Cisco Unified Wireless Network and Wireless Intrusion Detection System: Security Target

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Cisco Aironet 1130, 1230, and 1240 AG Series Access Points; Cisco 4400 Series Wireless LAN Controller; Cisco Catalyst 6500 Series Wireless Services Module (WiSM) with the Supervisor 720; Cisco Wireless Control System (WCS); Cisco 2710 Wireless Location Appliance; Kiwi Syslog Daemon; Syslog-ng and Cisco Secure Access Control Server (ACS) Target of Evaluation. 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.

March 23, 2009
Version: 1.0 Final

Table of Contents

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

List of Tables

Security Target Introduction

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

ST and TOE Identification

This section provides information needed to identify and control this ST and its TOE. This ST targets Evaluation Assurance Level EAL2 augmented with ACM_SCP.1, ALC_FLR.2, AVA_MSU.1.

ST Title	Cisco Wireless Local Area Network (WLAN) Access System with Integrated Wireless Intrusion Detection System (WIDS) Security Target
ST Version	Version 1.0 Final
Publication Date	March 23, 2009
Vendor	Cisco Systems, Inc.
TOE Identification	Cisco Unified Wireless Network and Wireless Intrusion Detection System Solution composed of the following components: Cisco Aironet 1130, 1230, and 1240 AG Series Access Points; Cisco 4400 Series Wireless LAN Controllers; Cisco Catalyst 6500 Series Wireless Integrated Services Module (WiSM) with the Supervisor 720; Cisco Wireless Control System (WCS); Cisco Secure Access Control Server (ACS), Cisco 2710 Wireless Location Appliance; Kiwi Syslog Daemon; Syslog-ng
CC Identification	Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005
Common Criteria Conformance Claim	The ST is compliant with the Common Criteria (CC) Version 2.3. The ST is EAL2 Augmented, Part 2 extended, and Part 3 conformant. The augmented components for the EAL2 Augmented assurance package are ACM_SCP.1, ALC_FLR.2, AVA_MSU.1. No NIAP or CCIMB interpretations are applicable to the ST as of February 17, 2006. This ST uses Precedent Decision 0141: Clarification on conformance to consistency issues noted in the U.S. Government Wireless Local Area Network (WLAN) Access System Protection Profile for Basic Robustness Environments This ST uses Precedent Decision 0135: "Overwriting" in the Context of Non-Disk Memory (Medium Robustness Profiles)
Protection Profile Conformance	This ST claims compliance to the US Government Wireless Local Area Network (WLAN), Access System, Protection Profile for Basic Robustness Environments, April 2006, Version 1.0.

Security Target Evaluation Status	Version 1.0 Final
Keywords	Wireless, WLAN, Access Point, AP, WIDS

Security Target Overview

The TOE consists of hardware and software used to provide a Cisco Unified Wireless Network and Wireless Intrusion Detection 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 1130, 1230, and 1240 AG Series Access Points; Cisco 4400 Series Wireless LAN Controllers; Cisco Catalyst 6500 Series Wireless Integrated Services Module (WiSM); Cisco Wireless Control System (WCS); Cisco Secure Access Control Server (ACS); Cisco 2710 Wireless Location Appliance; Kiwi Syslog Daemon; Syslog-ng. 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 or AP TOE component: Cisco Aironet 1130 AG Series Access Point hardware and WLAN software image version 4.1.185.10 FIPS, Cisco Aironet 1230 AG Series Access Point hardware and WLAN software image version 4.1.185.10 FIPS, and Cisco Aironet 1240 AG Series Access Point hardware and WLAN software image version 4.1.185.10 FIPS;
2. The Controller, hereafter referred to as the Controller or the Controller TOE component: Cisco 4400 Series Wireless LAN Controllers hardware and WLAN software image version 4.1.185.10 FIPS;
3. The Wireless Integrated Services Module (WiSM), hereafter referred to as the WiSM or WiSM TOE component: Cisco Catalyst 6500 Series Wireless Integrated Services Module (WiSM) (Version 4.1.185.10 FIPS), Supervisor 720 (version 12.2(18)SXF15A) and all software running on both cards;
4. The Wireless Control System (WCS), hereafter referred to as the WCS or WCS TOE component Cisco Wireless Control System (WCS) Version 4.2.97.0 software distribution; and
5. The Secure Access Control Server (ACS), hereafter referred to as the ACS or ACS TOE component: Cisco Secure Access Control Server (ACS) Version 4.2.0.124.8 software distribution (referred to as version 4.2 in the remainder of this Security Target).
6. The Wireless Location Appliance, hereafter referred to as the Location Appliance or Location Appliance TOE component: Cisco Wireless Location Appliance series 2710 (Software version 3.1.38.0)
7. Syslog, the Kiwi Syslog Daemon Version 8.3.30 software distribution or the Syslog-ng version 2.0.9 software distribution.

This ST is based on the US Government, Wireless Local Area Network (WLAN) Access System, Protection Profile for Basic Robustness Environments, April 2006, version 1.0 and describes Cisco product features that satisfy the security functional and assurance requirements identified in the PP.

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 August 2005, version 2.3, CCMB-2005-08-001
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 2005, version 2.3, CCMB--2005-08-002
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 2005, version 2.3, CCMB-2005-08-003
[CEM]	Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated August 2005, version 2.3 CCMB-2005-08-004
[WLANPP]	US Government, Wireless Local Area Network (WLAN) Access System, Protection Profile for Basic Robustness Environments, April 2006, version 1.0

Acronyms, Abbreviations, and Terms

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

Table 1 Acronyms

Acronyms / Abbreviations	Definition
AAA	Authentication, authorization, and accounting
ACS	Access Control Server
AES	Advanced Encryption Standard
AP	Access Point
CC	Common Criteria for Information Technology Security Evaluation
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology for Information Technology Security
CLI	Command Line Interface
CM	Configuration Management
DBMS	Database Management System
EAL	Evaluation Assurance Level
EAP	Extensible Authentication Protocol
EAP-TLS	Extensible Authentication Protocol-Transport Layer Security
FSP	Functional Specification
GUI	Graphical User Interface
HLD	High Level Design

Table 1 Acronyms (continued)

Acronyms / Abbreviations	Definition
HTTPS	Secure Hypertext Transfer Protocol
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IT	Information Technology
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LEAP	EAP Cisco Wireless authentication type
LWAPP	Lightweight Access Point Protocol
Mbps	Megabits per second
NAS	Network Access Server
NIAP	National Information Assurance Partnership
NIC	Network Interface Card
OS	Operating System
PAC	Private Access Credentials
PKI	Public Key Infrastructure
PMK	Pairwise Master Keys
PP	Protection Profile
PSK	Pre-shared key
RADIUS	Remote Authentication Dial-In User Service
RF	Radio Frequency
RSSI	Received Signal Strength Indication
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SNMPv3	Simple Network Management Protocol version 3
SOF	Strength of Function
SSH	Secure Shell
SSL	Secure Socket Layer
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
WIDS	Wireless Intrusion Detection System
Wi-Fi	Wireless fidelity
WiSM	Wireless Services Module

Table 1 Acronyms (continued)

Acronyms / Abbreviations	Definition
WLAN	Wireless LAN
WPA2	Wi-Fi Protected Access

The following terms are used in this Security Target:

Table 2 Terms

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 Host	The IT Environment that includes the hardware and operating system that hosts 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-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.
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.
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.
WCS Host	The IT Environment that includes the hardware and operating system that hosts the WCS software.
WPA2	Wi-Fi Protected Access

TOE Description

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

TOE Product Type

The Target of Evaluation (TOE) is a Wireless LAN access system (WLAN) with an integrated Wireless Intrusion Detection System (WIDS). The Wireless LAN access system defined in this ST are multiple products operating together to provide secure wireless access to a wired and wireless network. The Wireless Intrusion Detection System defined in this ST are the WIDS capabilities defined in this ST including intrusion detection signatures, rogue AP and rogue device detection with location tracking, and 802.11 management frame protection (MFP). This TOE as identified above is the Cisco Unified Wireless Network and Wireless Intrusion Detection System TOE which provides end-to-end wireless encryption, centralized WLAN management, authentication, authorization, and accounting (AAA) policy enforcement, and wireless intrusion detection (WIDS) with location tracking.

TOE Overview

The TOE is a system of products that are administratively configured to interoperate together to provide a WLAN. The TOE is meant to allow 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 Aironet 1130, 1230, and 1240 AG Series Access Points), Controller TOE components (Cisco 4400 Series Wireless Controllers and the Cisco Catalyst 6500 Series WiSM (Cisco Wireless Services Module) with Supervisor 720), ACS TOE component (Cisco Secure Access Control Server), WCS TOE components (Cisco Wireless Control System), a Location Appliance TOE component (Cisco 2710 Location Appliance), and Syslog TOE component (Kiwi Syslog Daemon and Syslog-ng).

Note that although there are several TOE components, there are only two administrative interfaces: the ACS and the WCS. Because of this, there are two main administrator roles on the TOE. Throughout the ST, these are individually identified as the WCS Administrator or the ACS Administrator where appropriate. Portions of the ST that identify only ‘administrator,’ should be understood to mean both the ACS Administrator and the WCS administrator.

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 “Security Functionality Included in the TOE Physical Boundary Not Included in the TOE’s Logical Boundary” section on page 26. 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 “Security Architecture” section on page 27.

The following table 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 3 TOE Components and Boundary

TOE Component Name	Required Number	Specific Versions	Within TOE Boundary?
AP	One or more	• Cisco Aironet 1130 AG Series Access Points: – AIR-LAP1131AG-A-K9 – AIR-LAP1131AG-C-K9 – AIR-LAP1131AG-E-K9 – AIR-LAP1131AG-I-K9 – AIR-LAP1131AG-J-K9 – AIR-LAP1131AG-K-K9 – AIR-LAP1131AG-N-K9 – AIR-LAP1131AG-P-K9 – AIR-LAP1131AG-S-K9 – AIR-LAP1131AG-T-K9 • Cisco Aironet 1230 AG Series Access Points or: – AIR-LAP1232AG-A-K9 – AIR-LAP1232AG-C-K9 – AIR-LAP1232AG-E-K9 – AIR-LAP1232AG-I-K9 – AIR-LAP1232AG-J-K9 – AIR-LAP1232AG-K-K9 – AIR-LAP1232AG-N-K9 – AIR-LAP1232AG-P-K9 – AIR-LAP1232AG-S-K9 – AIR-LAP1232AG-T-K9 – AIR-AP1232AG-A-K9 – AIR-AP1232AG-C-K9 – AIR-AP1232AG-E-K9 – AIR-AP1232AG-I-K9 – AIR-AP1232AG-J-K9 – AIR-AP1232AG-K-K9 – AIR-AP1232AG-N-K9 – AIR-AP1232AG-P-K9 – AIR-AP1232AG-S-K9 – AIR-AP1232AG-T-K9 • Cisco Aironet 1240 AG Series Access Points – 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-S-K9 – AIR-LAP1242AG-T-K9 Each running software Version 4.1.185.10 FIPS and including the Cisco FIPS kit part number AIRLAP-FIPSKIT	Yes

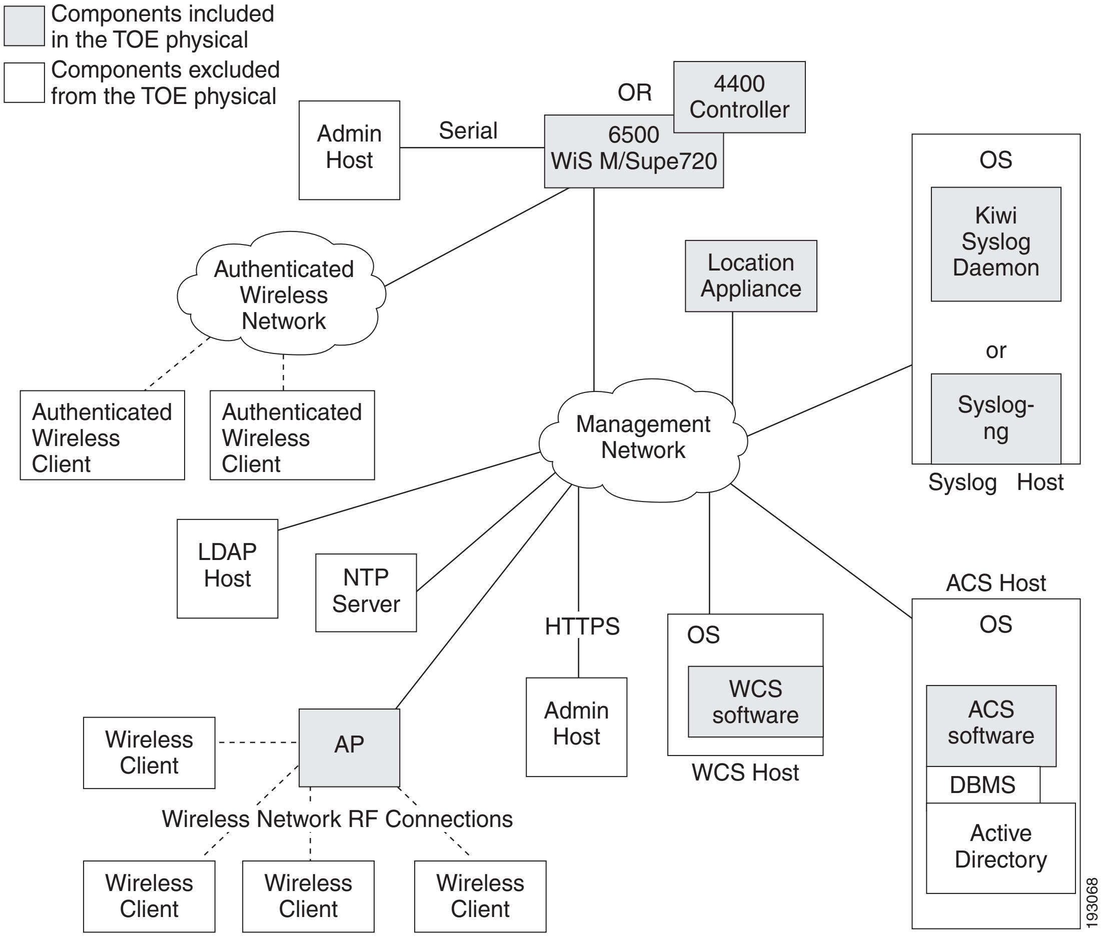
Table 3 TOE Components and Boundary (continued)

TOE Component Name	Required Number	Specific Versions	Within TOE Boundary?
4400 Controller[1] or 6500 WiSM/ Supervisor 720	One or more	• Cisco 4400 Series Wireless LAN Controller running software Version 4.1.185.10 FIPS; and the Cisco FIPS kit part number AIRWLC4400-FIPSKIT – The 4402 Cisco 4400 Series Wireless LAN Controller • AIR-WLC4402-12-K9 • AIR-WLC4402-25-K9 • AIR-WLC4402-50-K9 – The 4404 Cisco 4400 Series Wireless LAN Controller • AIR-WLC4404-100-K9 or • Catalyst 6500 Wireless Integrated Service Module (WiSM) w/software Version 4.1.185.10 FIPS (WS-SVC-WISM-1-K9); Supervisor 720 w/software IOS version 12.2(18)SXF15A; a 6503, 6504, 6506, 6509 or 6513 Catalyst chassis; and the Cisco FIPS kit part number CVPN6500FIPS/KIT	Yes
WCS Software	One	Cisco Wireless Control System (WCS) Version 4.2.97.0	Yes
WCS host OS	One	• Windows 2003 SP1 or greater Server, or • Red Hat Linux AS/ES Version 4 OS	No
ACS Software	One or more	Cisco Secure Access Control Server (ACS) Version 4.2.0.124.8 (available as a patch to the 4.2.0.124 download)	Yes
ACS host OS	One or more (equal to line above)	Windows 2000/2003 Server to host the ACS Software	No
Location Appliance	One or more	Cisco 2710 Wireless Location Appliances running version 3.1.38.0	Yes
Kiwi Syslog Daemon or Syslog-ng	One or more	• Kiwi Syslog Daemon Version 8.3.30, or • Syslog-ng Version 2.0.9	Yes
Syslog host OS	One or more	For Kiwi: • Windows 2000 or 2003 Server For Syslog-ng: • Red Hat Enterprise Linux Version 4 or 5	No
LDAP Host	Optional	No specific version requirements	No
NTP Server	Optional	No specific version requirements	No
Wireless Client	One or more	No specific version requirements	No

[1] Note that Figure 1 shows the 4400 Controller or the 6500 WiSM among the entities connected to the wired network. This is representative of the fact that these two controllers have identical interfaces and functionality.

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 1 Sample TOE Configuration



The following subsections describe the TOE components in detail.

Access Point (AP) TOE Component

The Cisco Aironet 1130 AG Series Access Points; Cisco Aironet 1230 AG Series Access Points; and Cisco Aironet 1240 AG Series Access Points (hereafter referred to as Access Points or APs) provides the connection point between wireless client hosts and the a wired network. Once authenticated as trusted nodes on the wired infrastructure, the APs provide the encryption service on the wireless network between themselves and the wireless client. The APs also communicate directly with the Controller or WiSM for management purposes.

Part of the physical boundary of the APs are 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 three 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 claimed by the TOE.

The serial or console interface to the AP is not included in the evaluated configuration of the TOE. This interface is not used for administration or configuration of the AP TOE component. All administration and configuration of the AP TOE component occurs through the WCS 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 Lightweight Access Point Protocol (LWAPP). LWAPP allows the APs and Controllers to carry out secure control and bridging communications over a FIPS 140-2 validated assured channel using AES-CCM encryption.

The AP maintains a security domain for its own execution. The security domain is all the hardware and software that makes up the AP. The AP maintains the security domain by controlling the actions that can occur at the interfaces described above and providing the hardware resources that carry out the execution of tasks on the AP. Further, the AP provides for isolation of the different wireless clients that have sessions with the WLAN to include maintaining the keys necessary to support encrypted session with wireless devices.

- By the AP controlling the actions and the manner external users may interact with its external interfaces the APs ensure that the enforcement functions of the these components are invoked and succeed before allowing the external user to carry out any other mediate security function with or through the AP.
- Wireless communications between clients and APs is carried out using the IEEE 802.11 protocol standard. The 802.11 standard governs communication transmission for wireless devices. For this evaluation the APs use 802.11a, 802.11b, and 802.11g 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).

Cisco Aironet 1130 AG Series Access Points

The Cisco Aironet 1130AG Series IEEE 802.11a/b/g Access Point is a fixed-configuration dual-band Access Point. The Cisco 1130AG 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 following ten Cisco Aironet 1130 AG Series Access Points which are considered hardware components of the TOE:

1. AIR-LAP1131AG-A-K9
2. AIR-LAP1131AG-C-K9
3. AIR-LAP1131AG-E-K9
4. AIR-LAP1131AG-I-K9
5. AIR-LAP1131AG-J-K9
6. AIR-LAP1131AG-K-K9
7. AIR-LAP1131AG-N-K9
8. AIR-LAP1131AG-P-K9
9. AIR-LAP1131AG-S-K9

10. AIR-LAP1131AG-T-K9

Cisco Aironet 1230AG Series Access Point

The Cisco Aironet 1230AG Series IEEE 802.11 a/b/g Access Point is a fixed-configuration, dual-band access point. Built into the access point are two radios each with dual antenna connectors for diversity. Table 4 lists 20 Cisco Aironet 1230 AG Series Access Points that are included in the TOE's physical boundary and are considered hardware components of the TOE.

Table 4 Cisco Aironet 1230 AG Series Access Points

LWAPP Load	IOS Load
AIR-LAP1232AG-A-K9	AIR-AP1232AG-A-K9
AIR-LAP1232AG-E-K9	AIR-AP1232AG-C-K9
AIR-LAP1232AG-C-K9	AIR-AP1232AG-E-K9
AIR-LAP1232AG-I-K9	AIR-AP1232AG-I-K9
AIR-LAP1232AG-J-K9	AIR-AP1232AG-J-K9
AIR-LAP1232AG-K-K9	AIR-AP1232AG-K-K9
AIR-LAP1232AG-N-K9	AIR-AP1232AG-N-K9
AIR-LAP1232AG-P-K9	AIR-AP1232AG-P-K9
AIR-LAP1232AG-S-K9	AIR-AP1232AG-S-K9
AIR-LAP1232AG-T-K9	AIR-AP1232AG-T-K9

The LWAPP load and IOS load for the APs provide the same functionality. The IOS load of APs provide the same interfaces and management capabilities when they are migrated to LWAPP load during the configuration of these APs.

Cisco Aironet 1240 AG Series Access Point

The Cisco Aironet 1240 AG Series IEEE 802.11 a/b/g Access Point is a fixed-configuration, dual-band access point. Built into the access point are two radios each with dual antenna connectors for diversity. The following nine Cisco Aironet 1240AG Series access points are included in the TOE's physical boundary.

