReadWrite) upon authentication, and for the duration of the interactive session. The TOE maintains a session ID for any administrative access session (SSH, TLS, or SNMPv3), and binds the username and the user's access mode (as established at authentication), with the session ID for the duration of the authenticated session. Regardless of whether an administrative session was authenticated locally (for SNMPv3 Users), or remotely (via RADIUS for Management Users) the username and access modeare bound to the session ID.
FIA_USB.1(2)	The TOE is able to associate wireless clients with their identifying attributes by matching the host MAC address with the session ID. Regardless of whether wireless user session was authenticated locally, or remotely (via RADIUS) the wireless client's MAC address are bound to the session ID.
FMT_MOF.1(1) FMT_SMF.1(1) FMT_SMF.1(3)	The Controller provides management interfaces for administration of the Controllers and the APs. The Controllers administer the APs that have been associated with the Controller during installation of the APs using CAPWAP. The Controller maintains a policy file for the APs that the Controller pushes out to the APs. The policy file contains the information on what encryption policies that the AP enforces. The encryption policies can be set on a per WLAN SSID basis. The Controller administrator sets the Controller to use WPA2 then selects between Preshared Key (PSK) and 802.1X requests, which get sent to the ACS/ISE for authentication. The Controller administrator configures cryptographic settings for the Controller and AP modules and has the ability to load and zeroize keys, select cryptographic algorithms, execute self test functions and configure the TOE to encrypt or not encrypt wireless transmissions. The

	Controller management interfaces permit management of cryptographic keys and key data in support of FDP_PUD_EXT as well as executing cryptographic key tests. The capability to verify integrity of stored code can only be performed through the Controller CLI, thus can only be performed by Management User accounts, not SNMPv3 User accounts.
FMT_MOF.1(2) FMT_SMF.1(2) FMT_MTD.1(1)	The Controller administrator is able to configure audit generation functions described earlier in this table for FAU_SEL.1(1). The Controller administrator is also able to 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. Related TOE IT Environment SFRs: FMT_MOF.1(4):The Syslog administrator, after authentication by the Syslog Host, may configure the audit preselection parameters, and start and stop syslog. The ACS/ISE administrator may configure audit preselection parameters and start and stop audit logging at the ACS/ISE.
FMT_MOF.1(3)	The Controller administrator is able to configure (enable/disable/define/re-define) authentication servers used by the Controller. The controller does not enforce account lockout for multiple failed login attempts to the local serial console, and requires that all remote administrative sessions (SSH or TLS) are authenticated to the remote authentication server so the remote authentication server can enforce lockout of accounts after successive failed login attempts. The TOE must be configured to defer all authentication of Management Users to the RADIUS server, though the administrator can allow or disallow use of the RADIUS server for wireless users, and can add or remove secondary, tertiary (up to 17 total) RADIUS servers. The Controller administrator defines the length of time that an administrative session can remain inactive before the session is terminated, and can configure serial console, SSH, and TLS with separate timeout limits.
FMT_MSA.2	In support of meeting FCS_COP and FCS_CKM, the AP, and Controller generate keys that meet all requirements defined in all iterations of FCS_CKM and FCS_COP to ensure that only secure values are accepted for security attributes. Cryptographic keys are generated using FIPS approved random number generators, with RSA keys subject to pairwise consistency tests to confirm their validity.
FMT_MTD.1(1)	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. See related controls in rationale for FMT_MOF.1(2), and FAU_SEL.1(1).
FMT_MTD.1(2) FMT_MTD.1(3)	The Controller administrator is able to query, modify, delete, clear, and create authentication credentials, and user identification credentials for users defined in the local user authentication database. The administrator can create users, and assign usernames and passwords, and can delete users and change user passwords. TOE users (administrators) with access to the administrative interfaces of the TOE (Controller CLI and Controller GUI) are able to modify their own passwords. FMT_MTD.1(2) is specific to credentials of administrative accounts defined within the local user database of the Controller (SNMPv3 Users). FMT_MTD.1(3) is specific to credentials of wireless user accounts defined within the local user database of the Controller. Relevant TOE IT Environment functions (not explicitly related to SFRs defined in the PP): ACS/ISE Administrators perform all aspects of user account management for accounts

<table>
<tr><td></td><td>stored in the ACS/ISE user database including TOE administrative accounts (ACS only, not ISE) and wireless client accounts (ACS or ISE). The ACS also provides an optional User Change Password web service that can be used to provide a web interface for users to manage their passwords. This can be provided for all users authenticated against the ACS, including wireless users and Controller and ACS administrators.

ACS/ISEcan implement certain administration capabilities forthe TOE. Specifically the ACS/ISE allows for the administration of wireless user authentication credentials and authorizations rights. ACS/ISE also allows for authentication and authorization of Controller administrators. The ACS/ISE contains a RADIUS server and the APs and Controllers may be configured to use the RADIUS server in ACS/ISE to carry out their respective TSF authentication and authorization capabilities. The administration capabilities provided by the ACScan be used to setup the policies for access control when the Controllers and APs have been administratively configured to have a RADIUS server carry out authentication and authorization for wireless users of the TOE. These policies include lockout failure settings available on ACS, or through ISE by ISE is referring authentication to a second-tier authentication server such as AD, LDAP, or ACS.</td></tr>
<tr><td>FMT_SMF.1(1)</td><td>See FMT_MOF.1(1)</td></tr>
<tr><td>FMT_SMF.1(2)</td><td>See FMT_MOF.1(2)</td></tr>
<tr><td>FMT_SMF.1(3)</td><td>See FMT_MOF.1(1)</td></tr>
<tr><td>FMT_SMR.1(1)</td><td>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.” Two types of Cisco WLAN Controller administrator accounts are covered by that definition: the Management User accounts; and the SNMPv3 User accounts. The Management User accounts are only able to access interactive administrative interfaces: the Controller GUI via TLS; and the Controller CLI via SSH. The SNMPv3 User accounts are only able to authenticate to the Controller SNMPv3 programmatic interface.

As a programmatic rather than interactive interface some SFRs do not apply to the SNMPv3 interface, including FTA_TAB.1 (displaying a login banner), and FIA_AFL.1 (authentication failure handling). Though the SNMPv3 connection is encrypted, it’s configured to only be accessible from an isolated/protected management network to mitigate the risk of brute-force password guessing.

Since the SNMPv3 User is an external entity instead of a human user, each SNMPv3 User account is to be used by only a single external entity, such as a single NCS, or WCS, and when multiple servers are deployed, they will each use a different SNMPv3 User account. That method ensures that audit records for login attempts, and administrative changes made through the SNMPv3 interface are able to uniquely identify the correct ‘subject’ (SNMPv3 User) that performed an authorized ‘operation’ (GET or SET) on the configuration ‘object’ (MIB object). Each “SNMPv3 User” account is used to authenticate a remote IT entity such as an instance of a NCS, or WCS and is not intended to (re)authenticate administrators who have individually authenticated to a WCS/NCS prior to initiating SNMPv3 GET or SET commands to a Controller. Thus, audit records generated by the Controller of actions performed on a Controller by an “SNMPv3 User” are actions performed by the authenticated NCS/WCS.

<table>
<tr><th>Administrative TOE Role</th><th>When used</th><th>Responsibilities</th></tr>
</table>
</td></tr>
</table>

	Controller Administrator	Used in Setup and Evaluated Configuration	Perform installation, configuration and management activities for Controllers and APs.
	Access Point (AP) Administrator	Setup Only	Installation and initial of AP TOE Components, enabling FIPS mode of operations

The TOE also maintains a non-administrative role for wireless users. Wireless users are not able to authenticate to any administrative interface of the TOE, and cannot modify any TSF data. All entities attempting to authenticate from wireless clients are authenticated as wireless users, and cannot attempt to authenticate as an administrator.

Access Point administrator will be able to log in locally to the AP, only limited capability and data will be accessible and no access to other TOE component data will be available. Write access is not accessible via the AP console. The Console port on the APs is not used during configuration or in the TOEs evaluated configuration and is covered with a tamper evident labelonce the FIPS Kit is installed.

Related TOE IT Environment SFRs:

FMT_SMR.1(2):

There are two administrator roles maintained by the TOE IT Environment in the evaluated configuration, the ACS/ISE Administrator, and the Syslog Administrator. The ACS Administrator is responsible for management of users and their authentication parameters for those Controller administrators that use SSH and TLS to access the Controller. ACS or ISE can be used for authentication of wireless user accounts. The Syslog Administrator manages the syslog server including restricting access to audit records, and configuring the syslog server's selective audit capability.