1. AIR-LAP1242AG-A-K9
2. AIR-LAP1242AG-C-K9
3. AIR-LAP1242AG-E-K9
4. AIR-LAP1242AG-N-K9
5. AIR-LAP1242AG-I-K9
6. AIR-LAP1242AG-K-K9
7. AIR-LAP1242AG-P-K9
8. AIR-LAP1242AG-S-K9
9. AIR-LAP1242AG-T-K9

Wireless LAN Controller TOE Component

The wireless LAN controllers TOE components (hereafter referred to as Controller) are used as management devices for one or more APs and the wireless LANs that are implemented on the APs. Through its network interface the Controller communicates with the APs, the WCSs, the Location Appliances, and the ACSs. Through a separate interface, the Controller communicates with the Syslog server. The Controllers provide WLAN security, monitoring, quality of service and radio resource management services for APs over redundant Gigabit Ethernet network interfaces. The security management services provided by the Controllers for APs range from 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 monitoring management services provided by the Controllers are 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 WIDS (wireless intrusion detection signatures) alerts, rogue device alerts, 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. Neither of these are included in the evaluated configuration of the TOE. After installation and initial FIPS 140-2 configuration of the Controller, these interfaces are not used for administration of the Controller TOE component.
- The administrative interface to the Controller is the WCS. WCS provides a graphical interface to the management capabilities of the Controller and communicates with Controllers using SNMPv3. The SNMPv3 module is installed as part of the WCS software. With the WCS interface to the Controller, the Controller requires that the WCS has the same password and privilege password that was configured into the Controller during initial configuration. The Controller ensures that this interface is invoked when a user is trying to use it and succeeds before allowing them to carry out any other mediated security function of the Controller.
- AES RADIUS key wrap is used to protect the 802.11i PMK distributed from ACS to the Controller after a successful wireless user authentication. The Controller ensures that this management interface between the Controller and the ACS is invoked and succeeds before allowing any other mediate security function dealing with authentication or accounting to proceed.
- The Controller interfaces with the Location Appliance. The interfaces between these two components are controlled by SNMPv3. The Controller ensures that the SNMPv3 enforcement interface is invoked and succeeds before allowing any other mediated security function between the Controller and Location Appliance to succeed that deal with transferring RSSI information that is used to calculate location of wireless devices.
- Lastly 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

By the Controller ensuring that all management interface enforcement functions succeed between the APs, WCSs, and ACSs before allowing any other mediated security function with the Controller to proceed, the Controller is enforcing non-bypassability of its security functions.

By utilizing a separate interface (and protected network) for connectivity with the Syslog server, the Controller enforces protection of audit events being logged.

The Controller maintains a security domain for its own use. The security domain is all the hardware and software that makes up the Controller.

- The Controller provides for isolation of management activities from regular user network communication flows by maintaining separation between administrative users interacting either locally or remotely from wireless users of the WLAN.

- By the Controller controlling all its interfaces and providing isolation of privileged administrative activities from wireless user communication flows the Controller maintains a security domains that protects if from interference and tampering by potentially untrusted subjects.

The wireless LAN (WLAN) controllers that are under evaluation are the Cisco 4400 series Controllers and the Catalyst 6500 WiSM Controllers.

Cisco 4400 Series Wireless LAN Controller Products

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. Table 5 provides a complete list of Cisco 4400 Wireless LAN Controller products included in the TOE's physical boundary.

The 4400 Controller TOE component supports one physical configuration interface, the WCS. WCS is the SNMPv3 client for all administration of the Controller TOE component.

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.

Table 5 Cisco 4400 WLAN Controller Products

Product Number	Gigabit Ethernet Ports Supported	Number of APs Supported
AIR-WLC4402-12-K9	2	12
AIR-WLC4402-25-K9	2	25
AIR-WLC4402-50-K9	2	50
AIR-WLC4404-100-K9	4	100

Catalyst 6500 WiSM Controller Family

The WiSM functionally is the same as the 4400 Controller. The Catalyst 6500 WiSM along with Supervisor 720 are hardware modules that plug into a Catalyst 6500 switch chassis. The Catalyst 6500 WiSM controller works with the Supervisor 720 to control access points. Each WiSM blade supports up to 300 Access Points. The Supervisor 720 provides the management interface to the WiSM.

The following five chassis are included in the TOE physical boundary to support the Catalyst 6500 WiSM controller TOE component. 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 blades with support for 1200 APs can be managed by a single 6509 or 6506 Catalyst chassis with a Supervisor 720. A fifth WiSM blade can be installed in the Catalyst 6509 or 6506 chassis for redundant failover. The following five chassis are included in the TOE physical boundary.

1. Catalyst 6503 chassis with Supervisor 720

2. Catalyst 6504 chassis with Supervisor 720
3. Catalyst 6506 chassis with Supervisor 720
4. Catalyst 6509 chassis with Supervisor 720
5. Catalyst 6513 chassis with Supervisor 720

Part of the physical boundary of the Catalyst 6500 series WiSM controller are FIPS Kits that change the physical interfaces of the Catalyst 6500 series WiSM controller to make them FIPS compliant. The FIPS Kits are part of the physical boundary of the Catalyst 6500 series WiSM controller. The FIPS Kits for the Catalyst 6500 series WiSM controllers are the Cisco product number CVPN6500FIPS/KIT.

Wireless Controller System (WCS) TOE Component

The Cisco Wireless Control System (WCS) Version 4.2.97.0 (hereafter referred to as WCS) is a software product that provides a centralized management service for WCS administrators to manage Cisco WLAN products, including the Cisco Access Points (APs), Cisco WLAN Controllers (Controllers), and Cisco Location Appliances. WCS also provides centralized management for the Wireless Intrusion Detection (WIDS) and location tracking functionality of the TOE. The WCS provides the only administrative interface for management of the Controller TOE component.

The WCS runs on a separate dedicated host, the WCS Host, and operates under Windows 2003 SP1 or greater Server or Red Hat Linux AS/ES Version 4.0 OS. The WCS provides graphical user interface (GUI) management support that enables the WCS administrators to manage and monitor the AP, Controller, and Location Servers (discussed in a forward section) and the wireless LAN (WLAN) system that these TOE components form.

WCS Administrators interface to the WCS via the WCS Host's or connecting to the WCS through a web browser (via HTTPS) on another IT Environment supplied administrative host. The WCS Host interfaces to the controllers via the SNMPv3 interface supplied by the WCS Host. The WCS provides high resolution location tracking, detailed WIDS reporting, network diagnostic screens, on demand charting and reporting, and configurable administrative tasks. In addition WCS provides centralized management capabilities that enable the WCS administrators to configure multiple Controllers and Location Servers from a single source using configurable templates. WCS allows WCS administrators to centrally push out policies to one or multiple Controllers.

The TOE component of the WCS is the Cisco Wireless Control System (WCS) Version 4.2.97.0 software distribution. The IT Environment supplies the WCS Host Hardware, WCS Host OS, and Ethernet network hardware. The WCS provides the management interface to the Controllers and Location Appliances. To access this management interface all users must first identify and authenticates themselves to the WCS. The WCS has network communication interfaces to the Controllers and Location Appliances. The network communication interfaces to the Controller and Location Appliance are controlled using SNMPv3. SNMPv3 provides the interface that Controllers, Location Appliances, and WCSs use to communicate with one another, once they are configured to do so. The WCS 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 mediate action to occur with any of its other security functions. Through these mediation and access control features of the interfaces of the WCS, the WCS achieves non-bypassability.

The WCS maintains a security domain by controlling the interfaces that are used by human users and the network communication interface that interacts with the Controllers and Location Appliances so that there is no arbitrary entry into or return from the secure domain of the WCS.

- Through the WCS control and mediation of its controlled interfaces it ensures that the resources and TSF data in the security domain of the WCS are not observed or modified by external users that are not supposed to have access to the resources and TSF data of the WCS.

- Through the strictly controlled interfaces of the WCS and only supplying a well defined set of features that identified and authenticated users may use and how a use can gain entry into and be returned from the security domain the WCS helps in maintaining a security domains for its own use.

Access Control Server (ACS) TOE Component

The Cisco Secure ACS Version 4.2 (hereafter referred to as the ACS) is a software product that provides centralized authentication, authorization and accounting. The ACS centralizes access control and accounting and enables ACS 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 WCS administrator account information attempting to access WCS to manage Controllers.

ACS runs on a dedicated host, the ACS Host. The IT Environment supplies the ACS Host Hardware, ACS Host OS which is Windows 2000/2003 Server, web browser, and Ethernet network hardware that connects the ACS Host to the wired network.

The Controller can be configured to require the APs to use the ACS to perform RADIUS authentication, authorization and accounting of wireless clients that connect to the TOE. When this is done the Controller is configured into ACS as an AAA client which enables APs to pass secure wireless user authentication requests 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.

For this evaluation the AAA server is the ACS. The RADIUS protocol is then used to communicate the 802.1X authentication information between the Controller and ACS. ACS verifies the username and password using the user databases it is configured to query, such as the local ACS user database, or a RADIUS store. ACS returns a success or failure response to the AP, which permits or denies user access, based on the response it receives. When the user authenticates successfully, ACS 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 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 is also responsible for authentication, authorization and accounting for administrators of the TOE. All administrator actions for management of the TOE occur on the WCS. The WCS is the AAA client for the AAA ACS server for RADIUS. WCS Administrators are configured through ACS for authentication and authorization using RADIUS. Controller TACACS+ accounting is used by ACS for logging administrator actions on the WCS.

- The network communication interface between ACS 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 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 the ACS achieves non-bypassability.

ACS Administrators interface to the ACS GUI via the ACS Host's web browser interface or remotely via the ACS Host's Ethernet interface using HTTPS. To access the management interface (the GUI) all users must first identify and authenticates themselves to the ACS host.

A separate interface and protected network are used to connect the ACS to the Syslog server in order to protect the transfer of audit records.

Cisco Wireless Location Appliance TOE Component

The Cisco Wireless Location Appliance series 2710 TOE Component (hereafter referred to as the Location Appliance) is a hardware appliance that collects received signal strength indication (RSSI) information from Controllers so that the Location Appliance can perform computations that determine the location of wireless intrusions or attacks such as rogue clients and rogue APs, the location of authorized clients and authorized APs, and the location 802.11 RFID tags to within several feet of their actual location. RSSI measures the power of a signal that the AP received from a wireless device. The Location Appliance actively collects RSSI information from Controllers with which the Location Appliance has been associated.

After an initial configuration of the Location Appliance through its command line interface (CLI), management of the Location Appliance is performed through WCS. The location data is then synchronized between the Location Appliance and the WCS, allowing administrators access to view it. The data can be sent using different transport types, including: SOAP or SNMP in the evaluated configuration. SOAP specifies Simple Object Access Protocol, a simple XML protocol, as the transport type

- For sending event notifications. SOAP sends notifications over HTTPS, and SNMP utilizes the protection of SNMPv3. The Location Appliance provides the location data that is necessary to determine the physical location of wireless devices within the RF domain of an AP associated with a Controller. Location information is displayed to users on a map that has been configured into the WCS.
- The map that is maintained by the WCS is setup during installation by the WCS administrator who places APs on the graphical map displayed by WCS.

The Location Appliance is a self contained hardware and software appliance. The Location Appliance controls and mediates all activities dealing with the management of the component and the communication that the Location Appliance does with the Controllers and WCSs.

- The Location Appliance provides a well defined management and communication interface that is restricted to performing only those activities necessary to gather information from the Controllers to perform location computation and posting the results of calculations to the WCS, and allowing management activities dealing with the association of Location Appliances with controllers and synchronization of the Location Appliance with the WCS that they have been associated with.
- The Location Appliance mediates the interfaces and communications and makes sure that the security enforcement functions are invoked and succeed before allowing any other mediate security function to be used. By doing this the Location Appliance ensures that it and its security functions are non-bypassable.

The CLI interface of the Location Appliance TOE component is not included in the evaluated configuration. After installation and initial configuration, this interface is not used for administration of the Location Appliance TOE component. All administration of the Location Appliance occurs through the WCS TOE component.

Syslog TOE Component

The Syslog TOE Component is made up of two different software syslog daemons: Kiwi Syslog and Syslog-ng. The Syslog daemons provide storage of audit data forwarded on from the Cisco ACS server and post-selection filtering of the audit data. Only one of the Syslog daemons is required for use with each TOE instance. Kiwi Syslog runs as an application on a Windows platform, and Syslog-ng runs as a system daemon on a UNIX platform.

The Kiwi Syslog Daemon that is included in the TOE is the version 8.3.30 software distribution. The physical boundary of the component is supplied by the software distribution. The IT Environment supplies the workstation hardware and OS.

The Syslog-ng that is included in the TOE is the version 2.0.9 software distribution. The physical boundary of the component is supplied by the software distribution. The IT Environment supplies the workstation hardware and OS.

The Syslog server sits on a separate protected network that allows it to receive audit records from the Controller and ACS.

TOE Logical Boundary

This section identifies the security functions that the TSF provides.

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

Administration (FMT)

The TOE's Administrator security functions provides security capabilities that guarantees all administrators are required to identify and authenticate to the TOE before any administrative or monitoring actions can be performed. The TOE only allows administration of the TOE 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.

Audit (FAU)

The TOE's Audit security function supports audit record generation and selective audit record generation functionality. 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.

- The TOE will generate a WIDS audit record that contains events about an IT system.

- The TOE monitors the wireless network traffic and performs analysis based on the information it has collected and generates events/alerts for potential intrusions that it has identified. The TOE has 17 standard Wireless Intrusion Detection Signatures (WIDS) which it uses to detect unauthorized or threatening WLAN activity including the following:
  - Denial of service/interference events, including
    - Association Request Flood
    - Reassociation Request Flood
    - Broadcast Request Flood
    - Disassociation Flood
    - Deauthentication Flood
    - EAPOL Flood
  - Events matching attack signatures, including
    - NULL Probe Response – Zero length SSID element
    - NULL Probe Response – No SSID element
    - Broadcast Deauthentication Frame
    - Reserved Management sub-types 6 and 7
    - Reserved Management sub-type D
    - Reserved Management sub-types E and F
    - NetStumbler 0.3.20
    - NetStumbler 0.3.23
    - NetStumbler 0.3.30
    - NetStumbler Generic
    - Wellenreiter
- Additionally, all administrator actions related to the management of TSF data and configuration data are logged by the TOE's audit generation functionality.

These audit records are viewable through the TOE's audit data viewing capability.

Encryption (FCS)

The TOE's wireless network Encryption security function ensure that when an administrator has configured encryption that all network packet data payloads are encrypted with the scheme defined by the administrator for those 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.

Identification and Authentication (FIA)

The TOE's Identification and Authentication security function provides I&A support of all wireless client hosts connecting to the trusted wired network from the wireless network along with providing I&A support to make sure all administrators are properly identified and authenticated before accessing TOE functionality.

Information Flow Control (FDP)

The TOE's Information Flow Control security function provides control of information by enforcing the encryption scheme that has been administratively configured.

Self Protection (FPT)

The TOE provides for non-bypassability and domain separation of functions within the TOE's scope of control (TSC). 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 ensures that no security functions within the TSC are bypassed and that there is a separate domain for the TOE that prevents the TOE from being interfered or tampered with for those users that are within the TSC.

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.

Wireless Client Hosts

All wireless client hosts connecting to the wired network from the wireless network are not included in the TOE's physical boundary.

Administrator Management Hosts

The TOE controllers, WCS Host and ACS Host all support remote access from a workstation via HTTPS. Additionally, the controllers support serial access from a workstation. Administrator Management Hosts are not included in the TOE's physical boundary.

ACS Host and OS

The TOE's ACS software distribution is included in the TOE's physical boundary. The resident ACS host and resident OS are not included in the TOE's physical boundary.

WCS Host and OS

The TOE's WCS software distribution is included in the TOE's physical boundary. The resident WCS host and resident OS are not included in the TOE's physical boundary.

Syslog Host and OS

The TOE's Kiwi Syslog Daemon and Syslog-ng software distributions are included in the TOE's physical boundary. The resident Syslog host and resident OS are not included in the TOE's physical boundary.

Networks

The ACS can be configured to retrieve certificates from an LDAP Host. The LDAP software and hardware are not included in the TOE's physical boundary.

ACS Host resident Active Directory implementation

The ACS can be configured to retrieve certificates from an LDAP Host or the ACS resident host's active directory implementation. The Active Directory implementation is not included in the TOE's physical boundary.

LDAP Host and Software

The ACS can be configured to retrieve certificates from an LDAP Host. The LDAP software and hardware are not included in the TOE's physical boundary.

ACS Host Resident DBMS Implementation

The ACS requires a DBMS implementation to store user security attributes. The DBMS software is not included in the TOE's physical boundary."

LDAP Host

The ACS can be configured to retrieve certificates from an LDAP Host. The LDAP software and hardware are not included in the TOE's physical boundary.

Hardware and OS Non-bypassability and Domain Separation Functionality

The responsibility for non-bypassability and separation for the WCS and ACS are split between the TOE and IT Environment supplied hardware and OS.

ACS Windows Web Client Java Runtime Environment (JRE) 1.4.2_04 or later

The ACS requires that JRE be installed on the client for proper display and operation of the ACS WEB GUI interface.

Security Functionality Included in the TOE Physical Boundary 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.

Identification and Authentication

ACS supports many different I&A protocols, and only a subset are included within the TOE. Table 6 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.

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

	I&A Wireless Agent Host	Administrative Hosts
ASCII/PAP	not supported	Supported
CHAP	not supported	Supported
MS-CHAP	not supported	not supported

Table 6 ACS I&A Methods Included in the TOE Physical Boundary (continued)

	I&A Wireless Agent Host	Administrative Hosts
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

Lightweight Access Point Protocol (LWAPP) Layer 2

The Lightweight Access Point Protocol (LWAPP) 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, LWAPP supports traffic handling, authentication, encryption and policy enforcement. LWAPP is the underlying protocol selected by the IETF Control and Provisioning of Wireless Access Points (CAPWAP) Working Group. LWAPP has also been validated by NIST for FIPS 140-2 Level 2 certification. The optional Layer 2 LWAPP mode is not claimed as security functionality of the TOE. However, the Layer 3 LWAPP mode is included in the evaluated configuration and provides the basis for the TOE's assured communications channel between APs and Controllers.

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 included in the evaluated configuration and performs the auditing functionality of the TOE.

Security Architecture

In the "Non-bypassability and Domain Separation" section on page 69, an explanation is provided for how each TOE component supports the secure operation of the TSF. Below are the explanations of how the IT environment of a component also supports secure operation of the TSF.

WCS TOE Component's IT Environment

The IT Environment of the WCS supplies the operating system (Windows 2003 SP1 or greater Server or Red Hat Linux AS/ES Version 4.0) and the hardware that Windows 2003 SP1 or greater Server or Red Hat Linux AS/ES Version 4.0 runs on to provide the execution environment for the WCS.

With this IT Environment the Windows 2003 SP1 or greater Server or Red Hat Linux AS/ES Version 4.0 platform (here after referred to as the WCS Host) makes sure that all users are identified and authenticated in the IT Environment before they are allowed to carry out any other mediated action with WCS Host and the resources that the WCS Host controls. (Note that the environment is not relied upon for identification and authentication of the WCS administrators. This is done by WCS, itself.) The WCS Host provides the control and mediation of network interfaces to the platform hosting the WCS. The ability of the WCS Host to mediate and control all the interfaces to it allows for the IT Environment to make sure that its enforcement functions are invoked and succeed before allowing any other mediated action with any of the other security functions hosted by the WCS Host. This provides for the non-bypassability of the IT Environment along with supporting the non-bypassability of the WCS operating on the host platform that includes the hardware. By the WCS Host providing non-bypassability it ensures that users on the OS are controlled and only use those interfaces and have access to those resources they are authorized for which helps in the non-bypassability of the WCS by controlling and giving access to those interfaces that are within the control of the WCS.

The WCS Host supplies process, memory, and address isolation for applications and processes that execute on it. Having process, memory, and address isolation allows for WCS Host to establish a security domain for its security functions and allows for the WCS Host to provide separation between running processes. With these mechanisms and the hardware included in the WCS Host which is provided by the IT Environment the IT Environment that the WCS operates in supplies domain separation.

The domain separation supplied by the WCS's IT Environment helps in the self protection of the WCS. The WCS Host provides for the isolation of the WCS process from the other processes executing by providing a separate domain from the other domains for the other processes that are running on the WCS Host. Further, with the physical memory supplied by the IT Environment hardware and the virtual memory capabilities along with the per process memory addressing capabilities of the OS that helps compose the WCS Host an isolated tamper proof security domain that can not be interfered with is provided for the WCS.

ACS TOE Component's IT Environment

The IT Environment of the ACS supplies the operating system (Windows 2000/2003 Server) and the hardware that Windows 2000/2003 Server runs on to provide the execution environment that the ACS runs on.

With this IT Environment the Windows 2000/2003 Server makes sure that all users are identified and authenticated into the IT Environment before they are allowed to carry out any other mediated action with the Windows 2000/2003 Server and the resources that the Window 2000/3 Server controls. The Windows 2000/2003 Server provides the control and mediation of network interfaces to the platform hosting the ACS. The ability of the Windows 2000/2003 Server to mediate and control all the interfaces to it allows for the IT Environment to make sure that its enforcement functions are invoked and succeed before allowing any other mediated action with any of the other security functions hosted by Windows 2000/2003 Server. This provides for the non-bypassability of the IT Environment along with supporting the non-bypassability of the ACS operating on the host platform composed of Windows 2000/2003 Server and the hardware. By Windows 2000/2003 Server providing non-bypassability it ensures that users on the OS are controlled and only use those interfaces and have access to those resources they are authorized for which helps in the non-bypassability of the ACS by controlling and giving access to those interfaces that are within the control of the ACS.

The Windows 2000/2003 Server supplies process, memory, and address isolation for applications and processes that execute on Windows 2000/2003 Server. Having process, memory, and address isolation allows for Windows 2000/2003 Server to establish a security domain for its security functions and allows for Windows 2000/2003 Server to provide separation between running processes. With these mechanisms and the hardware which is provided by the IT Environment for Windows 2000/2003 Server to run on the IT Environment that the ACS operates in supplies domain separation.

The domain separation supplied by the ACS's IT Environment helps in the self protection of the ACS. Windows 2000/2003 Server provides for the isolation of the ACS process from the other processes executing by providing a separate domain from the other domains for the other processes that are running on Windows 2000/2003 Server. Further, with the physical memory supplied by the IT Environment hardware and the virtual memory capabilities along with the per process memory addressing capabilities of the Windows 2000/2003 Server operating system an isolated tamper proof security domain that can not be interfered with is provided for the ACS.

Syslog TOE Component's IT Environment

The IT Environment of the Syslog supplies the operating system (Windows 2000/2003 or Linux) and the Server hardware, providing the execution environment upon which the Syslog software runs.

The IT Environment for the Windows 2000/2003 or Linux Server ensures that all users are identified and authenticated before they are allowed to carry out any other mediated action with the Server.

The Server provides the control and mediation of network interfaces.

- The ability of the Server to mediate and control all the interfaces to it, allows for the IT Environment to make sure that its enforcement functions are invoked and succeed before allowing any other mediated action

This provides non-bypassability of the IT Environment and Syslog software operating on the host platform.

The Server supplies process, memory, and address isolation for applications and processes that execute on the Server. Process, memory, and address isolation allows for the Server to establish a security domain for its security functions and allows for the Server to provide separation between running processes.

TOE Evaluated Configuration

The TOE's evaluated configuration requires one or more instances of a Controller which can be either an instance of the Cisco 4400 series controller or a Cisco Catalyst 6500 WiSM controller (or both); one or more of APs; one or more instances of the WCS; one or more instances of the ACS; one or more instances of the Location Appliance; and one or more instances of the Kiwi Syslog Daemon or Syslog-ng.

Additionally, the following list itemizes the evaluated configuration requirements:

1. The WCS is resident on a WCS Host
2. The ACS is resident on a ACS Host
3. The Syslog is resident on a Syslog Host
4. The WCS is the only interface to be used for management of the Controller, Location Appliance and AP TOE components since it is the only management interface that supports all audit functionality required in the evaluated configuration
5. The Location Appliance CLI, AP CLI, Controller CLI and Controller web interface are not included in the evaluated configuration of the TOE.
6. The Controllers are configured with SNMPv3 enable and SNMPv1 and SNMPv2 disabled
7. AES RADIUS key wrap is enabled between the Controllers and ACSs.
8. HTTP (web) and HTTPS (secure web) are disabled on the Controller
9. Telnet and SSH are disabled on the Controller
10. RADIUS is used for authentication of wireless clients
11. RADIUS is used for authentication and authorization of WCS administrators
12. TACACS+ is used for accounting of WCS administrator actions on the WCS
13. All APs are LWAPP APs

14. FTP, NTP, and TFTP are included locally on the Controller. NTP can be set on the Controller through the WCS, and TFTP can be used by WCS to transfer files to the Controller. A separate NTP server is included in the IT environment for use with the ACS, WCS, and the syslog components.
15. Wireless administration is disabled on the TOE.
16. Automatic administrator login is disabled on ACS to enforce admin login through the ACS GUI.

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 7 details the secure communication methods used between TOE components:

Table 7 TOE Component Communication Methods

TOE Components	Communication Method
WCS and ACS	RADIUS
WCS and Location Appliance	SOAP/XML
Controller and ACS	RADIUS w/ AES Key Wrap
Controller and APs	LWAPP
Controller and Controller	EoIP tunnels using SSL
AP and AP	Authenticated AP to AP wireless neighbor messages
Controller and Location Appliance	SNMPv3
Controller and WCS	SNMPv3

Security Environment

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.

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 8 TOE 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.ONE_WCS_ADMIN	There will be only one human user performing WCS administrator configuration and review functions.
A.SYSLOG_SEP	The syslog communications between the TOE components must happen over a separate protected network from the wireless client network.
A.SYSLOG_ADMIN	On the syslog host, all users are considered to be Syslog administrators.

Threats

Table 9 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 9 Threats

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.

Table 9 Threats (continued)

Threat Name	Threat Definition
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.UNIDENTIFIED_ ACTIONS	The administrator may not have the ability to notice potential security violations, thus limiting the administrator’s ability to identify and take action against a possible security breach.

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 10: Organizational Security Policies identifies the organizational security policies applicable to the WLAN.

Table 10 Organizational 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.CRYPTOGRAPHIC	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 provide location tracking for all 802.11 devices transmitting within the RF environment.

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.

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

Security Objectives for the TOE

Table 11: Security Objectives for the TOE identifies the security objectives of the TOE. These security objectives reflect the stated intent to counter identified threats and/or comply with any security policies identified. An explanation of the relationship between the objectives and the threats/policies is provided in the rationale section of this document.

Table 11 Security 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.IDS_AUDIT_GENERATION	The TOE will provide the capability to detect and create records of security relevant events from targeted IT System resource(s) (including the location of resources) and associate those events with the component that created the record.
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 in accordance with its security policy.

Table 11 Security Objectives for the TOE (continued)

Name	TOE Security Objective
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 time stamps.
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.

Security Objectives for the Environment

The assumptions identified in the "Assumptions" section on page 31 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 12: Security Objectives for the Environment identifies the security objectives for the environment.

Table 12 Security 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.

Table 12 Security Objectives for the Environment (continued)

Name	IT Environment Security Objective
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.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.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.ONE_WCS_ADMIN	The maintainers of the TOE will follow the instructions of the Administrator Guide to ensure that only one WCS Configuration Administrator is permitted.

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 2.3* and all National Information Assurance Partnership (NIAP) and international interpretations with the exception of the items listed below.

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~~** 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. FAU_SAR.1(1)) and the Security Functional Requirement element name followed by the instance number in parenthesis (e.g. FAU_SAR.1.1(1)). This document continues the iteration numbering for Security Functional Requirements that apply to both the TOE and the IT Environment.

Operations already completed within the Protection Profile (US Government Wireless Local Area Network (WLAN) Access System Protection Profile for Basic Robustness Environments, April 2006, Version 1.0) will not be repeated here in the Security Target. Please see the PP for these details.

Explicitly stated SFRs are identified by having a label 'Explicit Stated SFR for the TOE' after the requirement name for TOE SFRs and by having a label 'Explicit Stated SFR for the IT Environment' after the requirement name for IT Environment SFRs.

TOE Security Functional Requirements

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

Table 13 TOE Security Functional Requirements

Functional Component	
FAU_GEN.1(1)	Audit data generation
FAU_GEN.2	User identity association
FAU_GEN_EXP.1	Audit data generation (WIDS audit records)
FAU_SAR.1(1)	Audit review
FAU_SAR.2(1)	Restricted audit review
FAU_SAR.3(1)	Selectable audit review
FAU_SEL.1	Selective audit
FCS_BCM_EXP.1	Explicit: Baseline Cryptographic Module
FCS_CKM.1(1)	Cryptographic key generation
FCS_CKM.1(2)	Cryptographic key generation (SNMP)
FCS_CKM.1(3)	Cryptographic key generation (HTTPS/TLS)
FCS_CKM_EXP.2	Cryptographic key establishment
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1(1)	Cryptographic Operation (SNMP-encrypt)
FCS_COP.1(2)	Cryptographic Operation (SNMP-integrity)
FCS_COP_EXP.1	Explicit: Random Number Generation
FCS_COP_EXP.2	Explicit: Cryptographic Operation
FDP_PUD_EXP.1	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_EXP.5(1)	Multiple authentication mechanisms
FIA_UID.2(1)	User identification before any action
FIA_USB.1(1)	User-subject binding (Administrators)

Table 13 TOE Security Functional Requirements (continued)

Functional Component	
FIA_USB.1(2)	User-subject binding (Wireless Clients)
FMT_MOF.1(1)	Management of security functions behavior (Cryptographic Function)
FMT_MOF.1(2)	Management of security functions behavior (Audit Record Generation)
FMT_MOF.1(3)	Management of security functions behavior (Authentication)
FMT_MSA.2	Secure security attributes
FMT_MTD.1(1)	Management of Audit 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 Functions)
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_RVM.1(1)	Non-bypassability of the TOE Security Policy (TSP)
FPT_SEP.1(1)	TSF domain separation
FPT_STM_EXP.1	Reliable time stamps
FPT_TST_EXP.1	TSF Testing
FPT_TST_EXP.2	TSF Testing of Cryptographic Modules
FTA_SSL.3	TSF-initiated termination
FTA_TAB.1	Default TOE access banners
FTP_ITC_EXP.1(1)	Inter-TSF trusted channel
FTP_TRP.1	Trusted Path

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 14 SFR Auditable Events

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

Table 14 SFR Auditable Events (continued)

Requirement	Auditable Events	Additional Audit Record Contents
FAU_SEL.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_EXP.1	**None**	**None**
FCS_CKM.1(**1**)	Manual load of a key Success and Failure of the cryptographic activity.	The identity of the Administrator performing the function.
FCS_CKM.1(2)	**Manual load of a key** **Success and Failure of the cryptographic activity.**	**The identity of the Administrator performing the function.**
FCS_CKM.1(3)	**Manual load of a key** **Success and Failure of the cryptographic activity.**	**The identity of the Administrator performing the function.**
FCS_CKM_EXP.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 **Success and Failure of the cryptographic activity.**	If available - The identity of the Administrator performing the function
FCS_COP.1(1)	**Success and Failure of cryptographic operation**	**Type of operation**
FCS_COP.1(2)	**Success and Failure of cryptographic operation**	**Type of operation**
FCS_COP_EXP.1	None	None
FCS_COP_EXP.2	None	None
FDP_PUD_EXP.**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) and (2)**	None	None
FIA_UAU.1	Use of the authentication mechanism (success or failure)	User identity - the TOE SHALL NOT record invalid passwords the audit log.
FIA_UAU_EXP.5(**1**)	Failure to receive a response from the remote authentication server	Identification of the Authentication server that did not reply
FIA_UID.2(**1**)	~~None~~ **Unsuccessful use of the user identification mechanism,**	~~None~~ **user identity provided**

Table 14 SFR Auditable Events (continued)

Requirement	Auditable Events	Additional Audit Record Contents
FIA_USB.1**(1) and (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_RVM.1(1)	**None**	**None**
FPT_SEP.1(1)	**None**	**None**
FPT_STM_EXP.1	Changes to the time	None
FPT_TST_EXP.1	Execution of the self test	Success or Failure of test
FPT_TST_EXP.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**

Table 14 SFR Auditable Events (continued)

Requirement	Auditable Events	Additional Audit Record Contents
FTP_ITC_EXP.1(**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 of 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 of 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.

FAU_GEN.2 User Identity Association

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

FAU_GEN_EXP.1 Audit Data Generation (WIDS Audit Records) [Explicit Stated SFR for the TOE]

FAU_GEN_EXP.1.1 The TSF shall be able to generate a WIDS audit record for the following IDS events**:**

a) Denial of service/interference events, including

1) Association Request Flood

2) Reassociation Request Flood

3) Broadcast Request Flood

4) Disassociation Flood

5) Deauthentication Flood

6) EAPOL Flood

b) Events matching attack signatures, including

1) NULL Probe Response – Zero length SSID element

2) NULL Probe Response – No SSID element

3) Broadcast Deauthentication Frame

4) Reserved Management sub-types 6 and 7

5) Reserved Management sub-type D

6) Reserved Management sub-types E and F

7) NetStumbler 0.3.20

8) NetStumbler 0.3.23

9) NetStumbler 0.3.30

10) NetStumbler Generic

11) Wellenreiter

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

d) Events related to detection of rogue access points

e) Events related to detection of rogue clients

f) A violation in the authentication policy of a network

g) A violation in the encryption policy of a network

h) Spoofed 802.11 Management Frames

i) Events related to detection of authorized wireless devices

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

a) Date and time of the event, type of event**,** component identity

FAU_SAR.1(1) Audit Review

FAU_SAR.1.1(1) The TOE shall provide only the **ACS, WCS and Syslog** administrators with the capability to read all audit data from the audit records.

FAU_SAR.1.2(1) The TOE shall provide the audit records in a manner suitable for the administrator to interpret the information.

FAU_SAR.2(1) Restricted Audit Review

FAU_SAR.2.1(1) The TOE shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

Application Note This requirement is split between the TOE and the IT Environment. This TOE iteration applies to the WCS and ACS components of the TOE.

FAU_SAR.3(1) Selectable Audit Review

FAU_SAR.3.1(1) The TOE shall provide the ability to perform *searches, sorting, ordering* of audit data based on event type, date, time, [none].

FAU_SEL.1 Selective Audit

FAU_SEL.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) user identity, event type;

b) device interface, wireless client identity.

FCS_BCM_EXP.1 Explicit: Baseline Cryptographic Module [Explicit Stated SFR for the TOE]

FCS_BCM_EXP.1.1 All cryptographic modules shall comply with FIPS 140-2 when performing FIPS approved cryptographic functions in FIPS approved cryptographic modes of operation.

FCS_BCM_EXP.1.2 The cryptographic module implemented shall have a minimum overall rating of Level 1.

FCS_BCM_EXP.1.3 The FIPS validation testing of the TOE cryptographic module(s) shall be in conformance with FIPS ~~140-1,~~ 140-2~~, or the most recently approved FIPS 140 standard for which NIST is accepting validation reports from Cryptographic Modules Testing laboratories~~.

FCS_CKM.1(1) Crytpographic Key Generation (AES)

FCS_CKM.1.1(1) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [AES-CCM] and specified cryptographic key sizes [128 bits] that meet the following: [SP 800-56].

FCS_CKM.1(2) Cryptographic Key Generation (DES)

FCS_CKM.1.1(2) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [user password conversion] and specified cryptographic key sizes [20 octets (HMAC-SHA-1), 56 bits (DES)] that meet the following: [no standard].

FCS_CKM.1(3) Cryptographic Key Generation (RSA)

FCS_CKM.1.1(3) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [RSA] and specified cryptographic key sizes [1024 bits] that meet the following: [PKCS #1: RSA encryption].

FCS_CKM_EXP.2 Explicit: Cryptographic Key Establishment [Explicit Stated SFR for the TOE]

FCS_CKM_EXP.2.1 The TSF shall provide the following cryptographic key establishment technique: Cryptographic Key Establishment using Manual Loading. The crypto module shall be able to accept as input and be able to output keys in the following circumstances [use of the EAP-TLS, or EAP-FAST authentication capability] in accordance with a specified manual cryptographic key distribution method using FIPS-approved Key Management techniques that meets the FIPS 140-~~1/~~2 Key Management Security Levels 1, Key Entry and Output.

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) The Key Zeroization Requirements in FIPS PUB 140-~~1/~~2 Key Management Security Levels 1;

b) Zeroization of all private cryptographic keys, plaintext cryptographic keys, key data, and all other critical cryptographic security parameters shall be immediate and complete; and

c) The zeroization shall be executed by overwriting the key/critical cryptographic security parameter storage area ~~**three or more times**~~ **one time** with ~~**an alternating pattern**~~ **zeroes**.

d) The TSF shall overwrite each intermediate storage area for private cryptographic keys, plaintext cryptographic keys, and all other critical security parameters ~~**three or more**~~ **one** time~~s~~ with ~~**an alternating pattern**~~ **zeroes** upon the transfer of the key/CSPs to another location.]

Application Note This refinement was made based on PD-0135 and the fact that keys are stored in flash for the TOE; making the refinement the appropriate overwrite action.

FCS_COP.1(1) Cryptographic Operation (SNMP-encryption)

FCS_COP.1.1(1) The TSF shall perform [encryption, and decryption] in accordance with a specified cryptographic algorithm [DES] and cryptographic key sizes [56 bits] that meet the following: [FIPS 46-3].

FCS_COP.1(2) Cryptographic Operation (SNMP-authentication)

Hierarchical to: No other components.

FCS_COP.1.1(2) The TSF shall perform [authentication] in accordance with a specified cryptographic algorithm [HMAC-SHA-1] and cryptographic key sizes [20 octets] that meet the following: [FIPS 180-2].

FCS_COP_EXP.1 Explicit: Random Number Generation [Explicit Stated SFR for the TOE]

FCS_COP_EXP.1.1 The TSF shall perform all Random Number Generation used by the cryptographic functionality of the TSF using a FIPS-approved Random Number Generator implemented in a FIPS-approved crypto module running in a FIPS-approved mode.

FCS_COP_EXP.2 Explicit: Cryptographic Operation [Explicit Stated SFR for the TOE]

FCS_COP_EXP.2.1 A crypto module shall perform encryption and decryption using the FIPS-140-~~1/~~2 Approved *AES* algorithm and operating in [CCM (CCMP)] and supporting FIPS approved key sizes of [128 bits].

FDP_PUD_EXP.1 Protection of User Data [Explicit Stated SFR for the TOE]

FDP_PUD_EXP.1.1 When the WCS administrator has enabled encryption, 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_EXP.2;
- 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_EXP.2.

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

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.

FIA_AFL.1(1) Administrator Authentication Failure Handling

FIA_AFL.1.1(1) The TSF shall detect when an **ACS** administrator configurable positive integer within the range of [1 to 3] 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 until an action is taken by a local **ACS** administrator.

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, privilege].

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: [user ID, password, host MAC address].

FIA_UAU.1 Timing of Local Authentication

FIA_UAU.1.1 The TSF shall allow [access to the syslog component] on behalf of users 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.

Application Note The TOE relies on authentication of users accessing the Syslog Server by its host environment.

Explicit: Multiple Authentication Mechanisms (FIA_UAU_EXP.5(1)) [Explicit Stated SFR for the TOE]

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

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

FIA_UID.2(1) User Identification Before any Action

FIA_UID.2.1(1) The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

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: [password, username, privilege].

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: [upon successful authentication to 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: [administrators may change their own passwords].

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

FIA_USB.1.1(2) The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [user ID, 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 a user ID and 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: [the wireless user may make no changes to their own attributes].

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 **ACS and WCS** administrators.

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 behavior of the functions

- Audit: pre-selection of the events which trigger an audit record,
- Audit: start and stop of the audit function to **ACS and Syslog** administrators.

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 Authentication functions

- 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 **ACS and WCS** administrators.

FMT_MSA.2 Secure Security Attributes

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

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, create the set of rules used to pre-select audit events to the **ACS and Syslog** administrators.

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, user identification credentials to **ACS** administrators.

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

FMT_MTD.1.1(3) The TSF shall restrict the ability to modify the user authentication credentials to ~~TOE users~~ **ACS administrators**.

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_EXP.2) in conformance with the **WCS** administrator's configuration of the TOE.

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.

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_EXP and enable/disable verification of cryptographic key testing.

FMT_SMR.1(1) Security Roles

FMT_SMR.1.1(1) The TSF shall maintain the roles **ACS** administrator, **WCS administrator, Controller administrator, Supervisor administrator, Location Appliance administrator, Access Point administrator, Syslog administrator,** wireless user.

Application Note See Table 18, Administrator Accounts, for an explanation of responsibilities of the administrative roles listed above.

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

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.

FPT_RVM.1(1) Non-Bypassability of the TOE Security Policy (TSP)

FPT_RVM.1.1(1) The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

FPT_SEP.1(1) TSF Domain Separation

FPT_SEP.1.1(1) The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2(1) The TSF shall enforce separation between the security domains of subjects in the TSC.

FPT_STM_EXP.1 Reliable Time Stamps [Explicit Stated SFR for the TOE]

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

FPT_TST_EXP.1 TSF Testing [Explicit Stated SFR for the TOE]

FPT_TST_EXP.1.1 The TSF shall run a suite of self-tests during initial start-up and upon request, to demonstrate the correct operation of the hardware portions of the TSF.

FPT_TST_EXP.1.2 The TSF shall provide the capability to use a TSF-provided cryptographic function to verify the integrity of all TSF data except the following: audit data, *none*.

FPT_TST_EXP.1.3 The TSF shall provide the capability to use a TSF-provided cryptographic function to verify the integrity of stored TSF executable code.

FPT_TST_EXP.2 TSF Testing of Cryptographic Modules [Explicit Stated SFR for the TOE]

FPT_TST_EXP.2.1 The TSF shall run the suite of self-tests provided by the FIPS 140-~~**1/**~~2 crypto module during initial start-up (power on) and upon request, to demonstrate the correct operation of the cryptographic components of the TSF.

FPT_TST_EXP.2.2 The TSF shall be able to run the suite of self-tests provided by the FIPS 140-~~**1/**~~2 crypto module immediately after the generation of a key.

FTA_SSL.3 TSF-Initiated Termination

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

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.

FTP_ITC_EXP.1(1) Inter-TSF Trusted Channel [Explicit Stated SFR for the TOE]

FTP_ITC_EXP.1.1(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_EXP.1.2(1) The TSF shall permit the TSF, or the IT Environment entities to initiate communication via the trusted channel.

FTP_ITC_EXP.1.3(1) The TSF shall initiate communication via the trusted channel for all authentication functions, remote logging, time, [*Management Frame Protection*].

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*].

Security Requirements for the IT Environment

This Security Target provides functional requirements for the IT Environment. The IT environment includes the authentication server, the management console, and the audit collection server, and authorized IT entities (e.g., a certificate authority server, NTP server).

In support of the audit server, the environment shall provide the capability to protect audit information and authentication credentials. The environment shall also provide the capability to selectively view audit data.

In support of the authentication server, the environment shall provide facilities to manage authentication information and limit brute force password attacks.

Communications between these entities and the TOE will be protected. In addition the TOE IT environment is responsible for protecting itself and ensuring that its security mechanisms cannot be bypassed.