TOE IT Environment Role	When used	Responsibilities
ACS/ISE Administrator	Used duringSetup and in the Evaluated Configuration	Management of Administrative users for ACS/ISE and Controller and management of wireless clients
Syslog Administrator	Used during setup and in the Evaluated Configuration	Management of the selectable audit capability

FPT_ITT.1

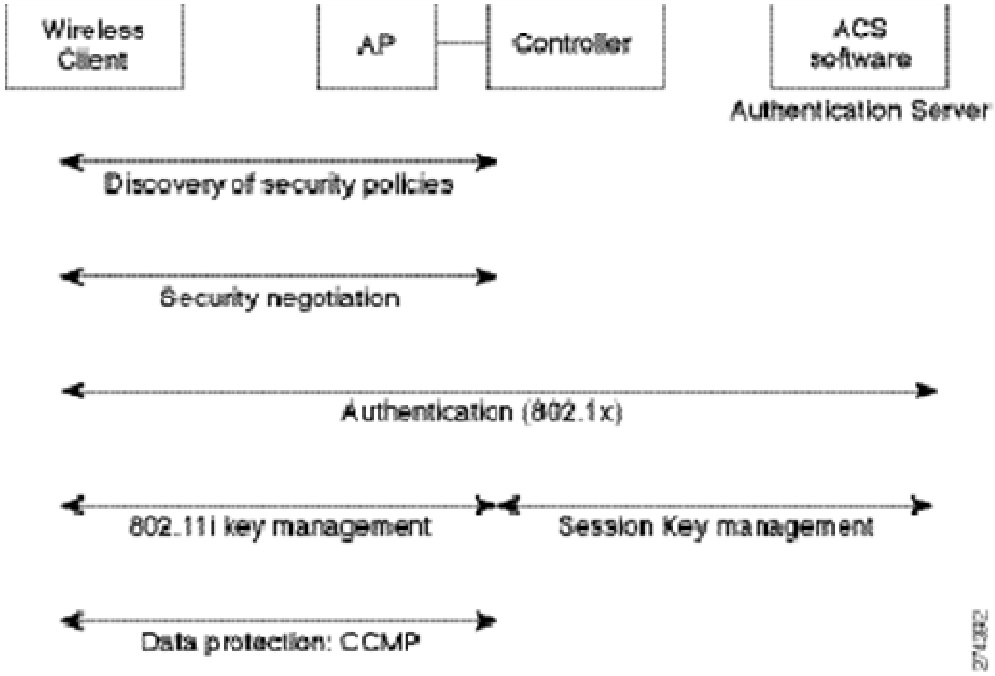
TSF data is protected from modification and disclosure by means of SNMPv3, CAPWAP and AES Key Wrap.

WLAN Internal Data Protection Mechanisms			
Authenticated Connectivity	Protocol	Authentication Mechanism	Description

<table>
<tr><td></td><td><table>
<tr><td>Controller to ACS/ISE</td><td>AES key wrap</td><td>Privacy Password (AES key) and Authentication Password (HMAC-SHA1 key) (passwords are on both systems)</td><td>The keywrap passwords are like pre-shared keys. Once set up correctly on each end then communication between the 2 endpoints takes place using the privacy of the keywrap protocol</td></tr>
<tr><td>Controller to AP</td><td>CAPWAP</td><td>X.509 certificates</td><td>X.509 auth takes place based on factory installed certificates</td></tr>
<tr><td>MSE to Controller</td><td>NMSP (TLS based)</td><td>X.509 certificates</td><td>Authentication takes place based on factory installed</td></tr>
<tr><td>Controller to MSE</td><td>NMSP (TLS based)</td><td>X.509 certificates</td><td>Authentication takes place based on factory installed</td></tr>
<tr><td>WCS or NCS to Controller</td><td>SNMPv3 (sha1/aes)</td><td>Password</td><td>HMAC-SHA-1 based authentication, AES encryption</td></tr>
</table></td></tr>
<tr><td>FPT_STM_(EXT).1</td><td>The Controllers each maintain their own hardware clock, which is settable by the Controller administrator. The Controller may be configured to receive automated clock updates via encrypted and authenticated connection from WCS/NCS. The Controller ensures that each of its managed APs maintain synchronized time with the Controller.
Related TOE IT Environment SFRs:
FPT_STM.1: The ACS/ISE, WCS/NCS, and Syslog server will each maintain their own clock to apply timestamps to the audit records which they generate, and should all be configured to synchronize their clocks with the same centralized time server.
FMT_MTD.1(4): The WCS/NCS administrator is able to set the clock on the WCS/NCS and configure the WCS/NCS to update the Controller clocks via SNMPv3.
FMT_MTD.1(5): The syslog server administrator is able to configure the syslog message filters to select upon receipt at the syslog server’s network interface which messages will be stored in the audit log.</td></tr>
<tr><td>FPT_TST_(EXT).1
FPT_TST.1(1)
FPT_TST.1(2)</td><td>The hardware components of the TOE perform TSF tests during initial start-up of the component. These include the cryptographic module testing on the APs and Controllers. The APs and Controllers also perform a SHA-1integrity check on the configuration files upon initial start up. The results for these tests are reported at the console upon boot up.
The Controller and APs execute FIPS 140-2 power on self tests and conditional tests to ensure the proper operation of the cryptographic functionality, including firmware integrity tests and cryptographic algorithm known answer tests. This verifies the functionality of the cryptographic implementations and the key generation functionality. 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 Management User accounts, not SNMPv3 User 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, not SNMPv3 User accounts.</td></tr>
</table>

FTA_SSL.3	The Controller GUI and CLI interfaces each enforce an inactivity timer and terminate interactive sessions when the time limit has been reached. The GUI timeout is configurable from 30 and 160 minutes (inclusive). The CLI automatically logs out users without saving any changes after an administratively configured time from 1 to 160 minutes, and serial and SSH timeout can be configured to separate limits.
FTA_TAB.1	The Controller management interfaces each display a login banner to administrative users, and optionally for wireless clients.This SFR applies only to interactive administrative interfaces, the Controller CLI, and the Controller GUI, and does not apply to the SNMPv3 interface.
FTP_ITC_(EXT).1(1)	The following Inter-TSF Trusted Channels are provided and utilized by the TOE: • The Controller initiates sending wIPS data to the MSE over TLS. • The Controller initiates sending alerts to WCS/NCS via SNMPv3. • The Controller initiates sending syslog data to the syslog server over TLS. Related TOE IT Environment SFRs: FTP_ITC_(EXT).1(2): • The WCS/NCS initiates encrypted and authenticated communication with the Controller over SNMPv3 to configuration updates, and to update the Controller clock. • The MSE initiates encrypted and authenticated communication with the Controller to update wIPS policies.
FTP_TRP.1	The administrator has control over whether or not unencrypted data will be allowed to pass through the TOE by providing the ability to enable and disable the encryption policy of the TOE. This encryption policy determines whether the APs and Controllers will encrypt and decrypt communications with wireless clients. After a wireless client has successfully authenticated to the TOE the wireless client can communicate with other wireless clients that have successfully authenticated through the TOE and with other wired clients that operate on the wired network controlled by the TOE. If the administrator has enabled encryption, the TOE will encrypt user data transmitted to a wireless client from the radio interface of the wireless access system and decrypt user data received from a wireless client by the radio interface of the wireless access system. This ensures that the TOE supports end-to-end wireless encryption. The TOE allows for the detection of modification of user data while carrying out network communications on the wireless network through the use of AES operating in CCM (CCMP). This is done through this standard through the integrity protection capabilities of the algorithm. The Cipher Block Chaining Message Authentication Code (CBC-MAC) component of CCMP provides data integrity. The CBC-MAC allows for the detection of a modified packet. If a CBC-MAC indicates a packet has been modified the packet is dropped. Details of Wireless User Identification & Authentication The TOE implements WiFi CERTIFIED WPA2 security which also includes IEEE 802.1X port access control to provide for the authentication of wireless clients and to restrict unauthorized access into the TOE. AP components of the TOE use 802.1X port based authentication. When a wireless user attempts to associate to a given network they must first associate with an AP. The TOE maintains the userID and MAC address for the user (and their client) throughout the user's session. During the security policy discovery phase of 802.11i, the wireless client determines the security methods enforced by the TOE which are advertised by the AP. Using those security methods the client responds with a request to authenticate to the TOE. Once the wireless client and AP have negotiated the required security methods the authentication phase of the process is initiated. If a user successfully associates to an AP then the AP only forwards 802.1X EAP authentication packets to the Controller. During this 802.1x authentication state, the AP denies all packets sent by the client which are not 802.1x

EAP packets to pass through the AP. The Controller encapsulates the same user 802.1X packets received from the AP using the RADIUS protocol and forwards them to the ACS/ISE. Once the wireless client has successfully authenticated with WPA2-PSK, EAP-TLS, or EAP-FAST using WPA2 they are granted access to the wired and wireless entities connected to the TOE based on the rights granted to the client by the ACS/ISE and the Controller. See below for this process flow.