The purpose of requirements on the IT environment is to supplement the TOE and to ensure that the TOE and the IT environment together satisfy all security objectives. In order to limit the scope of the IT environment only those IT environmental requirements that directly contribute to the satisfaction of objectives have been included in this ST. Requirements for the IT environment necessary simply to satisfy management guidance, audit guidance, or dependency chains have not been included in this ST.

Table 15 Security Functional Requirements for the TOE IT Environment

Functional Component	
FAU_GEN.1(2)	Audit data generation
FAU_SAR.1(2)	Audit review - Host OS
FAU_SAR.2(2)	Restricted audit review - Host OS
FAU_SAR.2(3)	Restricted audit review - Syslog
FAU_SAR.3(2)	Selectable audit review - Host OS
FAU_STG.1	Protected audit trail storage
FAU_STG.3	Action in case of possible audit data loss
FDP_RIP.1(2)	Subset Residual Information Protection
FIA_AFL.1(2)	Remote User failure handling
FIA_ATD.1(3)	User attribute definition
FIA_UAU_EXP.5(2)	Remote authentication mechanisms
FIA_UAU.2	User authentication before any action
FIA_UID.2(2)	User identification before any action
FMT_MOF.1(4)	Management of Security Functions Behavior
FMT_MTD.1(4)	Management of time data
FMT_SMR.1(2)	Security roles
FTP_ITC_EXP.1(2)	Inter-TSF trusted channel
FPT_RVM.1(2)	Non-bypassability of the TOE Security Policy (TSP)
FPT_SEP.1(2)	TSF domain separation
FPT_STM.1	Reliable time stamps

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) other specifically defined auditable events **in Table 16.**

Table 16 TOE IT Environment Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1(**2**)	None	None
FAU_SAR.1(**2**)	None	None
FAU_SAR.2(**2**)	Unsuccessful attempt to read the audit records	The identity of the user attempting to perform the function
FAU_SAR.3(**2**)	None	None
FAU_STG.1	None	None
FAU_STG.3	Any actions taken when audit trail limits are exceeded	None
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_EXP.5(**2**)	Use of the authentication mechanism (success or failure)	User identity - the TOE IT Environment SHALL NOT record valid or invalid passwords the audit log.
FIA_UAU.2	**Unsuccessful use of the authentication mechanisms**	**None**
~~FIA_UID.1~~ **FIA_UID.2(**2)	**~~None~~ Unsuccessful use of the user identification mechanisms**	**~~None~~ User identify provided.**
FMT_MOF.1(4)	Changes to audit server settings Changes to authentication server settings Changes to time server settings	None
FMT_MTD.1(4**)**	**Setting time/date**	**Identity of the administrator that performed the action**
FMT_SMR.1(**2**)	**~~None~~ Modifications to the group of users that are part of a role**	None

Table 16 TOE IT Environment Auditable Events (continued)

Requirement	Auditable Events	Additional Audit Record Contents
FTP_ITC_EXP.1(**2**)	~~**Initiation/Closure**~~ **Failure** of ~~**a**~~ trusted channel **functions;**	Identification of the **initiator and target of failed trusted channel functions** ~~**remote entity with which the channel was attempted/created;**~~ ~~**Success of failure of the event**~~
FPT_RVM.1(2)	None	None
FPT_SEP.1(2)	None	None
FPT_STM.1	Setting time/date	Identity of the administrator that performed the action

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 (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 T, information specified in column three of Table 16.

Application Note This IT Environment requirement applies to the IT Environment of the WCS, ACS, and Syslog components of the TOE.

FAU_SAR.1(2) Audit Review - Host OS

FAU_SAR.1.1(2) The TOE IT environment shall provide only the ~~**administrator**~~ **OS Admin** with the capability to read all audit data from the audit records.

FAU_SAR.1.2(2) The TOE IT environment shall provide the audit records in a manner suitable for the ~~**administrator**~~ **OS Admin** to interpret the information.

Application Note This IT Environment requirement applies to the IT Environment of the WCS, ACS, and Syslog components of the TOE.

FAU_SAR.2(2) Restricted Audit Review - Host OS

FAU_SAR.2.1(2) The TOE IT environment shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

Application Note This IT Environment requirement iteration applies to the IT Environment of the WCS, ACS, and Syslog components of the TOE.

FAU_SAR.2(3) Restricted Audit Review - Syslog

FAU_SAR.2.1(3) The TOE IT environment shall prohibit all users read access to the **TOE syslog** audit records, except those users that have been granted explicit read-access.

Application Note This requirement is split between the TOE and the IT Environment. This IT Environment requirement iteration applies to the IT Environment of the Syslog component of the TOE.

FAU_SAR.3(2) Selectable Audit Review - Host OS

FAU_SAR.3.1(2) The TOE IT environment shall provide the ability to perform *searches, sorting, ordering* of audit data based on event type, date, time, [none].

Application Note This IT Environment requirement applies to the IT Environment of the WCS, ACS, and Syslog components of the TOE.

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 stored audit records in the audit trail.

Application Note This IT Environment requirement applies to the IT Environment of the WCS, ACS, and Syslog components of the TOE.

FAU_STG.3 Action in Case of Possible Audit Data Loss

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

Application Note This IT Environment requirement applies to the IT Environment of the WCS, ACS, and Syslog components of the TOE.

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 pack objects.

Application Note This IT Environment requirement applies to the IT Environment of the WCS and ACS components of the TOE.

FIA_AFL.1(2) Remote User Authentication Failure Handling

FIA_AFL.1.1(2) The TOE IT Environment shall detect when an ~~**administrator**~~ **OS Admin** configurable positive integer within [1 to 3] 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 TSF shall prevent the remote user from authenticating until action is taken by an ~~**administrator**~~ **OS Admin**.

Application Note This IT Environment requirement applies to the IT Environment of the ACS and Syslog components of the TOE.

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: [authentication credentials].

Application Note This IT Environment requirement applies to the IT Environment of the ACS and Syslog components of the TOE.

FIA_UAU_EXP.5(2) Remote Authentication Mechanisms [Explicit Stated SFR for the IT Environment]

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

FIA_UAU_EXP.5.2(2) The TOE IT Environment shall authenticate any user’s claimed identity according to the [ACS will use user authentication credentials when it has externally configured databases that are to supply the authentication credentials].

Application Note This IT Environment requirement applies to the IT Environment of the ACS and Syslog components of the TOE.

FIA_UAU.2 User Authentication Before any Action

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

FIA_UID.2(2) Timing of Identification

FIA_UID.2.1(2) The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

Application Note This IT Environment requirement applies to the IT Environment of the ACS and Syslog components of the TOE.

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 the functions:

- Audit,
- Remote Authentication
- Time service

to the ~~**administrator**~~ **OS Admin**.

Application Note This IT Environment requirement applies to the IT Environment of the WCS and ACS components of the TOE.

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**~~ **OS Admin** or authorized IT entity.

FMT_SMR.1(2) Security Roles

FMT_SMR.1.1(2) The TOE IT environment shall maintain the roles ~~**administrator**~~ **OS Admin**.

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

Application Note This IT Environment requirement applies to the IT Environment of the WCS, ACS, and Syslog components of the TOE.

FTP_ITC_EXP.1(2) Inter-TSF Trusted Channel [Explicit Stated SFR for the IT Environment]

FTP_ITC_EXP.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_EXP.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_EXP.1.3(2) The TOE IT environment shall initiate communication via the trusted channel for all authentication functions, remote logging, time, *none*.

Application Note This IT Environment requirement applies to the IT Environment of the WCS and ACS components of the TOE.

FPT_RVM.1(2) Non-Bypassability of the IT Environment Security Policy (TSP)

FPT_RVM.1.1 The TOE IT Environment shall ensure that IT environment enforcement functions are invoked and succeed before each function within the IT environmental scope of control is allowed to proceed.

Application Note This IT Environment requirement applies to the IT Environment of the WCS and ACS components of the TOE.

FPT_SEP.1(2) TSF Domain Separation

FPT_SEP.1.1(2) The TOE IT Environment shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2(2) The TOE IT Environment shall enforce separation between the security domains of subjects in the IT environmental scope of control.

Application Note This IT Environment requirement applies to the IT Environment of the WCS, ACS, and Syslog components of the TOE.

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.

Application Note This IT Environment requirement applies to the IT Environment of the Controller, Location Appliance, WCS, ACS, and Syslog components of the TOE.

TOE Security Assurance Requirements

The TOE security assurance requirements summarized in Table 17: TOE Assurance Requirements identify the management and evaluative activities required to address the threats and policies identified in the "Security Environment" section on page 30 of this ST. This ST complies with assurance level EAL2 augmented with ACM_SCP.1 (CM Coverage), ALC_FLR.2 (Flaw Remediation), and AVA_MSU.1 (Misuse – Examination of guidance).

Table 17 TOE Assurance Requirements

Assurance Class	Assurance Components
Configuration Management	Configuration items (ACM_CAP.2) TOE CM Coverage (ACM_SCP.1)
Delivery and Operations	Delivery procedures (ADO_DEL. 1) Installation, generation, and start-up procedures (ADO_IGS.1)
Development	Informal functional specification (ADV_FSP.1) Security enforcing high-level design (ADV_HLD.1) Informal correspondence demonstration (ADV_RCR. 1)
Guidance Documents	Administrator guidance (AGD_ADM. 1) User guidance (AGD_USR. 1)
Life-Cycle Support	Flaw Reporting Procedures (ALC_FLR.2)

Table 17 TOE Assurance Requirements (continued)

Assurance Class	Assurance Components
Tests	Analysis of coverage (ATE_COV. 1) Functional testing (ATE_FUN. 1) Independent testing - sample (ATE_IND.2)
Vulnerability Assessment	Examination of guidance (AVA_MSU. 1) Strength of TOE security function evaluation (AVA_SOF. 1) Developer vulnerability analysis (AVA_VLA. 1)

SFRs With SOF Declarations

The claimed minimum strength of function for the TOE is SOF-basic.

The only probabilistic or permutational mechanism in the TOE is the password mechanism used to authenticate the users. The SFR that specifies this mechanism is FIA_UAU.1, and FIA_UAU_EXP.5(1).

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.

TOE Security Functions

Administration Security Function

Functional Requirements: 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

Administration of the TOE is implemented in multiple components of the TOE. The components of the TOE that implement the administration capabilities of the TOE are the ACS and the WCS. The Controller administrator (applicable to both 4400 and WiSM), Supervisor administrator, Location Appliance administrator, and Access Point administrator accounts are only used during IGS. Once the TOE is in its evaluated configuration, the only administrator roles in use are the ACS Administrator and the WCS Administrator. Although the Access Point administrator and Location Appliance Administrator will be able to log in locally to the AP and Location Appliance, 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 IGS or in the TOEs evaluated configuration and is covered with a tamper evident label.

WCS handles administration of the Controllers, the APs of the TOE and the 2710 Location Appliance. The WCS is the graphical user interface (GUI) to the administration capabilities of the Controllers, APs, and 2710 Location Appliances. Administration of the APs is done through the Controllers that the AP is associated through and is done by using LWAPP. The Controllers administer the APs that have been associated with the Controller during installation of the APs. The Controller carries out this administration by using LWAPP. 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 is suppose to enforce. The encryption policies can be set on a per WLAN SSID basis. The WCS administrator sets the Controller to use WPA2 then selects between Preshared Key (PSK) and 802.1X requests, which get sent to the ACS for authentication. A WCS Administrator, through the Controller, can issue LWAPP commands to instruct the APs to delete keys (by over writing with zeroes) and can also set when the APs should destroy keys (by overwriting with zeroes) after so much idle time. In order to manually initiate the deletion of keys the WCS administrator issues the following command through the Controller “config switchconfig key-zeroize” and reloads the Controller. Note that once the zeroization operation is performed for hardware certificates the TOE components will be non-communicative.

A WCS administrator may access this administration capability by using the WCS interface to the Controllers. WCS allows for an administrator to define templates that contain the policies that are then received by the Controllers and pushed out to the APs and enforce for all wireless clients trying to access the wired network being controlled by the TOE. These policies include the idle session timeout settings, which result in the access point disconnecting sessions that have remained idle longer than the administrator-specified period of time. WCS performs parameter validation during an administrator’s use of the WCS to ensure that incorrect values are not accepted that would result in the security functionality being disabled. Further, when a WCS administrator applies new settings (updates to policies on the Controllers) when the Controller receives the new settings the Controller also performs parameter validation of what it receives from the WCS.

ACS implements certain administration capabilities of the TOE. Specifically the ACS allows for the administration of wireless user authentication credentials and authorizations rights. ACS also allows for authentication and authorization of WCS administrators. The administration capabilities provided by the ACS are 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, and have error checking to ensure that incorrect values are not set that would result in the functionality being disabled. The ACS contains a RADIUS server and the APs, Controllers and WCS may be configured to use the RADIUS server in ACS to carry out the authentication and authorization capabilities of the TOE.

There are two administrator roles maintained by the TOE in the evaluated configuration: the WCS Administrator and the ACS Administrator. The ACS Administrator is responsible for management of WCS and ACS administrators and wireless users through the ACS. The WCS Administrator is responsible for management and configuration of the Controller, Location Appliance and AP TOE components through the WCS.

In addition to the roles defined for the evaluated configuration, there are additional administrator roles required for Installation, Generation and Start-up (IGS) of the TOE. These roles are only used during IGS and are not included in the evaluated configuration. The interfaces used by these administrative roles are necessary for IGS but are not included in the evaluated configuration of the TOE.

The table below lists each account that composes the administrator role, its status in the evaluated configuration and its responsibilities. Details about the specific IGS activities can be found in the IGS documentation. There is also a non-administrator account, the wireless user. See the “Remote Identification and Authentication (Wireless User)” section on page 65 for a description of how this user is authenticated.

Table 18 Administrator Accounts

Role	Status	Responsibilities
WCS Administrator	Used in IGS and Evaluated Configuration	Configuration and Management of Controller, Location Appliance and AP TOE components
ACS Administrator	Used in IGS and Evaluated Configuration	Management of Administrative users for ACS and WCS and management of wireless clients
Controller Administrator	IGS Only	Perform IGS activities for 4400 and 6500 WiSM Controller TOE Components including initial configuration, disabling network services, SNMPv3 configuration and FIPS configuration
Supervisor Administrator	IGS Only	Installation and initial configuration of Supervisor 720, FIPS configuration of WiSM
Location Appliance Administrator	IGS Only	Installation and initial configuration on of 2710 Location Appliance
Access Point Administrator	IGS Only	Installation and initial of AP TOE Components, FIPS configuration
Syslog Administrator	Used in IGS and Evaluated Configuration	Management of the selectable audit capability

The TOE provides for administrator monitoring support that enables an administrator to view audit records generated. The viewing of audit records includes viewing of audit records that were generated based on a wireless intrusion detection system (WIDS) signature or rogue device alarms being triggered through WCS. The TOE also provides real time location tracking monitoring for all authorized and unauthorized wireless hosts operating within the TOE’s RF environment.

The viewing of audit records also includes the ability to view TACACS+ accounting logs on the ACS related to administrative actions taken on the TOE via the WCS.

Audit Security Function

Functional Requirements: FAU_GEN.1(1), FAU_GEN.2, FAU_GEN_EXP.1, FAU_SAR.1(1), FAU_SAR.2(1). FAU_SAR.3(1), FAU_SEL.1, FPT_STM_EXP.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 APs, Controllers, and the ACS TOE for all of the events that are listed in Table 14 of this document as they occur on the respective components. During installation the administrator must configure the Controller to communicate with ACS for audit purposes, and the controller must be configured to receive the SNMP traps. ACS must also be configured to send logs to the syslog server. This configuration results in the start (or stop, if reversed) of the audit function and it is limited to administrators.

ACS generates those auditing records that deal with the management of user accounts controlled by the ACS, the encryption policies controlled by the ACS for wireless users, and the changing of auditing capabilities controlled by the ACS. The ACS auditing capability is implemented in three different logging capabilities of ACS. These logging capabilities are the CSV Failed Attempts, CSV Passed Authentication, and CSV RADIUS Accounting. Within each of these logging capabilities a user is able to selectively choose what they want audited based on the type of event.

In addition to the ACS audit capability outlined in the preceding paragraph, the ACS also provides the TOE functionality that allows for administrator actions through the WCS to be logged and viewed. (Note that the WCS is administratively configured to be the SNMPv3 client for the Controller, allowing for administration of the Controller via WCS). This is accomplished using Controller TACACS+ accounting. For this, the ACS acts as a AAA server and the Controller as the AAA client. Once a WCS administrator is authenticated and authorized into WCS by the ACS using RADIUS, all actions performed by that administrator on the Controller via WCS are forwarded back to ACS in the form of Controller TACACS+ accounting logs. These logs are then viewable through the ACS interface in the TACACS+ Administration Active CSV logs. This log, in conjunction with the Passed Authentication Active CSV log, provide the audit generation capability for the audit requirements stated in the "Security Requirements" section on page 36 of the ST.

The Controller has a Wireless Intrusion Detection System (WIDS) capability that generates audit records based on wireless networking traffic matching a set of predefined signature rules. The signatures define patterns of information in wireless network traffic that the APs use to monitor the RF environment. The audit records generated by the Controller on signature matches are displayed through the WCS interface. WCS also displays audit records for rogue devices that are detected within the RF environment

Along with the WIDS audit record generation capabilities of the Controller the Controller will generate SNMPv3 trap messages. The SNMPv3 trap messages are security relevant auditable events. When one of the SNMPv3 defined trap events occur it is logged to a log file with the security attributes necessary to determine the time it happened, the event that happened, and the devices involved in the event.

The Controller also generates audit records for detection of spoofed or exploited 802.11 management frames in support of Management Frame Protection (MFP).

WCS and the Location Appliance work together to generate audit records dealing with location of devices that emit RF energy. These records include the presence and location tracking of thousands of wireless nodes including rogue clients, ad-hoc rogues, rogue APs and authorized wireless devices. WCS and the Location Appliance work in conjunction with the Controllers to get the information needed to do the calculations which determine the location of wireless devices. The Controllers collect RSSI information from the APs, which is RF specific information that measures and describes the energy and noise levels associated with the 802.11 wireless devices (either wireless clients, RFID tags or APs) communicating within the RF environment. WCS collects the RSSI information from the Controller periodically and runs location algorithms on the data and forwards that info to the Location Appliance. The Location Appliance also receives updated RSSI information directly from the Controllers in addition to WCS which provides the Location Appliance with additional location tracking information. WCS and the Location Appliance may generate their location audit records based on the RSSI information generated from 1 AP, but if the RSSI information generated by 3 or more APs is available then the location accuracy is of a higher resolution. The location information is based on the configuration location of the APs and the specification of the AP TOE components physical locations and surrounding physical environment during configuration of the TOE. The Location Appliance stores all location audit records generated along with time stamping the audit records with the Location Appliance time of the time the location records was generated. The Location Appliance by default setting stores 30 days worth of historical location data, but it can be configured to store an unlimited amount of historical data based on available data storage.

The Location Appliance also provides location-based alerts. This feature provides the ability to proactively send location notifications based on wireless device movement in and out of predefined physical zones, device absence from physical zones, Wi-Fi tag battery level and Wi-Fi device position change. The Wi-Fi tag battery level notification indicates the Wi-Fi tag's power level. The Wi-Fi device position change notification sends an alert when the position of a device changes. All of these notifications can be delivered over multiple transport types: Simple Network Management Protocol (SNMP) traps, email, and Simple Object Access Protocol (SOAP) XML API. SOAP, is the simple XML protocol, as the transport type for sending event notifications. SOAP is used to send notifications over HTTPS.

Audit events generated by the TOE contain the following fields: a timestamp, an associated user identity (“user-name” in the example events at the end of the section), event type (“Message-type” in the example events at the end of the section), 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 an ntp server in the environment for synchronization. These events are available to be viewed on the ACS by the ACS administrator, and on the Syslog server by the Syslog administrator. These interfaces also provide for searching and sorting/ordering of audit events based on their event type and their timestamp (including date and time).

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, the wireless user "passed authentications" wireless user "failed attempts" and ACS admin "Administrative Audit" logs will be generated by ACS but not stored locally in ACS persistent storage. Instead these event records are forwarded by ACS 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 audit log files may be written into ACS 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 to the following wireless user audit log fields generated by ACS.

Table 19 Syslog Audit Log Mapping

FAU_SEL.1.1 Term	ACS Log Event Field
“user identity”	“User Name”
“event type”	“Priority” set to “Auth”
“device interface”	Implied WLAN interface [The ACS audit logs for wireless users “Passed Authentications” and “Failed Attempts” only apply to TOE audit events generated by a wireless users WLAN interface]
“wireless client identity”	“Caller-ID”. [The ACS “Caller-ID” field corresponds to the wireless client machine MAC ID address]

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.

Example of ACS “Passed Authentication” and “Failed Attempts” audit log fields:

```
07-11-2008 10:37:36 Auth.Info 192.168.30.12 Jul 11 17:36:37 192.168.30.12
CisACS_01_PassedAuth afly6g3 1 0 Message-Type=Authen OK, User-Name=army,
NAS-IP-Address=192.168.30.5, Caller-ID=00-12-17-62-FD-02,NAS-Port=1,Group-Name=DOD,Filter
Information=No Filters activated.,EAP Type=25,Access Device=Controller-RAD,EAP Type
Name=MS-EAP-TLS,

07-11-2008 10:36:20 Auth.Info 192.168.30.12 Jul 11 17:35:22 192.168.30.12
CisACS_02_FailedAuth 1onj1vs2 1 0 Message-Type=Authen failed, User-Name=fake-user,
NAS-IP-Address=192.168.30.5, Authen-Failure-Code=ACS user
unknown,Caller-ID=00-17-F2-EF-19-BC, NAS-Port=1, Group-Name=DOD,EAP Type=25,
```

Encryption Security Function

Functional Requirements: FCS_BCM_EXP.1, FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM.1(3), FCS_CKM_EXP.2, FCS_CKM.4, FCS_COP.1(1), FCS_COP.1(2), FCS_COP_EXP.1, FCS_COP_EXP.2

End-to-end wireless encryption is implemented in the TOE through the use of EAP-TLS, EAP-FAST or WPA2-PSK. To carry out encryption the AP, Controller, and ACS components of the TOE 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 LWAPP 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. LWAPP protects all control and bridging traffic between trusted network access points and the module with AES-CCM encryption.

For encryption implemented with EAP-TLS and EAP-FAST the APs, Controllers, and ACSs 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 (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.

When the ACS 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-CCM encryption.

Keys are input into the APs from the Controller/WiSM over a LWAPP session. During an LWAPP session, the APs first authenticate to the Controller/WiSM using an RSA key pair. After a successful authentication, the LWAPP session key generated in the Controller/WiSM is transported to the AP wrapped with AP’s RSA key.

The crypto modules of the TOE are the APs and Controllers. So for this evaluation the crypto modules are the Cisco Aironet APs 1131 1232, and 1242; Cisco controllers 4402 and 4404; and the Catalyst 6500 WiSM. These crypto modules are FIPS PUB 140-2 validated Level 2 and it is the APs and Controllers that perform cryptographic functions in FIPS approved modes of operation.

The APs perform FIPS 140-2 validated end-to-end wireless encryption and decryption required between a wireless device and the AP. APs act as the TOE’s trusted end point for wireless user access into the wired network.

During the association of a wireless client with an AP both the AP and Controller maintain keys that are used during the wireless client session with the TOE. If the wireless client session with an AP is terminated then the keys associated with that wireless client on the AP and Controller are destroyed. A reboot of the AP and Controller will destroy all keys resident on the APs and Controllers.

The Controller can issue LWAPP commands that can command the APs to delete keys and can also set when the APs should destroy keys after so much idle time. All keys on the TOE are overwritten with zeroes when they are deleted.

Key destruction (zeroization) is a one time operation for hardware, factory burned, certificates. It is performed through the Controller CLI, per the Controller FIPS 140-2 Security Policy, 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.

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.

SNMPv3 is used for authentication between the Location Appliance and the Controller and the WCS and the Controller. This authentication is secured using a SHA-1 hash that is 20 octets in length and DES encryption using a 56-bit key.

Identification and Authentication Security Function

Functional Requirements: FIA_AFL.1(1), FIA_ATD.1(1), FIA_ATD.1(2), FIA_UAU. 1, FIA_UAU_EXP.5(1), FIA_UID.2(1), FIA_USB.1(1), FIA_USB.1(2), FTA_TAB.1, FTP_ITC_EXP.1(1), FTP_TRP.1

The TOE provides local and remote identification and authentication. This security function will describe the different identification and authentication capabilities of the TOE and identify which TOE components are involved with the different identification and authentication capabilities.

Authentication performed by the TOE makes use of a password mechanism to authenticate the users. This is a permutational mechanism that meets the minimum strength of function rating of SOF-basic. The SFRs that specify this mechanism are FIA_UAU. 1, and FIA_UAU_EXP.5(1).

The following table identifies TOE authentication connectivity, authentication mechanism and user databases available.

Table 20 WLAN Authentication Mechanisms

WLAN Authentication Mechanisms				
Authenticated Connectivity	**Local Authentication**	**Remote Authentication**	**Authentication Mechanism**	**Available User Database(s)**
Browser (admin) to WCS	n/a	RADIUS to ACS	Password w/HTTPS auth	ACS
WCS to LocApp	Required	n/a	Password w/HTTPS auth	Location Appl.
Controller to ACS	AES key wrap	n/a	Privacy Password (AES key) and Authentication Password (HMAC-SHA1 key) (passwords are on both systems)	N/A 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

Table 20 WLAN Authentication Mechanisms (continued)

WLAN Authentication Mechanisms				
Authenticated Connectivity	**Local Authentication**	**Remote Authentication**	**Authentication Mechanism**	**Available User Database(s)**
Controller to AP	LWAPP	n/a	X509.1 Certificate	N/A x.509 auth takes place if both AP and Controller possess the same certs as shipped from the factory
LocApp to Controller	snmpv3 (sha1/des)	n/a	Password	WLC
WCS to Controller	snmpv3 (sha1/des)	n/a	Password	WLC
Console to Supervisor 720	Available but is not used in the evaluated configuration. Limited local data access with no access to other TOE components	RADIUS to ACS	Password	ACS
Browser (admin) to ACS	Required	n/a	HTTPS w/ Password	ACS
Wireless Client (user) to AP	WPA2 w/pres-shared key auth	RADIUS to ACS	WPA2 w/802.1X EAP authentication packets	ACS
Console to AP	Available (Security sealed per FIPS Cert.) Limited local data read access with no write access permitted or access to other TOE components.	n/a	Password	AP

Table 20 WLAN Authentication Mechanisms (continued)

WLAN Authentication Mechanisms				
Authenticated Connectivity	**Local Authentication**	**Remote Authentication**	**Authentication Mechanism**	**Available User Database(s)**
Console to Controller	Available (Security sealed per FIPS Cert.) Limited local data access with no access to other TOE components.	n/a	Password	WLC
Console to Location Appliance	Available. Limited local data read access with no write access permitted or access to other TOE components.	n/a	Password	Location Appl.

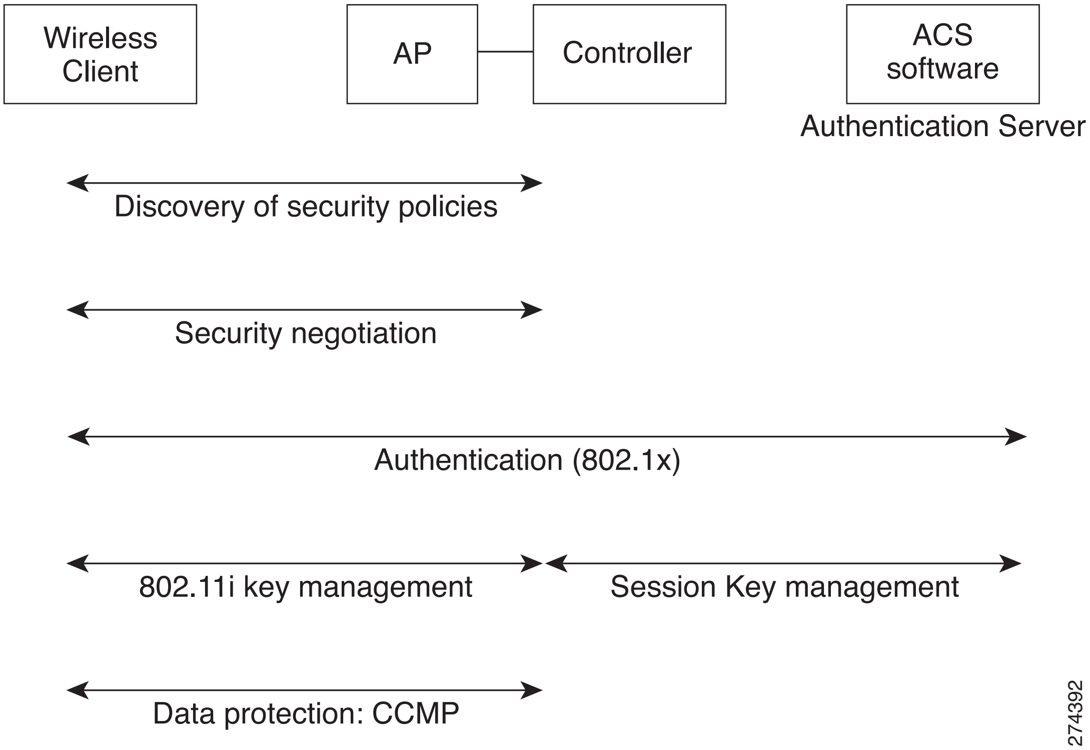
Remote Identification and Authentication (Wireless User)

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. 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 and the Controller. See Figure 2 for this process flow.

Figure 2 802.11i 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 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 in the IT Environment. 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 TOE component.

When EAP-TLS or EAP-FAST are 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. The PSK is a pass phrase that is set by the WCS

Administrator of the TOE through the WCS interface. Wireless clients trying to connect to the wired network controlled by the TOE needs to know the pass phrase for their wireless client software to successfully identify and authenticate to the TOE.

With EAP-FAST 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 able to allow for wireless administration however this feature is disabled in the evaluated configuration so the TOE does not allow administration from wireless clients.

The security attributes that are maintained by the AP, Controller, and ACS are the certificates when using EAP-TLS, the Private Access Credentials (PAC) when using EAP-FAST and the 802.11i session encryption keys that are used to encrypt wireless traffic during a supplicants session with the authenticator.

Remote administration is provided by the WCS for remote administration of the Controller. The WCS is the SNMPv3 client for the Controller. The WCS administrator must be successfully authenticated through ACS in order to be able to perform administration of the Controller TOE component. Additionally, the WCS provides remote administration functionality via for APs and Location Appliances associated with it.

Remote administration is also available for ACS. Using HTTPS and the ACS IP address, an ACS administrator can access ACS remotely by providing a valid username and password through the ACS login GUI.

Local Identification and Authentication

The WCS and ACS have local identification and authentication (I&A) capabilities. On the ACS, the administrator can start ACS and access the functionality of ACS after logging into the ACS host through the ACS IT Environment, then providing a valid username and password through the ACS login GUI.

For access to the WCS, administrators must login to the WCS GUI. For this local I&A, an administrator provides a username and password through the HTTPS client on the WCS machine. This authentication request is then forwarded to the ACS, which then authenticates and authorizes the administrator’s access into WCS using RADIUS. Through WCS the WCS administrator configures the login banner that will be displayed to all users attempting access to the TOE.

The WCS uses SOAP/XML to exchange of information with the Location Appliance and is authenticated by password with HTTPS authentication.

For the evaluation HTTPS is the configured option for web interface communication. HTTP is disabled and is not used for the evaluated configuration.

The Controller authenticates with the ACS using a Privacy Password (AES key) and an Authentication Password (HMAC-SHA1). Passwords are on both TOE components.

The AP Console port although available is Security sealed per the AP FIPS Security Policy. The console uses password authentication and has limited local data read access with no write access permitted or access to other TOE components. It is considered not security relevant.

The Location Appliance Console port although available is only relevant at the time of set up. The console uses password authentication and has limited local data read access with no write access permitted or access to other TOE components. It is considered not security relevant.

The Controller Console port although available is only relevant at the time of set up. It is physically secured and not used during normal operation of the. The console uses complex password authentication required by the Controller FIPS 140 Security Policy and has limited local data access with no access to other TOE components. It is considered not security relevant.

The syslog components rely on authentication in the IT environment prior to any actions by the administrators.

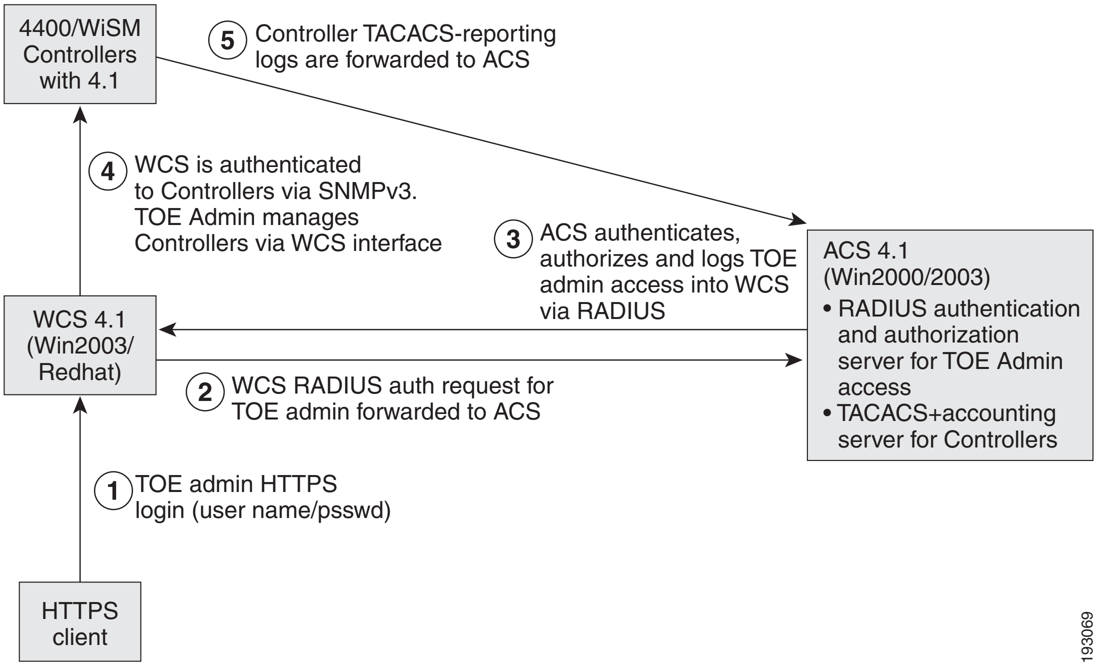
Remote Administrator Identification and Authentication

All WCS administrators can be configured and managed through the ACS. ACS uses RADIUS for authentication and authorization of administrators attempting to manage the TOE through the WCS management interface. ACS then uses Controller TACACS+ accounting to track and log all actions taken through WCS by those authenticated administrators. ACS enforces the login failure handling for these remotely authenticated administrators. Once the consecutive number of failed authentications per the setting within ACS (between 1 and 3, inclusively) is reached, that administrator account is locked until the ACS administrator takes an action to unlock it.

The ACS administrator can also utilize HTTPS to access ACS remotely using the ACS IP address, and must provide a username and password through the ACS GUI in order to gain access to ACS functionality.

The ACS TOE component provides the AAA server functionality of the TOE for authentication and authorization of WCS administrators using RADIUS. The WCS is the AAA RADIUS client for WCS administrators. The Controller is the AAA Client for TACACS+ accounting. Administrators attempting to log into WCS are authenticated and authorized by the ACS. Once authenticated, actions taken by the administrator on the WCS are logged by ACS using the Controller TACACS+ Accounting functionality. WCS is administratively configured to be the SNMPv3 client for the Controller. This creates a validated interface allowing the Controller to be managed by a particular WCS. The diagram below shows the flow of WCS administrator authentication using RADIUS and the TOE auditing using Controller TACACS+ accounting. TACACS+ accounting logs are then viewable through the ACS.

Figure 3 Common Criteria WLAN System RADIUS & TACACS+ FLOW


4400/WiSM Controllers with 4.1
5 Controller TACACS-reporting logs are forwarded to ACS
4 WCS is authenticated to Controllers via SNMPv3. TOE Admin manages Controllers via WCS interface
3 ACS authenticates, authorizes and logs TOE admin access into WCS via RADIUS
ACS 4.1 (Win2000/2003)
• RADIUS authentication and authorization server for TOE Admin access
• TACACS+accounting server for Controllers
WCS 4.1 (Win2003/ Redhat)
2 WCS RADIUS auth request for TOE admin forwarded to ACS
1 TOE admin HTTPS login (user name/psswd)
HTTPS client
193069

Information Flow Control Security Function

Functional Requirement: FDP_PUD_EXP.1

FDP_PUD_EXP.1 gives the administrator control over whether or not unencrypted data will be allowed to pass through the TOE by giving him or her ability to enable and disable the encryption policy of the TOE. This encryption policy decides 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

Self Protection Security Function

Functional Requirements: FDP_RIP.1(1), FPT_RVM.1(1), FPT_ITT.1, FPT_SEP.1(1), FPT_TST_EXP.1, FPT_TST_EXP.2

Non-bypassability and Domain Separation

Non-bypassability and domain separation is provided by the different components of the TOE. Different components of the TOE provide for non-bypassability and domain separation in different manners. There are two different categories of TOE components for non-bypassability and domain separation. The two categories are:

- Software and hardware TOE components and
- Software only TOE components

The following sections will describe how the different categories of TOE components provide for non-bypassability and domain separation.

Hardware TOE Components Protection

AP TOE Components Protection

The APs (the Cisco Aironet 1131, 1231, and 1242 access points) provide for non-bypassability through the use of well defined interfaces for connecting wireless clients to wired and wireless network. The APs mediate all actions that occur with the interface servicing wireless clients in the RF domain, the wired network interface, and the console interface. Mediation of an interface of the AP involves the component initiating a security enforcing function when a user interacts with one of the AP interfaces.

The TOE ensures that network traffic transmitted on the wireless network is protected from disclosure by supporting end-to-end encryption on the wireless network. All of the encryption modules that are within the TOE logical boundary are for wireless communications, and they are all FIPS certified. This includes the LWAPP encrypted channel which provides the channel between the AP and the Controllers.

- The trusted end points (Access Points) shall mutually authenticated via x.509 certificates before associating to and communicating with the Controllers
- All configuration and bridging communications shall be protected by AES-CCM encryption between trusted end points (Access Points) and Controllers.

Mediation of the interface to the wireless clients involves invoking the enforcement functions to control the communication of wireless clients based on the information flow, encryption, and access policies established for the AP. This mediation allows for the AP to successfully validate any request made by the wireless clients before the request is allowed to succeed. This helps ensure that AP is enforcing the SFP to wireless clients.

Mediation of the wired interface to the AP involves making sure that it is receiving management data from the Controller that it has been associated with and that the AP is allowing flows of information to and from successfully authenticated wireless client users The mediation conducted at the wired network interface allows for the AP to successfully validate any request made for management or information flow for clients of the wired interface before the request is allowed to succeed. This helps ensure that the AP is enforcing the SFP to the wireless clients and that management requests from the Controller are occurring.

The AP mediation done for the console interface involves invoking an access control mechanism before allowing any other action to succeed. Further, successfully identifying and authenticating users allows for the AP to enforce the SFP by only allowing properly authenticated users access to the security functions that they are authorized to use.

Through the mediation that the AP does to its interfaces a boundary of control is established for all communications and interactions that may occur with the component. This boundary is non-bypassable because it requires proper and successful validation of all those communications and interactions that can occur with the interfaces that make up the boundary. By doing this the APs ensure that the TSF that it has and the SFP that it enforces is non-bypassable.

In support of non-bypassability, the APs mutually authenticate with Controllers using X.509 certificates before associating to and communicating with Controllers. Once mutually authenticated, all configuration and bridging communications between the AP and Controller are protected the by FIPS 140-2 validated AES-CCM encryption.

The security domain for the AP is composed of all the hardware and software of the AP that are part of this evaluation and that have been identified in TOE Description, page 11. The AP does not allow for the initiation or setup of un-trusted user processes on it. All running processes on the AP are trusted and are used in helping to enforce the SFP. For this reason the AP is a security domain for the TSF enforcement functions implemented in it and the domain boundaries are the physical and logical interfaces to the component. The AP protects the security domain from interference and tampering by controlling how trusted and un-trusted subjects (users) interact to and through the component. The scope of control of subjects for the AP are those wireless clients that interact with or through the component and those information flows through the wireless network interface along with those users that try to manage the AP through the console port. The AP only controls those subject activities that go through it.

The AP enforces an RF security domain and a wired security domain. Individual subjects operating within the RF domain can be further separated when encryption is used. The encryption is in the RF domain. The AP does not have any control of the subjects in the RF domain.

Controller TOE Component Protection

The Controllers (Cisco 4402, Cisco 4404, and Catalyst 6503, 6504, 6506, 6509, 6513 WiSM with Supervisor 720) supports non-bypassability through the use of specific functionality related to controlling the SFP that the APs enforce. The Controller mediates all actions that occur with the interface managing APs, the WCSs, ACSs, and together with WCS the Location Appliances. Mediation of an interface of the Controller involves the component initiating a security enforcing function when a user interacts with one of the interfaces.

Mediation of the interface to the APs involves invoking the enforcement functions to control the management communications that occurs between the APs and Controllers. LWAPP allows the Controllers and APs to successfully validate any management requests made between these two components before the request is allowed to succeed. This helps ensure that the Controller is enforcing the SFP to the APs.

Mediation of the interface to the WCSs involves invoking the enforcement functions to control the management communications that occurs between the WCSs and Controllers. SNMPv3 allows the Controller and WCS TOE components to successfully validate any management requests made between these two components before the request is allowed to succeed. This helps ensure that only authorized users and an authorized WCS can manage Controllers and the APs associated with the Controller according to the management SFP.

Mediation of the interface to the Location Appliances involves invoking the enforcement functions to control the management communications that occur between the Location Appliances and Controllers for the collection of location data from the Controller to the Location Appliance. The mediation is accomplished using SNMPv3 which allows for the Controllers and Location Appliances to successfully validate requests to transfer the location data the Controller has to the Location Appliances before the request is allowed to succeed. This helps ensure that the SFP dealing with location is being enforced by those Location Appliances that are authorized to do so because of their association with the Controller through the use of SNMPv3.

Mediation of the interface to the ACSs for the purpose of wireless client authentication involves invoking the enforcement functions to control the communications of authentication and accounting information that occurs between the ACSs and Controllers. The mediation is done by using AES RADIUS key wrap to protect the transmission of Pairwise Master Keys between the Controllers and the ACSs. The ACSs and the Controllers successfully validate requests to transfer the authentication and accounting information between them using the RADIUS protocol before the request is allowed to succeed. This helps ensure that the SFP dealing with auditing, identification, and authentication is being enforced by the Controllers and ACSs.