The 802.1x protocol allows for different authentication methods. The different authentication methods are provided through the use of the Extensible Authentication Protocol (EAP). There are a variety of EAP variants. The authentication methods and therefore the EAP variants used by this TOE for authentication are EAP-TLS, EAP-MSCHAPv2, EAP-GCT, and EAP-FAST.

The TOE uses a supplicant, authenticator, and authentication server model to perform authentication for wireless users. The supplicant is a wireless client attempting to gain access to the wired network that the TOE controls. The supplicant is not part of the TOE. An example of a supplicant is a laptop computer with a wireless adapter card. For this evaluation the authenticators are the Controllers with the APs providing 802.1x port access control. The authentication server is the ACS/ISE TOE component.

When EAP-TLS, EAP-MSCHAPv2, EAP-GCT or EAP-FAST is configured, mutual authentication is performed between the supplicant (wireless user) and the TOE's authentication server.

The TOE is also able to implement FIPS 140-2 validated WPA2 using pre-share key (WPA2-PSK). Using WPA2-PSK does not require the use of an authentication server. When using WPA2-PSK all authentication is done between the supplicant and the authenticator. The PSK acts as a type of authentication credential when WPA2-PSK is used. Wireless clients trying to connect to the wired network controlled by the TOE needs to know the PSK for their wireless client software to successfully identify and authenticate to the TOE.

With EAP-FAST, EAP-MSCHAPv2, EAP-GCT, and EAP-TLS wireless human users are identified by login/password credentials and the MAC address of the client they are using to access the wired network that is controlled by the TOE. Further, after successful authentication of a wireless client an IP address will be another identifier associated with the

	wireless client that successfully authenticates if the client is using DHCP. If the client is not using DHCP then the IP address already configured into the client will be used as an additional identifier for the client along with the MAC address. The Controller components of the TOE are capable of allowing for wireless administration however this feature is disabled in the evaluated configuration so the TOE does not allow administration from wireless clients.
IPS_SDC_(EXT).1	The AP analyzes wireless network traffic, performing signature matching checks, data integrity checks, and measuring signal strength to generate wIPS audit records and alerts, and to support location tracking of wireless devices.
IPS_ANL_(EXT).1	The Controller has a Wireless Intrusion Prevention System (wIPS) capability that generates audit records based on wireless networking traffic matching a set of predefined signature rules. There is a set of standard signatures and custom signatures may be developed also. The signatures define patterns of information in wireless network traffic that the APs use to monitor the RF environment. wIPS profiles containing signatures are pushed onto Controllers from the wIPS service of a Cisco Mobility Services Engine (MSE) and are stored in flash memory at the Controller and pushed to APs that join the Controller. APs serve as monitors and send alerts to the wIPS service via the Controller as events are detected. The AP sends the message via CAPWAP control plane messaging to the Controller, which sends it to the Mobility Services Engine using the Network Mobility Services Protocol (NMSP) which is built on TLS. The Cisco wIPS is enabled by the MSE, which is an appliance-based solution that centralizes the processing of wIPS data intelligence collected by the APs. The wIPS service on the MSE can configure, monitor, and report wIPS policies and alarms. wIPS policies are not configured on the controller, but can be enabled/disabled at the controller. Instead, WCS or NCS forwards the profile configuration to the MSE's wIPS service, which in turn forwards the profile to the controller. The profile is stored in flash memory on the controller and sent to access points when they join the controller. When an access point disassociates and joins another controller, it receives the wIPS profile from the new controller. Access points in monitor mode send alarms based on the policy profile through the controller to the MSE's wIPS service which stores and processes the alarms and generates SNMP traps if further alerts are required. Alarms are transmitted individually by the APs as they are generated, and repeated in batches periodically, so the MSE can confirm no single alarm was missed. The following categories of attack signatures are included by default: • Broadcast deauthentication frame signatures - During a broadcast deauthentication frame attack, a hacker sends an 802.11 deauthentication frame to the broadcast MAC destination address of another client. This attack causes the destination client to disassociate from the access point and lose its connection. If this action is repeated, the client experiences a denial of service. • NULL probe response signatures - During a NULL probe response attack, a hacker sends a NULL probe response to a wireless client adapter. As a result, the client adapter locks up. • Management frame flood signatures - During a management frame flood attack, a hacker floods an access point with 802.11 management frames. The result is a denial of service to all clients associated or attempting to associate to the access point. This attack can be implemented with different types of management frames: association requests, authentication requests, reassociation requests, probe requests, disassociation requests, deauthentication requests, and reserved management subtypes. • Wellenreiter signature - Wellenreiter is a wireless LAN scanning and discovery utility that can reveal access point and client information. • EAPOL flood signature - During an EAPOL flood attack, a hacker floods the air with EAPOL frames containing 802.1X authentication requests. As a result, the 802.1X

	authentication server cannot respond to all of the requests and fails to send successful authentication responses to valid clients. The result is a denial of service to all affected clients. • NetStumbler signatures - NetStumbler is a wireless LAN scanning utility that reports access point broadcast information (such as operating channel, RSSI information, adapter manufacturer name, SSID, WEP status, and the latitude and longitude of the device running NetStumbler when a GPS is attached).
IPS_RCT_(EXT).1	The AP component enforces policies received via the WLC component from components external to the TOE including MSE (for signatures) and optionally IDS systems (for lists of malicious source IPs).

7.2 Assurance Measures

The TOE satisfies CC EAL4 assurance requirements augmented with ALC_FLR.2. This section identifies the Configuration Management, Delivery and Operation, Development, Flaw Remediation, Guidance Documents, Testing, and Vulnerability Assessment Assurance Measures applied by Cisco to satisfy the CC EAL4 assurance requirements. **Table 18**lists the details.

Table 18 Assurance Measures

Assurance Component	How Requirement Will Be Met
ADV_ARC.1	The architecture of the TOE that is used to protect the TSF documented by Cisco in their development evidence.
ADV_FSP.4	The externally visible interfaces of the TOE used by the users of the TOE along with the description of the security functions and a correspondence between the interfaces and the security functions from the ST are documented by Cisco in their development evidence. The development evidence also contains a tracing to the SFRs described in this ST.
ADV_IMP.1	Cisco provides access to the TSF implementation to the evaluation lab.
ADV_TDS.3	The design of the TOE will be described in the development evidence. This evidence will also contain a tracing to the TSFI defined in the FSP.
AGD_OPE.1	The administrative guidance is detailed to provide descriptions of how administrative users of the TOE can securely administer the TOE using those functions and interfaces detailed in the guidance.
AGD_PRE.1	Cisco documents the installation, generation, and startup procedures so that the users of the TOE can put the components of the TOE in the evaluated configuration.
ALC_CMC.4	Cisco performs configuration management on configuration items of the TOE. Configuration management is performed on the TOE and the implementation representation of the TOE.

ALC_CMS.4	Cisco uniquely identifies configuration items and each release of the TOE has a unique reference. The Configuration Management documentation contains a configuration item list.
ALC_DEL.1	Cisco documents the delivery procedure for the TOE to include the procedure on how to download certain components of the TOE from the Cisco website and how certain components of the TOE are physically delivered to the user. The delivery procedure detail how the end-user may determine if they have the TOE and if the integrity of the TOE has been maintained. Further, the delivery documentation describes how to acquire the proper license keys to use the TOE components.
ALC_DVS.1	Cisco implements security controls over the development environment. Cisco meets these requirements by documenting the security controls.
ALC_FLR.2	Cisco documents the flaw remediation and reporting procedures so that security flaw reports from TOE users can be appropriately acted upon, and TOE users can understand how to submit security flaw reports to the developer.
ALC_LCD.1	Cisco documents the TOE development life-cycle to meet these requirements.
ALC_TAT.1	Cisco uses well-defined development tools for creating the TOE.
ATE_COV.2	Cisco demonstrates the interfaces tested during functional testing using a coverage analysis.
ATE_DPT.2	Cisco demonstrates the TSF subsystems tested during functional testing using a depth analysis.
ATE_FUN.1	Cisco functional testing documentation contains a test plan, a description of the tests, along with the expected and actual results of the test conducted against the functions specified in the ST.
ATE_IND.2	Cisco will help meet the independent testing by providing the TOE to the evaluation facility.
AVA_VAN.3	Cisco will provide the TOE for testing.

8 Rationale

8.1 Security Objectives Rationale

This section demonstrates that the identified security objectives are covering all aspects of the security needs. This includes showing that each threat and assumption is addressed by a security objective and providing the mapping and rationale for the security objectives and the assumptions, threats, and policies identified in the Security Problem Definition.

As noted in section 3.2 and section 3.3.1, some Threats, Policies, Objectives and Assumptions were added to this ST beyond those specified in the WLAN PP. All these modifications augment those that were present in the WLAN PP, and to not interfere with any that were specified in the WLAN PP, and results in a statement of security objectives that is more restrictive than the statement of security objectives in the WLAN PP.