Mediation of the interface to the ACS for the purpose of AAA services for the management of Controllers via WCS is provided by RADIUS and Controller TACACS+. The ACS is configured to be the AAA RADIUS Server and AAA TACACS+ server for the authentication, authorization and accounting of WCS administrators. Users are added through ACS and given authorizations for management of WCS through ACS. The ACS enforces the authorizations for WCS administrators using WCS and provides auditing of all administrator actions in the WCS using Controller TACACS+ accounting. This ensures that only authorized users are able to carry out administrative actions within the TSF and enforces the management, auditing and identification and authentication SFPs.

Through the Controller's mediation of its interfaces, a boundary of control is established for all communications and interactions that may occur with the component. This boundary is non-bypassable because it requires, based on the interface, proper and successful validation of all those communications and interactions that can occur with the interfaces that make up the boundary. By doing this the Controller ensures that the TSF that it has and the SFP that it enforces is non-bypassable.

The security domain for the Controllers is composed of all the hardware and software of the Controllers that have been identified in the "TOE Description" section on page 11. The Controller does not allow for the initiation or setup of un-trusted user processes on it. All running processes on the Controller are trusted and are used in helping to enforce the SFP. For this reason the Controller is a security domain for the TSF enforcement functions implemented in it and the domain boundaries are the physical and logical interfaces to the component. The Controller protects the security domain from interference and tampering by only allowing trusted subjects (users) to interact with the component. The scope of control of subjects for the Controller are the APs associated with it, the WCS associated with the Controller, the Location Appliances associated with the Controller, and the ACSs associated with the Controller. By having a physical boundary and controlling the boundary interfaces and only allowing trusted subjects to interact with it the Controller maintain a separate security domain for its own execution that protects it from interference and tampering.

The TOE has 17 standard Wireless Intrusion Detection Signatures (WIDS) which it uses to detect unauthorized or threatening WLAN activity (see the list of standard signatures in parts a and b of FAU_GEN_EXP.1.1).

Location Appliance TOE Component Protection

The Location Appliance (Cisco 2710 Location Appliance) supports non-bypassability through the use of functions for calculating wireless devices based on RF measurements collected by the Controllers. The Location Appliance mediates all actions that occur with the network interface that it uses to collect RF measurement information from the Controllers. The results of the location calculations are published to the WCSs and it mediates all interactions with the CLI interface of the Location Appliance. Mediation of an interface of the Location Appliance involves the component initiating a security enforcing function when a user interacts with one of these interfaces.

Mediation of the interface to the Controllers and WCSs involves invoking the enforcement functions to control the management communications that occurs to collect RF measurement data from a controller and to publish location calculations to the WCSs. The mediation is done by using SNMPv3 which allows for the Controllers, WCS, and the Location Appliances to successfully validate any management requests made between these three components before the request is allowed to succeed. This helps ensure that the SFP dealing with management and determining location of wireless devices is being enforced.

Through the Location Appliance's mediation of its interfaces, a boundary of control is established for all communications and interactions that may occur with the component. This boundary is non-bypassable because it requires proper and successful validation of all those communications and interactions that can occur with the interfaces that make up the boundary. By doing this the Location Appliance ensures that the TSF and the SFP that it is helping to enforce is non-bypassable.

The security domain for the Location Appliance is composed of all the hardware and software of the Location Appliance is part of this evaluation and that has been identified in the "TOE Description" section on page 11. The Location Appliance does not allow for the initiation or setup of un-trusted user processes on it. It has a single purpose of collecting RF measurement data, calculating location based on the data, and sending the resulting calculated location out. All running processes on the Location Appliance are trusted and are used in helping to enforce the SFP. For this reason the Location Appliance is a security domain for the security function of calculating and generating an audit record for location of wireless devices and the domain boundary is the physical and logical interfaces to the component. The Location Appliance protects the security domain from interference and tampering by only allowing trusted subjects (users) to interact with the component. The scope of control of subjects for the Location Appliance are the Controllers and WCSs associated with it. By having a physical boundary and controlling the boundary interfaces and only allowing trusted subjects to interact with it the Location Appliance maintains a separate security domain for its own execution that protects it from interference and tampering.

Software TOE Components Protection

The ACS and WCS are software components that execute in an IT Environment that supplies its own non-bypassability and domain separation. For a discussion of non-bypassability and domain separation for the IT Environment, see the "Security Architecture" section on page 27.

ACS TOE Component Protection

The ACS supports non-bypassability through the use of well defined interfaces that are restricted in carrying out a very domain specific set of functions dealing with authentication and accounting (auditing) that are under the control of this component. The ACS mediates all actions that occur with the network interface that it uses to communicate with Controllers and that it uses to interact with human users. Mediation of an interface of the ACS involves the component initiating a security enforcing function when a user interacts with one of these interfaces to support the enforcement of a policy that involves how human users and Controllers can operate on the authentication and auditing data controlled by the ACS.

Mediation of the network interface the ACS has with the WCS involves invoking the enforcement functions to control the AAA communications between these two components. The mediation is done by using the RADIUS protocol between the ACS and the WCS for authentication and authorization and Controller TACACS+ for accounting. This allows the ACS and the WCS to successfully validate any AAA communications made between these two components before the request is allowed to succeed. This helps ensure that the authentication, authorization and accounting (auditing) SFP is being carried out.

The ACS mediates and enforces a control policy over all communications that are under its control dealing with its network interface to the Controller. AES RADIUS key wrap is used between ACS and the Controller to protect the distribution of the 802.11i PMK.

Mediation of the graphical user interface (GUI) the ACS has with human users is done by requiring human users to identify and authenticate themselves to the ACS and only allowing those that have successfully authenticated to the ACS to carry out management activities and how the TOE carries out auditing and authentication.

Through the mediation that the ACS does to its interfaces within its control and the non-bypassability features and support that the ACS's IT Environment supplies a boundary of control is established for all communications and interactions that may occur with the component. This boundary is non-bypassable because it requires proper and successful validation of all those communications and interactions that can occur with the interfaces that make up the boundary. By doing this the ACS ensures that the TSF that it has and the SFP that it is helping to enforce is non-bypassable.

The ACS maintains a security domain that protects the authentication and accounting functions that it carries out. The security domain for the ACS is achieved by the ACS providing strictly controlled interface that are used to carry out the well defined set of security functions of activities dealing with authentication and accounting. By the ACS controlling and mediating its interfaces the ACS has a well defined software boundary defined which for a security domain that protects the authentication and accounting functions of the ACS from interference and tampering.

The ACS is a software only TOE component that relies on a hosting IT Environment that supplies and supports the executing of the component and protection and security domain separation of the resource operating on the host IT Environment.

The ACS implements domain separation for based on the description of the ACS domain separation above along with the description of the domain separation description given for the hosting IT Environment of the ACS. Based on the domain separation capabilities supplied by both the ACS and the IT Environment for the ACS a separate security domain is provided for the ACS that protect it from tampering and interference by untrusted users or other processes running on the host IT Environment.

WCS TOE Component

The WCS supports non-bypassability through the use of well defined interfaces that are restricted in carrying out a very domain specific set of functions dealing with communicating management commands to the Controller and Location Appliance. The WCS mediates all actions that occur with the network interface that it uses to communicate with both the Controllers and Location Appliances and the GUI it uses to interact with human users. Mediation of an interface of the WCS involves the component initiating a security enforcing function when a user interacts with one of these interfaces to support the enforcement of a policy that involves how human users along with Controller and Location Appliances can operate with the WCS.

Mediation of the network interface the WCS has with the Controller and Location Appliances involves invoking the enforcement functions that control the management communication that occur between these components of the TOE. The mediation is done by using SNMPv3 and passwords that have been administratively configured between the WCS, Controller and Location Appliances. This allows the ACSs and the Controllers to successfully validate management communications made between these components before the request is allowed to succeed. This helps ensure that the SFP dealing with management is being carried out. The WCS mediates and enforces a control policy over all communications that are under its control dealing with its network interface to the Controllers and Location Appliances.

Mediation of the graphical user interface (GUI) the WCS has with human users is done by requiring human users to identify and authenticate themselves to the WCS and only allowing those that have successfully authenticated to the WCS to carry out management activities.

Through the mediation that the WCS does to its interfaces within its control and the non-bypassability features and support that the WCS's IT Environment supplies a boundary of control is established for all communications and interactions that may occur with the component. This boundary is non-bypassable because it requires proper and successful validation of all those communications and interactions that can occur with the interfaces that make up the boundary. By doing this the WCS ensures that the TSF that it has and the SFP that it is helping to enforce is non-bypassable.

The WCS maintains a security domain that protects the management functions that it carries out. The security domain for the WCS is achieved by the WCS providing strictly controlled interfaces that are used to carry out the well defined set of security functions of activities dealing with management of the Controllers and Location Appliances. By the WCS controlling and mediating its interfaces the WCS has a well defined software boundary which establishes a security domain that protects the management interface functions of the WCS from interference and tampering.

The WCS implements domain separation based on the description of the WCS domain separation above along with the description of the domain separation responsibilities defined for the hosting IT environment described in this ST. Based on the domain separation capabilities supplied by both the WCS and the IT Environment for the WCS a separate security domain is provided for the WCS operating on the ST defined hosting IT environment that protects it from tampering and interference by untrusted users or other processes running on the host IT Environment.

Syslog TOE Component

The Syslog (Kiwi Syslog Daemon 8.3.30 and Syslog-ng 2.0.9) component supports non-bypassability through the restriction of the functions it performs to store and filter audit records. The Syslog software mediates all actions that occur with the network interface that it uses to communicate with the ACS Server.

The Syslog is a software only TOE component that relies on the host OS in the IT Environment for execution, protection, and security domain separation of it's resources. The host OS protects the Syslog TOE component by providing limited access to the interfaces and separation of processes in memory. The Syslog component is also protected by being located on a trusted management network that is separate from the wireless client network.

TSF Testing

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 CRC-32 (checksum) check on the configuration files upon initial start up. The results for these tests are reported at the console upon boot up.

Assurance Measures

The TOE satisfies CC EAL2 assurance requirements augmented with ACM_SCP.1, ALC_FLR.2 and AVA_MSU.1. 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 EAL2 assurance requirements. Table 21 lists the details.

Table 21 Assurance Measures

Assurance Component	How requirement will be met
ACM_CAP.2 Configuration items	*Cisco WLAN Access System Configuration Management and Flaw Remediation* Documentation version 1.3
ACM_SCP.1 TOE CM Coverage	*Cisco WLAN Access System Configuration Management and Flaw Remediation* Documentation version 1.3
ADO_DEL.1 Delivery procedures	*Cisco WLAN Access System Delivery Documentation* version 4.0
ADO_IGS.1 Installation, generation and startup procedures	*Cisco WLAN Access System Installation, Generation and Start-Up Documentation* version 17.0 *Installation Guide for Cisco Secure ACS for Windows,* 78-16991-01 *User Guide for Cisco Secure Access Control Server for Windows Release 4.1*, OL-9971-01 *Cisco 4400 Series Wireless LAN Controller Quick Start Guide*, 78-17040-01 *Cisco Wireless Control System Configuration Guide Software Release 4.1*, April 2007 *Catalyst 6500 Series Switch Wireless Services Module Installation and Configuration Note* (Supervisor Install Guide), 78-15767-01 *Catalyst 6500 Series Switch Wireless Services Module Installation and Configuration Note* (WiSM Install Guide), 78-17121-01 *Catalyst 6500 Series Switches Installation Guide,* OL-5781-04 *Catalyst 6500 Series IOS Software Configuration Guide*, Release 12.2SX, OL-3999-07*Quick Start Guide Cisco Aironet 1130AG Access Point,* 78-15595-02 *Quick Start Guide Cisco Aironet 1240AG Series Access Point*, 78-16908-01 *Quick Start Guide Cisco Aironet 1200 Series Access Points*, 78-16238-03 *Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode*, OL-8092-01 *Cisco 2700 Series Location Appliance Installation and Configuration Guide*, 78-17180-01 *Quick Start Guide: Cisco Wireless Control System for Microsoft Windows*, OL-8459-01 *FIPS 140-2 Security Policy for Cisco 4402 and 4404 Wireless LAN Controllers, Version 1.11*, October 3, 2006, OL-9658-01 *FIPS 140-2 Security Policy for Cisco Aironet LWAPP AP1131AG, Cisco Aironet LWAPP AP1231G, Cisco Aironet LWAPP AP1232AG, and Cisco Aironet LWAPP AP1242AG Wireless Access Points*, OL-9659-01
ADV_FSP.1 Informal functional specification	*Cisco WLAN Access System Functional Specification* version 13.0
ADV_HLD.1 Descriptive high-level design	*Cisco WLAN Access System High Level Design* version 13.0

Table 21 Assurance Measures (continued)

Assurance Component	How requirement will be met
ADV_RCR.1 Informal correspondence demonstration	Cisco WLAN Access System Representation Correspondence Documentation version 5.0
AGD_ADM.1 Administrator guidance	*Cisco WLAN Access System Administrator Guide* version 13.0 *Cisco Location Appliance Configuration Guide* Version 3.0 February 2007, OL-12449-01 *User Guide for Cisco Secure Access Control Server for Windows* Release 4.1, OL-9971-01 *Cisco Wireless Control System Configuration Guide Software* Release 4.1, April 2007
AGD_USR.1 User guidance	*Cisco WLAN Access System User Guide* version 10.0 *Cisco Wireless Control System Configuration Guide Software Release 4.1*, April 2007 *Cisco Wireless Control System Configuration Guide Software Release 4.1*, April 2007
ALC_FLR.2 Flaw reporting procedures	*Cisco WLAN Access System Configuration Management and Flaw Remediation* Documentation version 1.3
ATE_COV.1 Evidence of coverage	*Cisco WLAN Access System Test Coverage* Documentation version 13.0
ATE_FUN.1 Functional testing	*Cisco WLAN Access System Test Coverage* Documentation version 13.0
ATE_IND.2 Independent testing – sample	*Cisco WLAN Access System Test Coverage* Documentation version 13.0
AVA_MSU.1 Examination of guidance	*Cisco WLAN Access System Administrator Guide* version 13.0
AVA_SOF.1 Strength of TOE security function evaluation	*Cisco WLAN Access System Strength of Function* Documentation version 9.0
AVA_VLA.1 Developer vulnerability analysis	*Cisco WLAN Access System Vulnerability Analysis* Documentation version 8.0

Protection Profile Claims

Protection Profile Reference

This ST claims conformance to the US Government Wireless Local Area Network (WLAN) Access System Protection Profile for Basic Robustness Environments, April 2006, Version 1.0.

Protection Profile Refinements

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

1. The wording of O.CRYPTOGRAPHY_VALIDATED was updated from referring to "FIPS 140-1/2" to "FIPS 140-2" which is the current FIPS 140 version. This change to "FIPS 140-2" was also done in the following SFRs: FCS_BCM_EXP.1, FCS_CKM.4, FCS_CKM_EXP.2, FCS_COP_EXP.2, FPT_TST_EXP.2,
2. The Table associated with FAU_GEN.1(1) was refined in the following ways:
   a. to indicate iteration numbers for FAU_GEN.1, FCS_CKM.1, FDP_RIP.1, FIA_AFL.1, FIA_ATD.1, FIA_UAU_EXP.5, FIA_UID.2, FIA_USB.1, FMT_SMR.1, and FTP_ITC_EXP.1;
   b. to add additional rows added via refinement for FAU_GEN_EXP.1, FCS_CKM.1(2), FCS_CKM.1(3), FCS_COP.1(1), FCS_COP.1(2), FMT_SMF.1(1), FMT_SMF.1(2), FMT_SMF.1(3), FPT_ITT.1, FPT_RVM.1(1), FPT_SEP.1(1), and FTA_TAB.1; and
   c. to change the FIA_UID.1 row to FIA_UID.2(1).
3. FAU_STG.1.2 requires …unauthorized modifications to the stored audit records in the audit trail as per CCv2.3. The requirement is shown below in its entirety.

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 stored audit records in the audit trail.

4. FCS_CKM.4 was updated as allowed by Precedent Decision 0135 to indicate a single overwrite and zeroes.
5. For FCS_CKM.1, added (1) to the requirement to reflect iteration one. Two additional iterations of requirement FCS_CKM.1 for SNMP and HTTPS/TLS have been added which required changing the original FCS_CKM.1 requirement to FCS_CKM.1(1). There is no content change.
6. FDP_PUD_EXP.1 was updated to remove the word "authenticated" from both bullets as the encryption happens prior to authentication.
7. For FIA_UID.2, added (1) to the requirement to reflect iteration one. One additional iteration of requirement was added to the environment. There is no content change.
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. 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.
10. FAU_GEN.1(2) was refined to explicitly refer to Table 16.
11. The Table associated with FAU_GEN.1(2) was refined in the following ways
    a. to indicate iteration numbers for FAU_GEN.1, FDP_RIP.1, FIA_AFL.1, FIA_ATD.1, FIA_UAU_EXP.5, FMT_SMR.1, and FTP_ITC_EXP.1;
    b. to add additional row added via refinement for FMT_MTD.1;
    c. to change the FIA_UID.1 row to FIA_UID.2(2);
    d. to update the auditable action for FMT_SMR.1(2) to "Modifications to the group of users that are part of a role"; and

e. to update the update the auditable action for FTP_ITC_EXP.1(2) to “Failure of trusted channel functions” and the additional details to “Identification of the initiator and target of failed trusted channel functions”.

12. FAU_SAR.1(2), FAU_STG.3, FIA_AFL.1(2), FMT_MOF.1(4), FMT_MTD.1(4), and FMT_SMR.1(2) were all refined to refer explicitly to the “OS Admin” role instead of the “administrator”.

13. FIA_UID.1 was refined to FIA_UID.2(2) as there were no actions allowed prior to identification.

14. FMT_SMR.1 was refined to list the actual administrator roles for the TOE.

15. FDP_PUD_EXP.1.1, FIA_AFL.1(1), FIA_UAU_EXP.5(1), FMT_MOF.1(1), FMT_MOF.1(2), FMT_MOF.1(3), FMT_MTD.1(1), FMT_MTD.1(2), FMT_SMF.1(1), and FTA_SSL.3 were refined to list the actual administrator roles with that responsibility.

16. FMT_MTD.1(3) was refined to list the actual administrator with the role responsibility.

Protection Profile Additions

1. The TOE for this ST contains functionality for Wireless IDS (WIDS) 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 WIDS functionality:

T.UNIDENTIFIED_ ACTIONS The administrator may not have the ability to notice potential security violations, thus limiting the administrator’s ability to identify and take action against a possible security breach.

P.WIRELESS_LOCATION_POLICY In concordance with the DOD 8100.2 Wireless LAN Policy, the TOE will provide location tracking for all 802.11 devices transmitting within the RF environment.

O.IDS_AUDIT_GENERATION The TOE will provide the capability to detect and create records of security relevant events from targeted IT System resource(s) (including the location of resources) and associate those events with the component that created the record.

2. The TOE evaluated configuration requires that there be only one WCS Configuration Administrator. This is captured in an assumption and environment objective. This ST claims conformance to the PP listed above with the following additions for the WCS Administrator.

A.ONE_WCS_ADMIN There will be only one administrator user performing WCS configuration administrator functions.

OE.ONE_WCS_ADMIN The maintainers of the TOE will follow the instructions of the Administrator Guide to ensure that only one WCS Configuration Administrator is permitted.

3. The TOE evaluated configuration requires that there be a separate network from the public client network for transfer of audit records to the syslog servers to protect the data. This is captured in an assumption and environment objective that already existed in the PP. This ST claims conformance to the PP listed above with the following addition for this network separation.

A.SYSLOG_SEP The syslog communications between the TOE components must happen over a separate protected network from the wireless client network.

4. The TOE evaluated configuration acknowledges that all users of the syslog host be will have access to the Syslog component of the TOE and are therefore assumed to by Syslog administrators.

A.SYSLOG_SEP	On the syslog host, all users are considered to be Syslog administrators.

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. Please see the original statements of these requirements in the "TOE Security Functional Requirements" section on page 37 to avoid inconsistency by copy and paste here.

The **FAU_GEN_EXP.1.1** SFR was added to cover the O.IDS_AUDIT_GENERATION which is not included in the PP.

The FCS_CKM.1(2) SFR was added to cover the SNMPv3 encryption channel provided by the TOE.

The FCS_CKM.1(3) SFR was added to cover the HTTPS encryption channel provided by the TOE.

The FCS_COP.1(1) and FCS_COP.1(2) SFRs were added to cover the SNMPv3 encryption channel provided by the TOE.

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

The FPT_ITT.1 SFR was added to cover the data transfer protection provided by the TOE between AP and Controller.

FAU_SAR.1, 2, and 3 were all iterated onto the TOE to cover the ability to review events being done on the TOE. FAU_SAR.2 was also iterated a third time onto the IT environment to address the IT environment providing access control to the syslog applications and their use to review the TOE events.

IT Environment Security Functional Requirement Additions:

The SFRs that were added to the set in the Protection Profile for the IT environment are listed in this section. Please see the original statements of these requirements in the "Security Requirements for the IT Environment" section on page 50 to avoid inconsistency by copy and paste here.

The SFR FIA_UAU.2 was added to satisfy the dependency of FIA_UID.2.

Rationale

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. Table 22 and Table 23 provide the mapping and rationale for the security objectives identified in the "Security Objectives" section on page 33 and the assumptions, threats, and policies identified in the "Security Environment" section on page 30.

Table 22 Threats, Assumptions, and 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_DE SIGN	O.IDS_AUDIT_GENERATION	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.ONE_WCS_ADMIN
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.UNIDENTIFIED_ ACTIONS									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	
P.WIRELESS_ OCATION_POLICY									X																					
A.NO_EVIL																					X									

Table 22 Threats, Assumptions, and Policies to Security Objectives Mapping (continued)

	O.ADMIN_GUIDANCE	O.AUDIT_GENERATION	O.CONFIGURATION_IDENTIFICATION	O.CORRECT_TSF_OPERATION	O.CRYPTOGRAPHY	O.CRYPTOGRAPHY_VALIDATED	O.DISPLAY_BANNER	O.DOCUMENTED_DE SIGN	O.IDS_AUDIT_GENERATION	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.ONE_WCS_ADMIN
A.NO_GENERAL_ PURPOSE																						X								
A.PHYSICAL																							X							
A.TOE_NO_BYPASS																													X	
A.ONE_WCS_ADMIN																														X
A.SYSLOG_SEP																								X						
A.SYSLOG_ADMIN																												X		

Table 23 Threats, Assumptions, and 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 ensure that the TOE will have adequate protection from external sources and that all TSP functions are invoked. OE.SELF_PROTECTION ensures that the TOE IT environment will have protection similar to that of the TOE

Table 23 Threats, Assumptions, and Policies to Security Objectives Rationale (continued)

Threat/Assumption/Policy	Security Objectives Rationale
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 IT environment. The environment also includes requirements that ensure protected channels are used to communicate with critical portions of the TOE IT environment. 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 or 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_RCR. 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.

Table 23 Threats, Assumptions, and Policies to Security Objectives Rationale (continued)

Threat/Assumption/Policy	Security Objectives Rationale
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 mitigate this threat by restricting access to administrative functions and management of TSF data to the administrator. OE.MANAGE ensures that the TOE IT environment 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 ensuing 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 IT environment 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 IT environment. 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.

Table 23 Threats, Assumptions, and Policies to Security Objectives Rationale (continued)

Threat/Assumption/Policy	Security Objectives Rationale
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.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 to 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 authorized or authenticated to have access to the data or TOE resources.
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.UNIDENTIFIED_ ACTIONS	O.IDS_AUDIT_GENERATION addresses this threat by providing an WIDS audit mechanism to create records based on the observed actions from specific IT System resources.
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 IT environment.

Table 23 Threats, Assumptions, and Policies to Security Objectives Rationale (continued)

Threat/Assumption/Policy	Security Objectives Rationale
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 IT environment 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 IT environment. 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 IT environment 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.CRYPTOGRAPHIC	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 crypto modules 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.

Table 23 Threats, Assumptions, and Policies to Security Objectives Rationale (continued)

Threat/Assumption/Policy	Security Objectives Rationale
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.IDS_AUDIT_GENERATION addresses this policy by providing an audit mechanism to create records based on the presence and location information 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 Environment" section on page 30. Therefore, these five objectives for the environment, OE.NO_EVIL, OE.PHYSICAL, OE.NO_GENERAL_PURPOSE, OE.TOE_NO_BYPASS, and OE.ONE_WCS_ADMIN trace to the assumptions trivially.

A.SYSLOG_SEP maps to OE.PROTECT_MGMT_COMMS by relying on a physically separate network to transfer audit information to the Syslog server.

A.SYSLOG_ADMIN maps to OE. TOE_ACCESS by relying on the IT environment to provide the access control to the Syslog server.

Rationale for Security Functional Requirements

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 24 identifies each Security Functional Requirement identified in "TOE Security Functional Requirements" section on page 37, the TOE security objective(s) identified in "Security Objectives for the TOE" section on page 34 that address it.

Table 24 and Table 26 provide the mapping and rationale for inclusion of each SFR in this ST.

Table 24 TOE 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.IDS_AUDIT_GENERATION	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_GEN_EXP.1									X								
FAU_SAR.1(1)		X															
FAU_SAR.2(1)		X															
FAU_SAR.3(1)		X															
FAU_SEL.1		X															
FCS_BCM_EXP.1					X	X											
FCS_CKM.1(1)					X	X											
FCS_CKM.1(2)					X	X											
FCS_CKM.1(3)					X	X											
FCS_CKM_EXP.2					X	X							X				
FCS_CKM.4					X	X							X				
FCS_COP.1(1)					X	X											
FCS_COP.1(2)					X	X											
FCS_COP_EXP.1					X	X											
FCS_COP_EXP.2					X	X											
FDP_RIP.1(1)													X				
FDP_PUD_EXP.1											X						
FIA_AFL.1(1)																X	
FIA_ATD.1(1)																X	
FIA_ATD.1(2)_																X	
FIA_UAU. 1											X					X	
FIA_UAU_EXP.5(1)											X					X	
FIA_UID.2(1)											X					X	
FIA_USB.1(1)		X															
FIA_USB.1(2)		X															
FMT_MOF.1(1)										X							
FMT_MOF.1(2)										X							

Table 24 TOE 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.IDS_AUDIT_GENERATION	O.MANAGE	O.MEDIATE	O.PARTIAL_FUNCTIONAL_TESTING	O.RESIDUAL_INFORMATION	O.SELF_PROTECTION	O.TIME_STAMPS	O.TOE_ACCESS	O.VULNERABILITY_ANALYSIS
FMT_MOF.1(3)										X							
FMT_MSA.2										X							
FMT_MTD.1(1)										X							
FMT_MTD.1(2)										X							
FMT_MTD.1(3)										X							
FMT_SMF.1(1)										X							
FMT_SMF.1(2)										X							
FMT_SMF.1(3)										X							
FMT_SMR.1(1)										X							
FPT_ITT.1														X			
FPT_RVM.1(1)														X			
FPT_SEP.1(1)														X			
FPT_STM_EXP.1		X													X		
FPT_TST_EXP.1				X													
FPT_TST_EXP.2				X													
FTA_SSL.3																X	
FTA_TAB.1							X										
FTP_ITC_EXP.1(1)		X														X	
FTP_TRP.1																X	
ACM_CAP.2			X														
ACM_SCP.1			X														
ADO_DEL.1	X																
ADO_IGS.1	X																
ADV_FSP.1								X									
ADV_HLD.1								X									
ADV_RCR.1								X									
AGD_ADM.1	X																
AGD_USR.1	X																
ATE_COV.1												X					

Table 24 TOE 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.IDS_AUDIT_GENERATION	O.MANAGE	O.MEDIATE	O.PARTIAL_FUNCTIONAL_TESTING	O.RESIDUAL_INFORMATION	O.SELF_PROTECTION	O.TIME_STAMPS	O.TOE_ACCESS	O.VULNERABILITY_ANALYSIS
ATE_FUN.1												X					
ATE_IND.2												X					
AVA_MSU.1	X																
AVA_SOF.1																X	X
AVA_VLA.1																	X
ALC_FLR.2			X														

Table 25 TOE Security Functional Requirement to TOE Security Objectives Rationale

Security Objective (TOE)	Security Functional Requirement Rationale
O.ADMIN_GUIDANCE	ADO_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 ADO_IGS.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_ADM. 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 setup and review the auditing features of the TOE. AGD_USR. 1 is 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. AVA_MSU. 1 ensures that the guidance documentation can be followed unambiguously to ensure the TOE is not mis-configured in an unsecure state due to confusing guidance.

Table 25 TOE Security Functional Requirement to TOE Security Objectives Rationale (continued)

Security Objective (TOE)	Security Functional Requirement Rationale
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_SAR.1(1) ensures that the TOE provides those responsible for the TOE with facilities to review the TOE audit records (e.g., the administrator can construct a sequence of events provided the necessary events were audited). FAU_SAR.2(1) restricts the ability to read the audit records to only the administrator. FAU_SAR.3(1) provides the administrator with the ability to selectively review the contents of the audit trail based on established criteria. This capability allows the administrator to focus their audit review to what is pertinent at that time. FAU_SEL.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 user identity 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_EXP.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_EXP.1(1) provides a trusted channel for services provided by the TOE IT environment (the audit server and the time server).
O.CONFIGURATION_ IDENTIFICATION	ACM_CAP.2 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. ACM_SCP. 1 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 those discovered by others. The flaw remediation process used by the developer corrects any discovered flaws and performs an analysis ensures new flaws are not created while fixing the discovered flaws.

Table 25 TOE Security Functional Requirement to TOE Security Objectives Rationale (continued)

Security Objective (TOE)	Security Functional Requirement Rationale
O.CORRECT_TSF_ OPERATION	FPT_TST_EXP. 1 is necessary to ensure the correct operation TSF hardware. If TSF software is corrupted it is possible that the TSF would no longer be able to enforce the security policies. This also holds true for TSF data, if TSF data is corrupt the TOE may not correctly enforce its security policies. The FPT_TST_EXP.2 functional requirement addresses the critical nature and specific handling of the cryptographic related TSF data. Since the cryptographic TSF data has specific FIPS PUB requirements associated with them it is important to ensure that any fielded testing on the integrity of these data maintains the same level of scrutiny as specified in the FCS functional requirements.
O.CRYPTOGRAPHY	The FCS requirements satisfy this objective by levying requirements that ensure the cryptographic standards include the NIST FIPS publications (where possible) and NIST approved ANSI standards. The intent is to have the satisfaction of the cryptographic standards be validated through a NIST FIPS 140-2 validation. FCS_BCM_EXP.1 is an explicit requirement that specifies the NIST FIPS rating level that the cryptographic module must satisfy. The level specifies the degree of testing of the module. The higher the level, the more extensive the module is tested. FCS_CKM_EXP.2 Cryptographic Key Handling and Storage requires that FIPS PUB 140-2 be satisfied when performing key entry and output. FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM.1(3) ensure that, if necessary, the TOE is capable of generating cryptographic keys. FCS_CKM.4 mandates the standards (FIPS 140-2) that must be satisfied when the TOE performs Cryptographic Key Zeroization. FCS_COP_EXP.1 requires that a NIST approved random number Generator is used. FCS_COP_EXP.2 requires that for data decryption and encryption that a NIST approved algorithm is used, and that the algorithm meets the FIPS PUB 140-2 standard. FCS_COP.1(1) requires that for data decryption and encryption that a NIST approved algorithm is used, and that the algorithm meets the FIPS PUB 46-3 standard. FCS_COP.1(2) requires that for data authentication that a NIST approved algorithm is used, and that the algorithm meets the FIPS PUB 180-2 standard.

Table 25 TOE Security Functional Requirement to TOE Security Objectives Rationale (continued)

Security Objective (TOE)	Security Functional Requirement Rationale
O.CRYPTOGRAPHY_ VALIDATED	The FCS requirements satisfy this objective by levying requirements that ensure the cryptographic standards include the NIST FIPS publications (where possible) and NIST approved ANSI standards. The intent is to have the satisfaction of the cryptographic standards be validated through a NIST FIPS 140-2 validation. FCS_BCM_EXP.1 is an explicit requirement that specifies the NIST FIPS rating level that the cryptographic module must satisfy. The level specifies the degree of testing of the module. The higher the level, the more extensive the module is tested. FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM.1(3) ensure that, if necessary, at the TOE is capable of generating cryptographic keys. FCS_CKM_EXP.2 Cryptographic Key Handling and Storage requires that FIPS PUB 140-2 be satisfied when performing key entry and output. FCS_CKM.4 mandates the standards (FIPS 140-2) that must be satisfied when the TOE performs Cryptographic Key Zeroization. FCS_COP_EXP.1 requires that a NIST approved random number Generator is used. FCS_COP_EXP.2 requires that for data decryption and encryption that a NIST approved algorithm is used, and that the algorithm meets the FIPS PUB 140-2 standard. FCS_COP.1(1) requires that for data decryption and encryption that a NIST approved algorithm is used, and that the algorithm meets FIPS PUB 46-3 standard. FCS_COP.1(2) requires that for data authentication that a NIST approved algorithm is used, and that the algorithm meets the FIPS PUB 180-2 standard.
O.DISPLAY_BANNER	FTA_TAB. 1 meets this objective by requiring the TOE display a 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.1, ADV_HLD.1, ADV_RCR.1 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_RCR. 1 ensures that the TOE design is consistent across the High Level Design and the Functional Specification.
O.IDS_AUDIT_ GENERATION	FAU_GEN_EXP.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 WIDS 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 WIDS audit record for each auditable event. There is a minimum set of information that must be present in every WIDS audit record and this requirement defines that.

Table 25 TOE Security Functional Requirement to TOE Security Objectives Rationale (continued)

Security Objective (TOE)	Security Functional Requirement Rationale
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 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 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_EXP.1 allows the administrator to control whether or not unencrypted data will be allowed to pass through the TOE. FIA_UAU.1, FIA_UAU_EXP.5(1) and FIA_UID.2(1) ensure that the TOE has the ability to mediate packet flow based on the authentication credentials of the wireless user.
O.PARTIAL_ FUNCTIONAL_ TESTING	In order to satisfy O.FUNCTIONAL_TESTING, the ATE class of requirements is necessary. 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.1 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.

Table 25 TOE Security Functional Requirement to TOE Security Objectives Rationale (continued)

Security Objective (TOE)	Security Functional Requirement Rationale
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_EXP.2 places requirements on how cryptographic keys are managed within the TOE. This requirement places restrictions in addition to FDP_RIP.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	FPT_SEP.1(1) was chosen to ensure the TSF provides a domain that protects itself from untrusted users. If the TSF cannot protect itself it cannot be relied upon to enforce its security policies. FPT_RVM.1(1) ensures that the TSF makes policy decisions on all interfaces that perform operations on subjects and objects that are scoped by the policies. Without this non-bypassability requirement, the TSF could not be relied upon to completely enforce the security policies, since an interface(s) may otherwise exist that would provide a user with access to TOE resources (including TSF data and executable code) regardless of the defined policies. This includes controlling the accessibility to interfaces, as well as what access control is provided within the interfaces. FPT_ITT.1 ensures that the TSF protects TSF data from modification and disclosure as it is transmitted between separate parts of the TOE.
O.TIME_STAMPS	FPT_STM_EXP.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.

Table 25 TOE Security Functional Requirement to TOE Security Objectives Rationale (continued)

Security Objective (TOE)	Security Functional Requirement Rationale
O.TOE_ACCESS	FIA_UID.2(1) 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. AVA_SOF.1 requires that any permutational or probabilistic mechanism in the TOE be analyzed be found to be resistant to attackers possessing a "low" attack potential. This provides confidence that security mechanisms vulnerable to guessing type attacks are resistant to casual attack. FIA_UAU.1 and FIA_UAU_EXP.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 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 a inactive user and administrative sessions are dropped. FTP_TRP.1 ensures that remote users have a trusted path in order to authenticate. FTP_ITC_EXP.1 provides a trusted channel for services provided by the TOE IT environment (the remote authentication server)
O.VULNERABILITY_ ANALYSIS	AVA_VLA.1 requires the developer to perform a search for obvious vulnerabilities in all the TOE deliverables. The developer must then document the disposition of those obvious vulnerabilities. The evaluator then builds upon this analysis during vulnerability testing. This component provides the confidence that obvious security flaws have been either removed from the TOE or otherwise mitigated. AVA_SOF.1 requires that any permutational or probabilistic mechanism in the TOE be analyzed be found to be resistant to attackers possessing a "low" attack potential. This provides confidence that the security mechanisms vulnerable to guessing type attacks are resistant to casual attack.

Rationale for Security Functional Requirements of the IT Environment

This section provides rationale for the IT Environment's Security Functional Requirements demonstrating that the IT Environment's Security Functional Requirements are suitable to address the IT Environment's security objectives. Table 26 and Table 27 provide the mapping and rationale for IT environment security objectives and SFRs.

Table 26 IT Environment Security Functional Requirements to IT Environment Security Objectives Mapping

	OE.AUDIT_PROTECTION	OE.AUDIT_REVIEW	OE.MANAGE	OE.NO_EVIL	OE.PROTECT_MGMT_COMMS	OE.RESIDUAL_INFORMATION	OE.SELF_PROTECTION	OE.TOE_ACCESS	OE.TIME_STAMPS	OE.TOE_NO_BYPASS
FAU_GEN.1(2)		X								
FAU_SAR.1(2)		X								
FAU_SAR.2(2)	X									
FAU_SAR.2(3)	X									
FAU_SAR.3(2)		X								
FAU_STG.1	X									
FAU_STG.3	X									
FDP_RIP.1(2)						X				
FIA_AFL.1(2)								X		
FIA_ATD.1(3)								X		
FIA_UAU_EXP.5(2)								X		X
FIA_UAU.2								X		X
FIA_UID.2(2)								X		X
FMT_MOF.1(4)	X		X							
FMT_MTD.1(4)									X	
FMT_SMR.1(2)	X		X							
FPT_STM.1									X	
FPT_RVM.1(2)							X			
FPT_SEP.1(2)							X			
FTP_ITC_EXP.1(2)					X					
AGD_ADM.1				X						

Table 27 IT Environment Security Functional Requirements to IT Environment Security Objectives Rationale

Security Objective (IT Environment)	Security Objectives Rationale
OE.AUDIT_PROTECTION	FAU_SAR.2(2) and FAU_SAR.2(3) restrict the ability to read the audit records to only the administrator. The exception to this is that all administrative roles have access to the audit record information presented in the alarm indicating a potential security violation. FAU_STG.1 restricts the ability to delete or modify audit information to the administrators. The TSF will prevent modifications of the audit records in the audit trail. FAU_STG.3 ensures that the administrator will take actions when the audit trail exceeds pre-defined limits. FMT_MOF.1(4) and FMT_SMR.1(2)specifies the ability of the administrators to control the security functions associated with audit and alarm generation. The ability to control these functions has been assigned to the appropriate administrative roles.
OE.AUDIT_REVIEW	FAU_SAR.1(2) ensures that the IT environment provides those responsible for the TOE with facilities to review the TOE audit records (e.g., the administrator can construct a sequence of events provided the necessary events were audited). FAU_SAR.3(2) provides the administrator with the ability to selectively review the contents of the audit trail based on established criteria. This capability allows the administrator to focus their audit review to what is pertinent at that time. FAU_GEN.1(2) ensures that the TOE IT environment will generate appropriate audit events to support the TOE.
OE.MANAGE	FMT_MOF.1(4) ensures that the TOE IT environment limits access to TSF management functions to the administrator. FMT_SMR.1(2) ensures that the TOE IT environment provides an administrative role that may be used to manage both the TOE and the IT environment.
OE.NO_EVIL	The AGD_ADM.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 setup and review the auditing features of the TOE.
OE.PROTECT_MGMT_COMMS	FTP_ITC_EXP.1(2) provides a trusted channel for services provided by the TOE IT environment to the TOE (the remote authentication server; and time server)
OE.RESIDUAL_INFORMATION	FDP_RIP.1(2) ensures that the TOE IT environment provides same protections for residual information in a network packet that the TOE will provide. This ensures that neither the TOE nor the TOE IT environment will allow data from previously transmitted packets to be inserted into new packets.
OE.SELF_PROTECTION	The TOE IT environment must protect itself in a manner similar to that provided for the TOE. FPT_SEP.1(2) ensures the environment provides a domain that protects itself from untrusted users. If the environment cannot protect itself it cannot be relied upon to enforce its security policies. FPT_RVM.1(2) ensures that the environment makes policy decisions on all interfaces that perform operations on subjects and objects that are scoped by the policies.

Table 27 IT Environment Security Functional Requirements to IT Environment Security Objectives Rationale

Security Objective (IT Environment)	Security Objectives Rationale
OE.TOE_ACCESS	The TOE IT environment will provide a remote authentication mechanism in order to support TOE authentication of users. FIA_UAU_EXP.5(2) and FIA_UID.2(2) ensure that users are identified and authenticated. FIA_ATD.1(3) and FIA_AFL.1(2) ensure that the proper attributes are associated with users and that authentication failure is handled properly.
OE.TOE_NO_BYPASS	FIA_UAU_EXP.5(2), FIA_UAU.2, and FIA_UID.2(2) ensure that the wireless user's authentication credentials are used to make sure that the wireless client cannot bypass the TOE.
OE.TIME_STAMPS	FPT_STM.1 requires that the TOE IT environment be able to provide reliable time stamps for its own use and that of the TOE. 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. FMT_MTD.1(4) helps satisfy this objective by providing that there be a management function of the administrator or an authorized IT entity that will set the time and date used to provide reliable time stamps to the TOE.

TOE Security Functions

This section demonstrates the suitability of the security functions defined in the "TOE Security Functions" section on page 57, of meeting the TOE's Security Functional Requirements identified in the "TOE Security Functional Requirements" section on page 37 and that the security functional requirements are completely and accurately met by the TOE's Security Functions identified in "TOE Security Functions".

Table 28 demonstrates the correspondence between the Security Functions and the TOE Security Functional Requirements. With the demonstration of correspondence given in Table 29 and the descriptions of the security functions given in "TOE Security Functions" on how the security functions are providing the functionality to meet the security functional requirements this provides the evidence of suitability of the security functions in meeting the security functional requirements stated in "TOE Security Functional Requirements".