Table 19Threats, Assumptions & Policies to Security Objectives Mapping

	O.ADMIN_GUIDANCE	O.AUDIT_GENERATION	O.CONFIGURATION_IDENTIFICATION	O.CORRECT_TSF_OPERATION	O.CRYPTOGRAPHY	O.CRYPTOGRAPHY_VALIDATED	O.DISPLAY_BANNER	O.DOCUMENTED_DESIGN	O.WIPS_FUNCTIONS	O.MANAGE	O.MEDIATE	O.PARTIAL_FUNCTIONAL_TESTING	O.RESIDUAL_INFORMATION	O.SELF_PROTECTION	O.TIME_STAMPS	O.TOE_ACCESS	O.VULNERABILITY_ANALYSIS	OE.AUDIT_PROTECTION	OE.AUDIT_REVIEW	OE.MANAGE	OE.NO_EVIL	OE.NO_GENERAL_PURPOSE	OE.PHYSICAL	OE.PROTECT_MGMT_COMMS	OE.RESIDUAL_INFORMATION	OE.SELF_PROTECTION	OE.TIME_STAMPS	OE.TOE_ACCESS	OE.TOE_NO_BYPASS	OE.CLIENT_PROTECT
T.ACCIDENTAL_ ADMIN_ ERROR	X									X											X	X								
T.ACCIDENTAL_ CRYPTO_ COMPROMISE													X	X											X	X				
T. MASQUERADE																X												X	X	
T. POOR_DESIGN			X					X									X													
T.POOR_ IMPLEMENTATION			X									X					X													
T.POOR_TEST				X				X				X					X													
T.RESIDUAL_DATA													X												X					
T.TSF_COMPROMISE										X			X	X						X					X	X				
T.UNATTENDED_ SESSION																X														
T.UNAUTHORIZED_ ACCESS										X	X			X		X				X						X		X	X	
T.UNAUTH_ADMIN_ ACCESS	X									X						X				X	X							X		
T.WIRELESS_ INTRUSION									X																					
T.CLIENT_INSECURE																														X
P.ACCESS_BANNER							X																							
P.ACCOUNTABILITY		X								X					X	X		X	X	X							X	X		
P.CRYPTOGRAPHIC					X								X																	
P.CRYPTOGRAPHY_ VALIDATED					X	X																								
P.ENCRYPTED_ CHANNEL					X	X					X													X						
P.NO_AD_HOC_NET WORKS											X																		X	

	O.ADMIN_GUIDANCE	O.AUDIT_GENERATION	O.CONFIGURATION_IDENTIFICATION	O.CORRECT_TSF_OPERATION	O.CRYPTOGRAPHY	O.CRYPTOGRAPHY_VALIDATED	O.DISPLAY_BANNER	O.DOCUMENTED_DESIGN	O.WIPS_FUNCTIONS	O.MANAGE	O.MEDIATE	O.PARTIAL_FUNCTIONAL_TESTING	O.RESIDUAL_INFORMATION	O.SELF_PROTECTION	O.TIME_STAMPS	O.TOE_ACCESS	O.VULNERABILITY_ANALYSIS	OE.AUDIT_PROTECTION	OE.AUDIT_REVIEW	OE.MANAGE	OE.NO_EVIL	OE.NO_GENERAL_PURPOSE	OE.PHYSICAL	OE.PROTECT_MGMT_COMMS	OE.RESIDUAL_INFORMATION	OE.SELF_PROTECTION	OE.TIME_STAMPS	OE.TOE_ACCESS	OE.TOE_NO_BYPASS	OE.CLIENT_PROTECT
P.WIRELESS_ LOCATION_POLICY									X																					
A.NO_EVIL																					X									
A.NO_GENERAL_ PURPOSE																						X								
A.PHYSICAL																							X							
A.TOE_NO_BYPASS																													X	
A.CLIENT_PROTECT																														X

Table 20Threats, Assumptions & Policies to Security Objectives Rationale

Threat/Assumption/Policy	Security Objectives Rationale
T.ACCIDENTAL_ADMIN_ ERROR	O.ADMIN_GUIDANCE helps to mitigate this threat by ensuring the TOE administrators have guidance that instructs them how to administer the TOE in a secure manner. Having this guidance helps to reduce the mistakes that an administrator might make that could cause the TOE to be configured in a way that is insecure. O.MANAGE also contributes to mitigating this threat by providing administrators the capability to view and manage configuration settings. For example, if the administrator made a mistake when configuring the set of permitted users' authentication credentials, providing them the capability to view the lists of authentication credentials affords them the ability to review the list and discover any mistakes that might have been made. OE.NO_EVIL contributes to mitigating this threat by ensuring that the administrators are non-hostile and are trained to appropriately manage and administer the TOE. OE.NO_GENERAL_PURPOSE also helps to mitigate this threat in ensuring that can be no accidental errors by providing that there are no general-purpose or storage repository applications available on the TOE.
T.ACCIDENTAL_CRYPTO_ COMPROMISE	O.RESIDUAL_INFORMATION; OE.RESIDUAL_INFORMATION contributes to the mitigation of this threat by ensuring that any residual data is removed from network packet objects and ensuing that cryptographic material is not accessible once it is no longer needed. O.SELF_PROTECTION ensures that the TOE will have adequate protection from external sources and that all TSP functions are invoked. OE.SELF_PROTECTION ensures that the TOE operationalenvironment will have protection similar to that of the TOE

T. MASQUERADE	O.TOE_ACCESS mitigates this threat by controlling the logical access to the TOE and its resources. By constraining how and when authorized users can access the TOE, and by mandating the type and strength of the authentication mechanism this objective helps mitigate the possibility of a user attempting to login and masquerade as an authorized user. In addition, this objective provides the administrator the means to control the number of failed login attempts a user can generate before an account is locked out, further reducing the possibility of a user gaining unauthorized access to the TOE. Finally, the TOE includes requirements that ensure protected channels are used to authenticate wireless users and to communicate with critical portions of the TOE IT environment. OE.TOE_ACCESS supports the TOE authentication by providing an authentication server in the TOE operationalenvironment. The environment also includes requirements that ensure protected channels are used to communicate with critical portions of the TOE operationalenvironment. OE.TOE_NO_BYPASS contributes to mitigating this threat by ensuring that wireless clients must be configured for all information flowing between a wireless client and any other host on the network without passing through the TOE.
T. POOR_DESIGN	O.CONFIGURATION_IDENTIFICATION plays a role in countering this threat by requiring the developer to provide control of the changes made to the TOE's design documentation and the ability to report and resolve security flaws. O.DOCUMENTED_DESIGN counters this threat, to a degree, by requiring that the TOE be developed using sound engineering principles. The use of a high level design and the functional specification ensure that developers responsible for TOE development understand the overall design of the TOE. This in turn decreases the likelihood of design flaws and increases the chance that accidental design errors will be discovered. ADV_TDS.1 ensures that the TOE design is consistent across the High Level Design and the Functional Specification. O.VULNERABILITY_ANALYSIS_TEST ensure that the TOE has been analyzed for obvious vulnerabilities and that any vulnerabilities found have been removed or otherwise mitigated. This includes analysis of any probabilistic or permutational mechanisms incorporated into the TOE.
T.POOR_IMPLEMENTATION	O.CONFIGURATION_IDENTIFICATION plays a role in countering this threat by requiring the developer to provide control of the changes made to the TOE's design. This ensures that changes to the TOE are performed in structure manner and tracked. O.PARTIAL_FUNCTIONAL_TESTING ensures that the developers provide evidence and demonstration that all security functions perform as specified through independent sample testing. O.VULNERABILITY_ANALYSIS_TEST ensures that the TOE has been analyzed and tested to demonstrate that it is resistant to obvious vulnerabilities.
T.POOR_TEST	O.PARTIAL_FUNCTIONAL_TESTING ensures that the developers provide evidence and demonstration that all security functions perform as specified through independent sample testing. O.CORRECT_ TSF_OPERATION ensure that users can verify the continued correct operation of the TOE after it has been installed in its target environment. O.VULNERABILITY_ANALYSIS_TEST ensures that the TOE has been analyzed and tested to demonstrate that it is resistant to obvious vulnerabilities. O.DOCUMENTED_DESIGN helps to ensure that the TOE's documented design

	satisfies the security functional requirements. In order to ensure the TOE's design is correctly realized in its implementation, the appropriate level of functional testing of the TOE's security mechanisms must be performed during the evaluation of the TOE.
T.RESIDUAL_DATA	O.RESIDUAL_INFORMATION; OE.RESIDUAL_INFORMATION contribute to the mitigation of this threat by ensuring that any residual data is removed from network packet objects and ensuing that cryptographic material is not accessible once it is no longer needed.
T.TSF_COMPROMISE	O.MANAGE mitigates this threat by restricting access to administrative functions and management of TSF data to the administrator. OE.MANAGE ensures that the TOE operationalenvironment limits access to management functions to the administrator. O.RESIDUAL_INFORMATION and OE.RESIDUAL_INFORMATION contributes to the mitigation of this threat by ensuring that any residual data is removed from network packet objects and ensuring that cryptographic material is not accessible once it is no longer needed. O.SELF_PROTECTION requires that the TOE be able to protect itself from tampering and that the security mechanisms in the TOE cannot be bypassed. Without this objective, there could be no assurance that users could not view or modify TSF data or TSF executables. OE.SELF_PROTECTION ensures that the TOE operationalenvironment will have protection similar to that of the TOE.
T.UNATTENDED_ SESSION	The only sessions that are established with the TOE are anticipated to be administrative sessions. Hence, this threat is restricted to administrative sessions. The termination of general user sessions is expected to be handled by the operationalenvironment. O.TOE_ACCESS helps to mitigate this threat by including mechanisms that place controls on administrator sessions. Administrator sessions are dropped after an administrator defined time period of inactivity. Dropping the connection of a session (after the specified time period) reduces the risk of someone accessing the machine where the session was established, thus gaining unauthorized access to the session.

T.UNAUTHORIZED_ ACCESS	O.MEDIATE works to mitigate this threat by ensuring that all network packets that flow through the TOE are subject to the information flow policies. O.TOE_ACCESS and OE.TOE ACCESS The TOE requires authentication prior to gaining access to certain services on or mediated by the TOE. O.SELF_PROTECTION and OE.SELF_PROTECTION The TSF and its environment must ensure that all configured enforcement functions (authentication, access control rules, etc.) must be invoked prior to allowing a user to gain access to TOE or TOE mediated services. O.MANAGEand OE.MANAGE. The TOE and its environment restrict the ability to modify the security attributes associated with access control rules, access to authenticated and unauthenticated services, etc., to the administrator. These objectives ensure that no other user can modify the information flow policy to bypass the intended TOE security policy. OE.TOE_NO_BYPASS contributes to mitigating this threat by ensuring that wireless clients must be configured to use the wireless access system for all information flowing between a wireless client and any other host on the network. If the clients are properly configured, any information passing through the TOE will be inspected to ensure it is authorized by TOE polices.
T.UNAUTH_ADMIN_ACCESS	O.ADMIN_GUIDANCE help to mitigate this threat by ensuring the TOE administrators have guidance that instructs them how to administer the TOE in a secure manner. Having this guidance helps to reduce the mistakes that an administrator might make that could cause the TOE to be configured in a way that is unsecure. O.MANAGE and OE.MANAGE - mitigate this threat by restricting access to administrative functions and management of TSF data to the administrator. O.TOE _ACCESS and OE.TOE_ACCESS helps to mitigate this threat by including mechanisms to authenticate TOE administrators and place controls on administrator sessions. OE.NO_EVIL help to mitigate this threat by ensuring the TOE administrators have guidance that instructs them how to administer the TOE in a secure manner.
T.WIRELESS_INTRUSION	O.WIPS_FUNCTIONS addresses this threat by providing:1) a wIPS analysis function to identify wIPS events; 2) a wIPS audit mechanism to create records based on the observed actions from specific IT System resources; and 3) a wIPS reaction function to deny unauthorized traffic and block rogue access points and clients.
T.CLIENT_INSECURE	OE.CLIENT_PROTECT addresses this threat by ensuring wireless clients and/or their hosts will be configured to not allow unauthorized access to networking services of the wireless client or to stored TOE authentication credentials.
P.ACCESS_BANNER	O.DISPLAY_BANNER satisfies this policy by ensuring that the TOE displays an administrator configurable banner that provides all users with a warning about the unauthorized use of the TOE. A banner will be presented for all TOE services that require authentication. In other words, it will be required for all administrative actions. The presentation of banners prior to actions that take place as a result of the passing of traffic through the TOE is assumed to be provided by the operational environment.

P.ACCOUNTABILITY	O.AUDIT_GENERATION addresses this policy by providing the administrator with the capability of configuring the audit mechanism to record the actions of a specific user, or review the audit trail based on the identity of the user. Additionally, the administrator's ID is recorded when any security relevant change is made to the TOE (e.g., access rule modification, start/stop of the audit mechanism, establishment of a trusted channel, etc.). OE.AUDIT_PROTECTION provides protected storage of TOE and operationalenvironment audit data in the environment. OE.AUDIT_REVIEW - Further supports accountability by providing mechanisms for viewing and sorting the audit logs O.MANAGE ensures that access to administrative functions and management of TSF data is restricted to the administrator. OE.MANAGE ensures that the administrator can manage audit functionality in the TOE operationalenvironment. O.TIME_STAMPS plays a role in supporting this policy by requiring the TOE to provide a reliable time stamp (via an external NTP server). The audit mechanism is required to include the current date and time in each audit record. All audit records that include the user ID, will also include the date and time that the event occurred. OE.TIME_STAMPS ensures that the TOE operationalenvironment provides time services. O.TOE_ACCESS and OE.TOE_ACCESS support this policy by controlling logical access to the TOE and its resources. This objective ensures that users are identified and authenticated so that their actions may be tracked by the administrator.
P.CRYPTOGRAPHY	O.CRYPTOGRAPHY satisfies this policy by requiring the TOE to implement NIST FIPS validated cryptographic services. These services will provide confidentiality and integrity protection of user data while in transit to remote parts of the TOE. O.RESIDUAL_INFORMATION satisfies this policy by ensuring that cryptographic data is cleared according to FIPS 140-2.
P.CRYPTOGRAPHY_ VALIDATED	O.CRYPTOGRAPHY satisfies this policy by requiring the TOE to implement NIST FIPS validated cryptographic services. These services will provide confidentiality and integrity protection of user data while in transit to remote parts of the TOE. O.CRYPTOGRAPHY_VALIDATED satisfies this policy by requiring that all cryptomodules for cryptographic services be NIST 140-2 validated. This will provide assurance that the NIST-approved security functions and random number generation will be in accordance with NIST and validated according the FIPS 140-2.

P.ENCRYPTED_CHANNEL	O.CRYPTOGRAPHY and O.CRYPTOGRAPHY_VALIDATED satisfies this policy by requiring the TOE to implement NIST FIPS validated cryptographic services. These services will provide confidentiality and integrity protection of user data while in transit wireless clients that are authorized to join the network. O.MEDIATE allows the TOE administrator to set a policy to encrypt all wireless traffic. OE.PROTECT_MGMT_COMMS provides that the remote network management information and authentication data will be protected by means of an encrypted channel in the environment.
P.NO_AD_HOC_NET WORKS	O.MEDIATE works to mitigate this policy by ensuring that all network packets that flow through the TOE are subject to the information flow policies. OE.TOE_NO_BYPASS supports this policy by ensuring that wireless clients must be configured to use the wireless access system for all information flowing between a wireless client and any other host on the network. If the clients are properly configured, any information passing through the TOE will be inspected to ensure it is authorized by TOE polices.
P.WIRELESS_LOCATION_ POLICY	O.WIPS_FUNCTIONS addresses this policy by providing an audit mechanism to create records based on the presence and relative location information (based on wireless signal strength detected at one or multiple APs) for ad-hoc rogues, rogue access points, rogue clients and authorized wireless devices.

Five of the security objectives for the IT environment are simply restatements of an assumption found in the Security Problem Definition. Therefore, these five objectives for the environment, OE.NO_EVIL, OE.PHYSICAL, OE.NO_GENERAL_PURPOSE and OE.TOE_NO_BYPASS, and OE.CLIENT_PROTECT traces to the assumptions trivially.

8.2 Rationale for Security Functional Requirements

8.2.1 Rationale for Security Functional Requirements of the TOE Objectives

This section provides rationale for the Security Functional Requirements demonstrating that the Security Functional Requirements are suitable to address the security objectives. Table 21identifies each Security Functional Requirement and the associated TOE security objective(s) addressed by that SFR.

As noted in sections 3.2 and section 3.3.2, some SFRs were added to this ST beyond those specified in the WLAN PP, and some refinements were made to SFRs from the PP. All these modifications serve augment the set of SFRs that were present in the WLAN PP, they do not interfere with any that were specified in the WLAN PP, and the additions and refinements result in a statement of security requirements that is more restrictive than the statement of security requirements in the WLAN PP.

Table 21TOE Security Functional Requirement to TOE Security Objectives Mapping

	O.ADMIN_GUIDANCE	O.AUDIT_GENERATION	O.CONFIGURATION_IDENTIFICATION	O.CORRECT_TSF_OPERATION	O.CRYPTOGRAPHY	O.CRYPTOGRAPHY_VALIDATED	O.DISPLAY_BANNER	O.DOCUMENTED_DESIGN	O.WIPS_FUNCTIONS	O.MANAGE	O.MEDIATE	O.PARTIAL_FUNCTIONAL_TESTING	O.RESIDUAL_INFORMATION	O.SELF_PROTECTION	O.TIME_STAMPS	O.TOE_ACCESS	O.VULNERABILITY_ANALYSIS
FAU_GEN.1(1)		X															
FAU_GEN.2		X															
FAU_SEL.1(1)		X															
FCS_BCM_(EXT).1					X	X											
FCS_CKM.1(1),(2)					X	X											
FCS_CKM.2					X	X											
FCS_CKM_(EXT).2					X	X							X				
FCS_CKM.4					X	X							X				
FCS_COP.1(1),(2),(3),(4)					X	X											
FCS_COP_(EXT).1					X	X											
FDP_PUD_(EXT).1											X						
FDP_RIP.1(1)													X				
FIA_AFL.1(1)																X	
FIA_ATD.1(1),(2)																X	
FIA_UAU.1											X					X	
FIA_UAU_(EXT).5(1)											X					X	
FIA_UID.2											X					X	
FIA_USB.1(1),(2)		X															
FMT_MOF.1(1),(2),(3)										X							
FMT_MSA.2										X							
FMT_MTD.1(1),(2),(3)										X							
FMT_SMF.1(1),(2),(3)										X							
FMT_SMR.1(1)										X							
FPT_ITT.1														X			

	O.ADMIN_GUIDANCE	O.AUDIT_GENERATION	O.CONFIGURATION_IDENTIFICATION	O.CORRECT_TSF_OPERATION	O.CRYPTOGRAPHY	O.CRYPTOGRAPHY_VALIDATED	O.DISPLAY_BANNER	O.DOCUMENTED_DESIGN	O.WIPS_FUNCTIONS	O.MANAGE	O.MEDIATE	O.PARTIAL_FUNCTIONAL_TESTING	O.RESIDUAL_INFORMATION	O.SELF_PROTECTION	O.TIME_STAMPS	O.TOE_ACCESS	O.VULNERABILITY_ANALYSIS
FPT_STM_(EXT).1		X													X		
FPT_TST_(EXT).1				X													
FPT_TST.1(1),(2)				X													
FTA_SSL.3																X	
FTA_TAB.1							X										
FTP_ITC_(EXT).1		X														X	
FTP_TRP.1																X	
IPS_SDC_(EXT).1									X								
IPS_ANL_(EXT).1									X								
IPS_RCT_(EXT).1									X								
ADV_ARC.1														X			
ADV_FSP.4								X									
ADV_TDS.3								X									
AGD_OPE.1	X																
AGD_PRE.1	X																
ALC_CMC.4			X														
ALC_CMS.4			X														
ALC_DEL.1	X																
ALC_FLR.2			X														
ATE_COV.2												X					
ATE_DPT.2												X					
ATE_FUN.1												X					
ATE_IND.2												X					
AVA_VAN.3																	X

Table 22TOE Security Functional Requirement to TOE Security Objectives Rationale

Security Objective (TOE)	Security Functional Requirement Rationale
O.ADMIN_GUIDANCE	ALC_DEL.1 ensures that the administrator has the ability to begin their TOE installation with a *clean* (e.g., malicious code has not been inserted once it has left the developer's control) version of the TOE, which is necessary for secure management of the TOE The AGD_PRE.1 requirement ensures the administrator has the information necessary to install the TOE in the evaluated configuration. Often times a vendor's product contains software that is not part of the TOE and has not been evaluated. The Installation, Generation and Startup (IGS) documentation ensures that once the administrator has followed the installation and configuration guidance the result is a TOE in a secure configuration. The AGD_OPE.1 requirement mandates the developer provide the administrator with guidance on how to operate the TOE in a secure manner. This includes describing the interfaces the administrator uses in managing the TOE and any security parameters that are configurable by the administrator. The documentation also provides a description of how to set up and use the auditing features of the TOE. The AGD_OPE is also intended for non-administrative users. If the TOE provides facilities/interfaces for this type of user, this guidance will describe how to use those interfaces securely. This could include guidance on the setup of wireless clients for use with the TOE. If it is the case that the wireless clients may be configured by administrators that are not administrators of this TOE, then that guidance may be user guidance from the perspective of this TOE. AGD_OPE.1 AND AGD_PRE.1 analysis during evaluation will ensure that the guidance documentation can be followed unambiguously to ensure the TOE is not misconfigured in an insecure state due to confusing guidance.
O.AUDIT_GENERATION	FAU_GEN.1(1) defines the set of events that the TOE must be capable of recording. This requirement ensures that the administrator has the ability to audit any security relevant event that takes place in the TOE. This requirement also defines the information that must be contained in the audit record for each auditable event. There is a minimum of information that must be present in every audit record and this requirement defines that, as well as the additional information that must be recorded for each auditable event. FAU_GEN.2 ensures that the audit records associate a user identity with the auditable event. In the case of authorized users, the association is accomplished with the user ID. In all other cases, the association is based on the source network identifier, which is presumed to be the correct identity, but cannot be confirmed since these subjects are not authenticated. FAU_SEL.1(1) allows for the selection of events to be audited. This requires that the criteria used for the selection of auditable events to be defined. For example, the event type can be used as selection criteria for the events to be audited. FIA_USB.1(1), FIA_USB.1(2) play a role is satisfying this objective by requiring a binding of security attributes associated with wireless users and administrators that are authenticated with the subjects that represent them in the TOE. This only applies to authorized users, since the identity of unauthenticated users cannot be confirmed. Therefore, the audit trail may not always have the proper identity of the subject that causes an audit record to be generated (e.g., presumed network address of an unauthenticated user may be a spoofed address). FPT_STM_(EXT).1 supports the audit functionality by ensuring that the TOE is capable of obtaining a time stamp for use in recording audit events. FTP_ITC_(EXT).1 provides a trusted channel for services provided by the TOE

	operational environment (the audit server and the time server).
O.CONFIGURATION_ IDENTIFICATION	ALC_CMC.4 contributes to this objective by requiring the developer have a configuration management plan that describes how changes to the TOE and its evaluation deliverables are managed. ALC_CMS.4 is necessary to define the items that must be under the control of the CM system. This requirement ensures that the TOE implementation representation, design documentation, test documentation (including the executable test suite), user and administrator guidance, and CM documentation are tracked by the CM system. ALC_FLR.2 plays a role in satisfying this objective by requiring the developer to have procedures that address flaws that have been discovered in the product, either through developer actions (e.g., developer testing) or discovery by others. The flaw remediation process used by the developer corrects any discovered flaws and performs an analysis to ensure new flaws are not created while fixing the discovered flaws.
O.CORRECT_TSF_ OPERATION	FPT_TST_(EXT).1, FPT_TST.1(1) and FPT_TST.1(2) are necessary to ensure the correct operation of the TSF hardware and software and FIPS 140-2 self tests.

O.CRYPTOGRAPHY	Baseline cryptographic services are provided in the TOE by FIPS PUB 140-2 compliant modules implemented in hardware, in software, or in hardware/software combinations [FCS_BCM_(EXT).1]. The cryptographic services offered by this baseline capability are augmented and customized in the TOE to support robustness environments. These TOE services are based primarily upon functional security requirements in the areas of key management and cryptographic operations. In the area of key management there are functional requirements that address the generation of symmetric keys [FCS_CKM.1(1)], and the generation of asymmetric keys [FCS_CKM.1(2)]; methods of manual and automated cryptographic key distribution [FCS_CKM.2]; cryptographic key destruction [FCS_CKM.4]; techniques for cryptographic key validation and packaging [FCS_CKM.1]; and cryptographic key handling and storage [FCS_CKM_(EXT).2]. Specific functional requirements in the area of cryptographic operations address data encryption and decryption [FCS_COP.1(1)]; cryptographic signatures [FCS_COP.1(2)]; cryptographic hashing [FCS_COP.1(3)]; cryptographic key agreement [FCS_COP.1(4)]; and improved random number generation [FCS_COP_(EXT).1].
O.CRYPTOGRAPHY_ VALIDATED	Baseline cryptographic services are provided in the TOE by FIPS PUB 140-2 compliant modules implemented in hardware, in software, or in hardware/software combinations [FCS_BCM_(EXT).1]. The cryptographic services offered by this baseline capability are augmented and customized in the TOE to support medium robustness environments. These TOE services are based primarily upon functional security requirements in the areas of key management and cryptographic operations. In the area of key management there are functional requirements that address the generation of symmetric keys [FCS_CKM.1(1)], and the generation of asymmetric keys [FCS_CKM.1(2)]; methods of manual and automated cryptographic key distribution [FCS_CKM.2]; cryptographic key destruction [FCS_CKM.4]; techniques for cryptographic key validation and packaging [FCS_CKM.1]; and cryptographic key handling and storage [FCS_CKM_(EXT).2]. Specific functional requirements in the area of cryptographic operations address data encryption and decryption [FCS_COP.1(1)]; cryptographic signatures [FCS_COP.1(2)]; cryptographic hashing [FCS_COP.1(3)]; cryptographic key agreement [FCS_COP.1(4)]; and improved random number generation [FCS_COP_(EXT).1].
O.DISPLAY_BANNER	FTA_TAB.1 meets this objective by requiring the TOE display an administrator defined banner before a user can establish an authenticated session. This banner is under complete control of the administrator in which they specify any warnings regarding unauthorized use of the TOE and remove any product or version information if they desire. The only time that it is envisioned that an authenticated session would need to be established is for the performance of TOE administration. Bannering is not necessary prior to use of services that pass network traffic through the TOE.
O.DOCUMENTED_ DESIGN	ADV_FSP.4 and ADV_TDS.3 support this objective by requiring that the TOE be developed using sound engineering principles. The use of a high level design and the functional specification ensure that developers responsible for TOE development understand the overall design of the TOE. This in turn decreases the likelihood of design flaws and increases the chance that accidental design errors will be discovered. ADV_FSP.4 and ADV_TDS.3 are also used to ensure that the TOE design is consistent across the Design and the Functional Specification.

O.MANAGE	The FMT requirements are used to satisfy this management objective, as well as other objectives that specify the control of functionality. The requirement's rationale for this objective focuses on the administrator's capability to perform management functions in order to control the behavior of security functions. FMT_MOF.1(1)(2) and (3) ensure that the administrator has the ability manage the cryptographic, audit, and authentication functions. FMT_MSA.2 provides the administrator the ability to accept only secure values and modify security attributes. The requirement FMT_MTD.1(1), (2), and (3) that the administrator can manage TSF data including audit pre-selection, identification and authentication data. FMT_SMR.1(1) defines the specific security roles to be supported. FMT_SMF.1(1), (2), and (3) support this objective in that it identifies the management functions of cryptographic data, audit records, and cryptographic key data.
O.MEDIATE	FDP_PUD_(EXT).1 allows the administrator to control whether or not unencrypted data will be allowed to pass through the TOE. FIA_UAU.1, FIA_UAU_(EXT).5(1) and FIA_UID.2 ensure that the TOE has the ability to mediate packet flow based on the authentication credentials of the wireless user.
O.PARTIAL_ FUNCTIONAL_ TESTING	ATE_FUN.1 requires the developer to provide the necessary test documentation to allow for an independent analysis of the developer's security functional test coverage. In addition, the developer must provide the test suite executables and source code, which the evaluator uses to independently verify the vendor test results and to support of the test coverage analysis activities. ATE_COV.2 requires the developer to provide a test coverage analysis that demonstrates the extent to which the TSFI are tested by the developer's test suite. This component also requires an independent confirmation of the extent of the test suite, which aids in ensuring that correct security relevant functionality of a TSFI is demonstrated through the testing effort. ATE_IND.2 requires an independent confirmation of the developer's test results, by mandating a subset of the test suite be run by an independent party. This component also requires an independent party to craft additional functional tests that address functional behavior that is not demonstrated in the developer's test suite. Upon successful completion of these requirements, the TOE's conformance to the specified security functional requirements will have been demonstrated.

O.RESIDUAL_ INFORMATION	FDP_RIP.1(1) is used to ensure the contents of resources are not available once the resource is reallocated. For this TOE it is critical that the memory used to build network packets is either cleared or that some buffer management scheme be employed to prevent the contents of a packet being disclosed in a subsequent packet (e.g., if padding is used in the construction of a packet, it must not contain another user's data or TSF data). FCS_CKM_(EXT).2 places requirements on how cryptographic keys are managed within the TOE. This requirement places restrictions in addition to FDP_RIP.1(1), in that when a cryptographic key is moved from one location to another (e.g., calculated in some scratch memory and moved to a permanent location) that the memory area is immediately cleared as opposed to waiting until the memory is reallocated to another subject. FCS_CKM.4 applies to the destruction of cryptographic keys used by the TSF. This requirement specifies how and when cryptographic keys must be destroyed. The proper destruction of these keys is critical in ensuring the content of these keys cannot possibly be disclosed when a resource is reallocated to a user.
O.SELF_PROTECTION	ADV_ARC.1 provides the security architecture description of the security domains maintained by the TSF that are consistent with the SFRs**.** Since self-protection is a property of the TSF that is achieved through the design of the TOE and TSF, and enforced by the correct implementation of that design, self-protection will be achieved by that design and implementation. FTP_ITT.1 provides self protection by protection communications between TOE components.
O.TIME_STAMPS	FPT_STM_(EXT).1 requires that the TOE be able to provide reliable time stamps for its own use and therefore, partially satisfies this objective. Time stamps include date and time and are reliable in that they are always available to the TOE, and the clock must be monotonically increasing.

O.TOE_ACCESS	FIA_UID.2 plays a small role in satisfying this objective by ensuring that every user is identified before the TOE performs any mediated functions. In most cases, the identification cannot be authenticated (e.g., a user attempting to send a data packet through the TOE that does not require authentication). It is impractical to require authentication of all users that attempt to send data through the TOE, therefore, the requirements specified in the TOE require authentication where it is deemed necessary. This does impose some risk that a data packet was sent from an identity other than specified in the data packet. FIA_UAU.1, and FIA_UAU_(EXT).5(1) contributes to this objective by ensuring that administrators and users are authenticated before they are provided access to the TOE or its services. In order to control logical access to the TOE, an authentication mechanism is required. The local administrator authentication mechanism is necessary to ensure an administrator has the ability to login to the TOE regardless of network connectivity (e.g., it would be unacceptable if an administrator could not login to the TOE because the authentication server was down, or that the network path to the authentication server was unavailable). FIA_AFL.1(1) ensures that the TOE can protect itself and its users from brute force attacks on their authentication credentials. FIA_ATD.1(1),(2) Management requirements provide additional control to supplement the authentication requirements. FTA_SSL.3 ensures that an inactive user and administrative sessions are dropped. FTP_TRP.1 ensures that remote users have a trusted path in order to authenticate. FTP_ITC_(EXT).1 provides a trusted channel for services provided by the TOE operational environment (the remote authentication server).
O.VULNERABILITY_ ANALYSIS	The AVA_VAN.3 component provides the necessary level of confidence that vulnerabilities do not exist in the TOE that could cause the security policies to be violated. AVA_VAN.3 requires the evaluator to perform a search for potential vulnerabilities in all the TOE deliverables. For those vulnerabilities that are not eliminated by the developer, a rationale must be provided that describes why these vulnerabilities cannot be exploited by a threat agent with a basic attack potential, which is in keeping with the desired assurance level of this TOE. This component provides the confidence that security flaws do not exist in the TOE that could be exploited by a threat agent of basic attack potential to violate the TOE's security policies. For this TOE, the vulnerability analysis is specified for an attack potential of basic. This requirement ensures the evaluator has performed an analysis of the authentication mechanism to ensure the probability of guessing a user's authentication data would require a medium-attack potential, as defined in Annex B of the CEM.
O.WIPS_FUNCTIONS	IPS_SDC_(EXT).1 defines the types of traffic that the AP will be able to collect. IPS_ANL_(EXT).1 defines the set of events that the TOE must be capable of recording. This requirement ensures that the administrator has the ability to audit wIPS security relevant events based on the signature that takes place in the targeted IT System resources. This requirement also defines the information that must be contained in the wIPS audit record for each auditable event. There is a minimum set of information that must be present in every wIPS audit record and this requirement defines that. IPS_RCT_(EXT).1 defines the types of reactions that the AP will be able to take in response to detection of wIPS events.

8.3 TOE Security Functional Component Hierarchies & Dependencies

This section of the ST demonstrates that the identified TOE Security Functional Requirements include the appropriate hierarchical SFRs and dependent SFRs. Table 23 lists the TOE Security Functional Components and the Security Functional Components each are hierarchical to and dependent upon and any necessary rationale. N/A in the Rationale column means the Security Functional Requirement has no dependencies and therefore, no dependency rationale is required. Satisfied in the Rationale column means the Security Functional Requirements dependency was included in the ST.

Table 23TOE Security Functional Requirements Dependency Rationale

Security Functional Requirement (TOE)	Hierarchical To	Dependency	Rationale
FAU_GEN.1(1)	No other components	FPT_STM.1	Satisfied (by FPT_STM_(EXT).1)
FAU_GEN.2	No other components	FAU_GEN.1 FIA_UID.1	Satisfied (by FAU_GEN.1(1) FIA_UID.2
FAU_SEL.1(1)	No other components	FAU_GEN.1; FMT_MTD.1	Satisfied by FAU_GEN.1(1); FMT_MTD.1(1)
FCS_BCM_(EXT).1	N/A	None	N/A
FCS_CKM.1(1)	No other components	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	Satisfied by FCS_CKM_(EXT).2 FCS_COP_(EXT).1 FCS_CKM.4
FCS_CKM.1(2)	No other components	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	Satisfied by FCS_COP.1(1) and FCS_COP.1(2) FCS_CKM.4
FCS_CKM.2	No other components	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	Satisfied by FCS_CKM.1(1) FCS_CKM.4
FCS_CKM_(EXT).2	N/A	[FDP_ITC.1 or FCS_CKM.1]	Satisfied by FCS_CKM.1(1)
FCS_CKM.4	No other components	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Satisfied by FCS_CKM.1(1) FCS_CKM.1(2)

FCS_COP.1(1)	N/A	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	Satisfied by FCS_CKM.1(1) FCS_CKM.4
FCS_COP.1(2)	N/A	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	Satisfied by FCS_CKM.1(2) FCS_CKM.4 FMT_MSA.2
FCS_COP.1(3)	N/A	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	Satisfied by FCS_CKM.1(1) FCS_CKM.4
FCS_COP.1(4)	N/A	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	Satisfied by FCS_CKM.1(1) FCS_CKM.4
FCS_COP_(EXT).1	N/A	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	Satisfied by FCS_CKM.1(1) FCS_CKM.4
FDP_PUD_(EXT).1	N/A	None	N/A
FDP_RIP.1(1)	No other components	None	N/A
FIA_AFL.1(1)	No other components	FIA_UAU.1	Satisfied by FIA_UAU.1
FIA_ATD.1(1)	No other components	None	N/A
FIA_ATD.1(2)	No other components	None	N/A
FIA_UAU.1	No other components	FIA_UID.1	Satisfied by FIA_UID.2
FIA_UAU_(EXT).5(1)	No other components	None	N/A
FIA_UID.2	FIA_UID.1	None	N/A
FIA_USB.1(1)	No other components	FIA_ATD.1	Satisfied by FIA_ATD.1(1)
FIA_USB.1(2)	No other components	FIA_ATD.1	Satisfied by FIA_ATD.1(2)

FMT_MOF. 1(1)	No other components	FMT_SMF.1 FMT_SMR.1	Satisfied by FMT_SMF.1(1) FMT_SMR.1(1)
FMT_MOF. 1(2)	No other components	FMT_SMF.1 FMT_SMR.1	Satisfied by FMT_SMF.1(2) FMT_SMR.1(1)
FMT_MOF.1(3)	No other components	FMT_SMF.1 FMT_SMR.1	Partially satisfied by FMT_SMR.1(1) See Unsupported Dependency Rationale
FMT_MSA.2	No other components	[FDP_ACC.1 or FDP_IFC.1] FMT_MSA.1 FMT_SMR.1	Unsatisfied: See Unsupported Dependency Rationale
FMT_MTD.1(1)	No other components	FMT_SMR.1 FMT_SMF.1	Satisfied by FMT_SMR.1(1) FMT_SMF.1(2)
FMT_MTD.1(2)	No other components	FMT_SMR.1 FMT_SMF.1	Partially satisfied by FMT_SMR.1(1) See Unsupported Dependency Rationale
FMT_MTD.1(3)	No other components	FMT_SMR.1 FMT_SMF.1	Partially satisfied by FMT_SMR.1(1) See Unsupported Dependency Rationale
FMT_SMF.1(1)	No other components	None	N/A
FMT_SMF.1(2)	No other components	None	N/A
FMT_SMF.1(3)	No other components	None	N/A
FMT_SMR.1(1)	No other components	FIA_UID.1	Satisfied by FIA_UID.2
FPT_ITT.1	No other components	None	N/A
FPT_STM_(EXT).1	N/A	None	N/A
FPT_TST_(EXT).1	N/A	None	N/A
FPT_TST.1(1)	N/A	None	N/A

FPT_TST.1(2)	N/A	None	N/A
FTA_SSL.3	No other components	None	N/A
FTA_TAB.1	No other components	None	N/A
FTP_ITC_(EXT).1	N/A	None	N/A
FTP_TRP.1	No other components	None	N/A
IPS_SDC_(EXT).1	N/A	FPT_STM.1	Satisfied FPT_STM.1
IPS_ANL_(EXT).1	N/A	FPT_STM.1	Satisfied FPT_STM.1
IPS_RCT_(EXT).1	N/A	FPT_STM.1	Satisfied FPT_STM.1

Table 24Table 24 identifies the functional requirement, its correspondent dependency and the analysis and rationale for not supporting the dependency in this ST.

Table 24Unsupported Dependency Rationale

Requirement	Unsatisfied Dependencies	Dependency Analysis and Rationale
FMT_MOF.1(3)	FMT_SMF.1	This ST is based on the PP which was validated as acceptable without the inclusion of this dependency.
FMT_MSA.2	FDP_ACC.1 or FDP_IFC.1, FMT_MSA.1	This ST is based on the PP which was validated as acceptable without the inclusion of this dependency.
FMT_MTD.1(2)	FMT_SMR.1 FMT_SMF.1	This ST is based on the PP which was validated as acceptable without the inclusion of this dependency.
FMT_MTD.1(2)	FMT_SMR.1 FMT_SMF.1	This ST is based on the PP which was validated as acceptable without the inclusion of this dependency.

8.4 Rationale for Extended Requirements and Extended Components Definition

Table 25 presents the rationale for the inclusion of the explicit requirements found in this ST.

These requirements were mostly derived from the PP, and were designed to fit into their respective requirement classes: FAU, FCS, FDP, FIA, FPT, and FTP.

Table 25Rationale for Explicit Requirements for the TOE

Explicit Requirement	Identifier	Rationale
FCS_BCM_(EXT).1	Baseline cryptographic module	This explicit requirement is necessary since the CC does not provide a means to specify a cryptographic baseline of implementation.
FCS_CKM_(EXT).2	Cryptographic key handling and storage	This explicit requirement is necessary since the CC does not specifically provide components for key handling and storage.
FCS_COP_(EXT).1	Random number generation	This explicit requirement is necessary since the CC cryptographic operation components address only specific algorithm types and operations requiring specific key sizes.
FDP_PUD_(EXT).1	Protection of User Data	This explicit requirement is necessary because the Common Criteria IFC/AFC requirements do not accommodate access control policies that are not object/attribute based. The FDP_PUP_(EXT).1 requirement allows the administrator allow or disallow access based upon an administrator setting indicating whether or not unencrypted data may transit the wireless LAN.
FIA_UAU_(EXT).5(1)	Multiple authentication mechanisms	This explicit requirement is needed for local administrators because there is concern over whether or not existing CC requirements specifically require that the TSF provide authentication. Authentication provided by the TOE is implied by other FIA_UAU requirements and is generally assumed to be a requirement when other FIA_UAU requirements are included in a TOE. In order to remove any potential confusion about this PP, an explicit requirement for authentication has been included. This PP also requires the IT environment to provide an authentication server to be used for authentication of remote users. It is important to specify that the TSF must provide the means for local administrator authentication in case the TOE cannot communicate with the authentication server. In addition, the TOE must provide the portions of the authentication mechanism necessary to obtain and enforce an authentication decision from the IT environment.
FPT_STM_(EXT).1	Reliable time stamps	This explicitly generated requirement was done because this requirement requires the TSF to be able to ‘obtain’ a reliable time stamp while the CC requirement requires the TOE to supply the time stamp so the two requirements do not require the same functionality.
FPT_TST_(EXT).1	TSF Testing	This explicit requirement is necessary because there are several issues with the CC version of FPT_TST. 1. First, the wording of FPT_TST.

		1.1 appears to make sense only if the TOE includes hardware; it is difficult to imagine what software TSF “self-tests” would be run. Secondly, some TOE data are dynamic (e.g., data in the audit trail, passwords) and so interpretation of “integrity” for FPT_TST. 1.2 is required, leading to potential inconsistencies amongst TOEs. Therefore, the explicit requirement is used in this ST.
FTP_ITC_(EXT).1	Inter-TSF trusted channel	This explicit requirement is necessary because the existing trusted channel requirement is written with the intent of protecting communication between distributed portions of the TOE rather than between the TOE and its trusted IT environment.
IPS_SDC_(EXT).1	IPS Data Collection	This explicit requirement is necessary to define the types of data the AP will be able to collect for internal analysis or for forwarding to the MSE for further analysis.
IPS_ANL_(EXT).1	IPS Analysis	This explicit requirement is necessary to define the types of traffic that the AP will be able to analyze, and the type of data the AP will be able to record with respect to wIPS analysis.
IPS_RCT_(EXT).1	IPS Reaction	This explicit requirement is necessary to define the types of reactions that the AP will be able to take in response to detection of wIPS events.

9 Obtaining Documentation, Support & Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What’s New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html