Table 28 TOE Security Functional Requirement to TOE Security Functions Mapping

TOE Security Functional Requirement	Administration	Audit	Encryption	Identification and Authentication	Information Flow Control	Self Protection
FAU_GEN.1(1)		X				
FAU_GEN.2		X				

Table 28 TOE Security Functional Requirement to TOE Security Functions Mapping (continued)

TOE Security Functional Requirement	Administration	Audit	Encryption	Identification and Authentication	Information Flow Control	Self Protection
FAU_GEN_EXP.1		X				
FAU_SAR.1(1)		X				
FAU_SAR.2(1)		X				
FAU_SAR.3(1)		X				
FAU_SEL.1		X				
FCS_BCM_EXP.1			X			
FCS_CKM.1(1)			X			
FCS_CKM.1(2)			X			
FCS_CKM.1(3)			X			
FCS_CKM_EXP.2			X			
FCS_CKM.4			X			
FCS_COP.1(1)			X			
FCS_COP.1(2)			X			
FCS_COP_EXP.1			X			
FCS_COP_EXP.2			X			
FDP_PUD_EXP.1					X	
FDP_RIP.1(1)						X
FIA_AFL.1(1)				X		
FIA_ATD.1(1)				X		
FIA_ATD.1(2)				X		
FIA_UAU.1				X		
FIA_UAU_EXP.5(1)				X		
FIA_UID.2(1)				X		
FIA_USB.1(1)				X		
FIA_USB.1(2)				X		
FMT_MOF. 1(1)	X					
FMT_MOF. 1(2)	X					
FMT_MOF.1(3)	X					
FMT_MSA.2	X					

Table 28 TOE Security Functional Requirement to TOE Security Functions Mapping (continued)

TOE Security Functional Requirement	Administration	Audit	Encryption	Identification and Authentication	Information Flow Control	Self Protection
FMT_MTD.1(1)	X					
FMT_MTD.1(2)	X					
FMT_MTD.1(3)	X					
FMT_SMF.1(1)	X					
FMT_SMF.1(2)	X					
FMT_SMF.1(3)	X					
FMT_SMR.1(1)	X					
FPT_ITT.1						X
FPT_RVM.1(1)						X
FPT_SEP.1(1)						X
FPT_STM_EXP.1		X				
FPT_TST_EXP.1						X
FPT_TST_EXP.2						X
FTA_SSL.3	X					
FTA_TAB.1				X		
FTP_ITC_EXP.1(1)				X		
FTP_TRP.1				X		

Table 29 Rationale of How the SF(s) Meet the SFR(s)

SFR	SF and Rationale
FAU_GEN.1	Is implemented by the Audit security function. The Audit security function generates audit records based on security relevant events that occur when using security functions.
FAU_GEN.2	Is implemented by the Audit security function. The Audit security function ensures that auditable events that occur based because of an action of an identified user will be associated with the auditable event in the audit record generated by the Audit security function.
FAU_GEN_EXP.1	Is implemented by the Audit security function. The Audit security function will generates audit records based on wireless intrusions that it detects based on signatures analysis of the observed network traffic.
FAU_SAR.1(1)	Is implemented by the Audit security function. The Audit security function allows administrators to view audit events through the ACS GUI and the syslog interfaces.

Table 29 Rationale of How the SF(s) Meet the SFR(s) (continued)

SFR	SF and Rationale
FAU_SAR.2(1)	Is implemented by the Audit security function. The Audit security function restricts the ability to review the audit data to ACS and Syslog administrators.
FAU_SAR.3(1)	Is implemented by the Audit security function. The Audit security function allows administrators to selectively review the contents of the audit trail based on event type, date, and time.
FAU_SEL.1	Is implemented by the Audit security function. The Audit security function allows administrators to enable or disable auditable events through the use of GUI administrative interfaces. The enabling and disabling of auditable events allows an administrator to select (selectively audit) those events they want or do not want audited.
FCS_BCM_EXP.1	Is implemented by the Encryption security function. The Encryption security function implements this requirement by having the APs and Controllers going through an outside independent FIPS 140-2 validation at a FIPS approved laboratory. The APs and Controllers are the crypto modules. The FIPS Certificates are #693, #695 and #729 for the Controller, APs and WiSM, respectively
FCS_CKM.1(1)	Is implemented by the Encryption security function. The Encryption security function implements this requirement by having FIPS validated APs and Controllers that use 128 bit keys for the AES cryptographic algorithm.
FCS_CKM.1(2)	Is implemented by the Encryption security function. The Encryption security function implements this requirement by contributing to the SNMPv3 functionality to protect the SNMP interface by the generation of keys based on user passwords
FCS_CKM.1(3)	Is implemented by the Encryption Security Function Function. The TOE implements the cryptographic key generation functions of the TLS protocols to protect the communication channel for remote administration.
FCS_CKM_EXP.2	The TOE supports manual key loading by providing for encryption capabilities that allow for the use of manually loaded certificates for both the Controllers and ACS.
FCS_CKM.4	Is implemented by the Encryption security function. The Encryption security function implements this requirement by having FIPS validated APs and Controllers that use and satisfy the key zeroization requirements specified in FIPS PUB 140-2 Key Management Security Levels 1 as validated by an independent accredited FIPS laboratory.
FCS_COP.1(1) and FCS_COP.1(2)	Is implemented by the Encryption Security Function by contributing to the SNMPv3 functionality to protect the SNMP interface (encryption and decryption).
FCS_COP_EXP.1	Is implemented by the Encryption security function. The Encryption security function implements this requirement by having FIPS validated APs and Controllers that use and satisfy the random number generation requirements by using a FIPS approved random number generator.
FCS_COP_EXP.2	Is implemented by the Encryption security function. The Encryption security function implements this requirement by having FIPS validated APs and Controllers that are crypto modules that encrypt and decrypt based on the FIPS-140-2 approved AES algorithm that operates in the FIPS approved CCM (CCMP) mode of operation using 128 bit keys. These encryption capabilities were validated by an independent accredited FIPS laboratory. The TOE implements TLS crypto operations to protect the communication channel for remote administration.
FDP_PUD_EXP.1	Is implemented by the Information Flow Control security function. The Information Flow Control security function keeps track of the encryption policy that has been administratively established. Based on the encryption policy being enabled or disabled will decide whether the APs and Controllers will encrypt and decrypt communications with wireless clients.
FDP_RIP.1(1)	Is implemented by the Self Protection security function. The Self Protection security function ensures that the AP does not send any information from a previous user session to any wireless clients.

Table 29 Rationale of How the SF(s) Meet the SFR(s) (continued)

SFR	SF and Rationale
FIA_AFL.1(1)	Is implemented by the Identification and Authentication security function. The Identification and Authentication security function provides the administrator the capability to set how many failed login attempts are accepted based on those administrators attempting to login remotely. Further, if the number of attempts is exceeded the TOE will prevent any further login attempts.
FIA_ATD.1(1)	Is implemented by the Identification and Authentication security function. The Identification and Authentication security function provides for the capability to determine if an administrator can just view information (read) or be able to modify information (read/write).
FIA_ATD.1(2)	Is implemented by the Identification and Authentication security function. The Identification and Authentication security function provides for the maintenance of the cryptographic session keys for a user that is involved with encrypted communications with an AP.
FIA_UAU. 1	Is implemented by the Identification and Authentication security function. The Identification and Authentication security function provides logins for all administrators trying to gain access to a TOE component. The Identification and Authentication security function provides GUI and command line login capabilities depending on the way the administrator is trying to login and requires the successful logging in of the administrator before they are granted the use of any other security functions.
FIA_UAU_EXP.5(1)	Is implemented by the Identification and Authentication security function. The Identification and Authentication security function provides administrators the ability to configure if the ACS is to be used for authenticating remote users and administrators. Further, all components of the TOE have the ability to local authenticate users trying to authenticate locally if the capability is enabled.
FIA_UID.2(1)	Is implemented by the Identification and Authentication security function. The Identification and Authentication security function identifies all wireless users, remote administrators, and local administrators before allowing the use of any other function of the TOE. For wireless users the security function identifies them by MAC address, SSID, and the authentication credentials when EAP-TLS or EAP-FAST is used along with the use of user's names and passwords. For either remote or local administrators the security function provides login capabilities that require a user identifier.
FIA_USB.1(1)	Is implemented by the Identification and Authentication security function. The Identification and Authentication security function provides the capability to associate the viewing and/or modification capabilities an administrator has to the subjects that are created on their behalf when they have successfully identified and authenticated to the TOE. Further, the security function will only allow an administrator to change the capabilities of a user with administrator capabilities.
FIA_USB.1(2)	Is implemented by the Identification and Authentication security function. The Identification and Authentication security function associates a session ID and session keys to wireless users of the TOE. The security functions does these association of security attributes to wireless users after they have successfully authenticated. The session ID security attribute will only change if the wireless disassociates and then re-associates with an AP and the session keys security attributes will change periodically based on the key management established by the administrator.
FMT_MOF. 1(1)	Is implemented by the Administration security function. The Administration security function requires that a user successfully authenticate as an administrator before they can manage any of the cryptographic capabilities dealing with loading a key, deleting/zeroizing a key, setting a key lifetime, setting the cryptographic algorithm, enabling or disabling encryption, and executing hardware self test for the crypto modules.
FMT_MOF. 1(2)	Is implemented by the Administration security function. The Administration security function requires that a user successfully authenticate as an administrator before they are allowed to carry out an activities involving enabling, disabling, and modification of the auditing capabilities of the TOE.

Table 29 Rationale of How the SF(s) Meet the SFR(s) (continued)

SFR	SF and Rationale
FMT_MOF.1(3)	Is implemented by the Administration security function. The Administration security function requires that a user successfully authenticate as an administrator before they are allowed to carry out an activities involving modification to the authentication capabilities of the TOE. Specifically the Administration security function requires a user to be successfully authenticated as an administrator to allow or disallow the use of an ACS, to set the number of failures for authentication, and for defining the time limit for a session.
FMT_MSA.2	Is implemented by the Administration security function. The Administration security function validates all attributes that a successfully authenticated administrator may input. The validation occurs and the WCSs and at the Controllers.
FMT_MTD.1(1)	Is implemented by the Administration security function. The Administration security function requires a user to have successfully authenticated as an administrator before they are allowed to query, modify, clear, or create the set of rules the determine auditable events by using the management features available in the Controllers, the WCSs, and the ACSs.
FMT_MTD.1(2)	Is implemented by the Administration security function. The Administration security function requires a user to have successfully authenticated as an administrator before they are allowed to query, modify, clear, or create the authentication credentials and user identification credentials by using the management features available in the Controllers, the WCSs, and the ACSs.
FMT_MTD.1(3)	Is implemented by the Administration security function. The Administration security function requires an ACS Administrator to have successfully authenticated in order to be able to modify identification and authentication credentials associated with any user.
FMT_SMF.1(1)	Is implemented by the Administration security function. The Administration security function allows an authenticated administrator to configure the encryption and decryption capabilities (defined in FCS_COP_EXP.2) of the AP by using the WCS.
FMT_SMF.1(2)	Is implemented by the Administration security function. The Administration security function only allows successfully authenticated administrators to query, enable, or disable auditing and accounting through the use of the WCS and ACS management interfaces.
FMT_SMF.1(3)	Is implemented by the Administration security function. The Administration security function only allows successfully authenticated administrators to query, set, modify, and delete the keys dealing with wireless users and the encryption and decryption done with wireless users, and doing cryptographic testing through the use of the WCS and ACS management interfaces.
FMT_SMR.1(1)	Is implemented by the Administration security function. The Administration security function maintains roles for administrators and for wireless users through the APs, Controllers, WCSs, and the ACSs.
FPT_ITT.1	Is implemented by the Self Protection Security Function. The TOE enforces protected communication of bridging and control information between the APs and Controllers using x.509 certificates for mutual authentication, and AES-CCM for encryption.
FPT_RVM.1(1)	Is implemented by the Self Protection security function. All components of the TOE make sure that their security enforcing functions are invoked and succeed before allowing any other mediated action to occur with respect to that component based on the component and the IT Environment the component is operating in. (Also see the "TOE Summary Specification" section on page 57, for discussion of self protection)

Table 29 Rationale of How the SF(s) Meet the SFR(s) (continued)

SFR	SF and Rationale
FPT_SEP.1(1)	Is implemented by the Self Protection security function. All components of the TOE maintain a security domain for themselves based on the component and the IT environment the component operates in. The TOE maintains a security domain for its own use that is free of interference and tampering as a system of components based on the security capabilities offered by the individual components and the domain separation requirements that have been levied on the IT Environment that host the ACSs and WCSs. (Also see the "TOE Summary Specification" section on page 57, for discussion of self protection)
FPT_STM_EXP.1	Is implemented by the Audit security function. The Audit security function allows successfully authenticated administrator to configure the TOE components to obtain time stamps for its own use from an NTP server.
FPT_TST_EXP.1	Is implemented by the Self Protection security function. The portions of the TSF that are hardware based and TSF enforcing are the APs and the Controllers. These hardware components perform self test when rebooted which is able to be command by a successfully authenticated administrator.
FPT_TST_EXP.2	Is implemented by the Self Protection security function. The portions of the TSF are crypto modules are the APs and the Controllers. These components perform cryptographic testing based on FIPS 140-2. The compliance to this was verified during an independent FIPS validation at a FIPS approved testing laboratory.
FTA_SSL.3	Is implemented by the Administration security function. The Administration security function allows a successfully authenticated administrator to configure a time interval of inactivity for users that will terminate a local interactive session or a remote wireless session. This is done through the ACSs and WCSs.
FTA_TAB.1	Is implemented by the Identification and Authentication security function. The Identification and Authentication security functions allows for the establishment of an access banner for users before they are authenticated.
FTP_ITC_EXP.1(1)	Is implemented by the Identification and Authentication security function. The Identification and Authentication provides for the use of AES RADIUS key wrap, HTTPS, SNMPv3, and AES to established trusted channels between TOE components and IT resources in the IT Environment to protect all communications dealing with management and authentication.
FTP_TRP.1	Is implemented by the Identification and Authentication security function. The Identification and Authentication provides the use of 802.11i, WPA2, 802.1x and the EAP-TLS and EAP-FAST protocols and methods of protection to setup trusted paths between wireless clients and the APs and the ACSs for those interaction dealing with authentication. The use of these protocols and methods allows for the creation of logically distinct paths, provides assured identification of its end points and protects the communication from replay.

TOE Security Functional Component Hierarchies and Dependencies

This section of the ST demonstrates that the identified TOE and IT Security Functional Requirements include the appropriate hierarchical SFRs and dependent SFRs. Table 30 lists the TOE Security Functional Components and the Security Functional Components each are hierarchical to and dependent upon and any necessary rationale. Table 31 lists the IT Environment 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 30 TOE 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_EXP.1)
FAU_GEN.2	No other components	FPT_STM.1	Satisfied (by FPT_STM_EXP.1)
FAU_GEN_EXP.1	N/A	FPT_STM.1	Satisfied (by FPT_STM_EXP.1)
FAU_SAR.1(1)	No other components	FAU_GEN.1	Satisfied by FAU_GEN.1(1)
FAU_SAR.2(1)	No other components	FAU_SAR.1	Satisfied by FAU_SAR.1(1)
FAU_SAR.3(1)	No other components	FAU_SAR.1	Satisfied by FAU_SAR.1(1)

FAU_SEL.1	No other components	FAU_GEN.1;
		FMT_MTD.1
			Satisfied by FAU_GEN.1(1);
			FMT_MTD.1(1)

FCS_BCM_EXP.1	N/A	None	N/A
FCS_CKM.1(1)	No other components	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4 FMT_MSA.2	Satisfied by FCS_CKM_EXP.2 FCS_COP_EXP.1 FCS_CKM.4 FMT_MSA.2
FCS_CKM.1(2)	No other components	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4 FMT_MSA.2	Satisfied by FCS_COP.1(1) and FCS_COP.1(2) FCS_CKM.4 FMT_MSA.2
FCS_CKM.1(3)	No other components	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4 FMT_MSA.2	Satisfied by FCS_COP_EXP.2 FCS_CKM.4 FMT_MSA.2
FCS_CKM_EXP.2	N/A	[FDP_ITC.1 or FCS_CKM.1] FMT_MSA	Satisfied by FCS_CKM.1(1) FMT_MSA.2
FCS_CKM.4	No other components	[FDP_ITC.1 or FCS_CKM.1] FMT_MSA.2	Satisfied by FCS_CKM.1(1) FMT_MSA.2
FCS_COP.1(1)	N/A	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	Satisfied by FCS_CKM.1(2) FCS_CKM.4 FMT_MSA.2

Table 30 TOE Security Functional Requirements Dependency Rationale (continued)

Security Functional Requirement (TOE)	Hierarchical To	Dependency	Rationale
FCS_COP.1(2)	N/A	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	Satisfied by FCS_CKM.1(2) FCS_CKM.4 FMT_MSA.2
FCS_COP_EXP.1	N/A	[FDP_ITC.1 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	Satisfied by FCS_CKM.1(1) FMT_MSA.2
FCS_COP_EXP.2	N/A	[FDP_ITC.1 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	Satisfied by FCS_CKM.1(1) FCS_CKM.4 FMT_MSA.2
FDP_PUD_EXP.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(1)
FIA_UAU_EXP.5(1)	N/A	FIA_UID.1	Satisfied by FIA_UID.2(1)
FIA_UID.2(1)	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 FMT_SMR.1
FMT_MOF. 1(2)	No other components	FMT_SMF.1 FMT_SMR.1	Satisfied by FMT_SMF.1 FMT_SMR.1
FMT_MOF.1(3)	No other components	FMT_SMF.1 FMT_SMR.1	Satisfied by FMT_SMF.1 FMT_SMR.1

Table 30 TOE Security Functional Requirements Dependency Rationale (continued)

Security Functional Requirement (TOE)	Hierarchical To	Dependency	Rationale
FMT_MSA.2	No other components	ADV_SPM.1 [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	Satisfied by FMT_SMR.1
FMT_MTD.1(2)	No other components	FMT_SMR.1	Satisfied by FMT_SMR.1
FMT_MTD.1(3)	No other components	FMT_SMR.1	Satisfied by FMT_SMR.1
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(1)
FPT_ITT.1	No other components	None	N/A
FPT_RVM.1(1)	No other components	None	N/A
FPT_SEP.1(1)	No other components	None	N/A
FPT_STM_EXP.1	N/A	None	N/A
FPT_TST_EXP.1	N/A	FCS_CKM.2, FCS_CKM.4, FCS_COP_EXP.1, FCS_COP_EXP.2	Satisfied by FCS_CKM_EXP.2, FCS_CKM.4, FCS_COP_EXP.1, FCS_COP_EXP.2
FPT_TST_EXP.2	N/A	FCS_CKM.2, FCS_CKM.4, FCS_COP_EXP.1, FCS_COP_EXP.2	Satisfied by FCS_CKM_EXP.2, FCS_CKM.4, FCS_COP_EXP.1, FCS_COP_EXP.2
FTA_SSL.3	No other components	None	N/A
FTA_TAB.1	No other components	None	N/A

Table 30 TOE Security Functional Requirements Dependency Rationale (continued)

Security Functional Requirement (TOE)	Hierarchical To	Dependency	Rationale
FTP_ITC_EXP.1(1)	N/A	None	N/A
FTP_TRP.1	No other components	None	N/A

Table 31 IT Environment Security Functional Requirements Dependency Rationale

Security Functional Requirement (IT Environment)	Hierarchical To	Dependency	Rationale
FAU_GEN.1(2)	No other components	None	N/A
FAU_SAR.1(2)	No other components	FAU_GEN.1	Satisfied by FAU_GEN.1(2)
FAU_SAR.2(2)	No other components	FAU_SAR.1	Satisfied by FAU_SAR.1(2)
FAU_SAR.2(3)	No other components	FAU_SAR.1	Satisfied by FAU_SAR.1(1)
FAU_SAR.3(2)	No other components	FAU_SAR.1	Satisfied by FAU_SAR.1(20
FAU_STG.1	No other components	FAU_GEN.1	Satisfied by FAU_GEN.1(2)
FAU_STG.3	No other components	FAU_STG.1	Satisfied by FAU_STG.1
FDP_RIP.1(2)	No other components	None	N/A
FIA_AFL.1(2)	No other components	FIA_UAU.1	Satisfied by FIA_UAU.2
FIA_ATD.1(3)	No other components	None	N/A
FIA_UAU_EXP.5(2)	N/A	FIA_UID.1	Satisfied by FIA_UID.2(2)
FIA_UAU.2	FIA_UAU.1	FIA_UID.1	Satisfied by FIA_UID.2(2)
FIA_UID.2(2)	FIA_UID.1	None	N/A
FMT_MOF.1(4)	No other components	FMT_SMF.1 FMT_SMR.1	Satisfied by FMT_SMR.1(2)
FMT_SMR.1(2)	No other components	None	N/A
FPT_STM.1	No other components	None	N/A
FPT_RVM.1(2)	No other components	None	N/A

Table 31 IT Environment Security Functional Requirements Dependency Rationale (continued)

Security Functional Requirement (IT Environment)	Hierarchical To	Dependency	Rationale
FPT_SEP.1(2)	No other components	None	N/A
FTP_ITC_EXP.1(2)	N/A	None	N/A

Table 32 identifies the functional requirement, its correspondent dependency and the analysis and rationale for not supporting the dependency in this ST.

Table 32 Unsupported Dependency Rationale

Requirement	Unsatisfied Dependencies	Dependency Analysis and Rationale
FMT_MSA.2	ADV_SPM.1	The US Government has determined that the requirement for the vendor to provide an informal TOE security policy model (ADV_SPM.1) is beyond what is required at EAL2. Typically, this requirement is part of an EAL 4 requirement set.
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.
ACM_SCP.1	ACM_CAP.3	This ST is based on the PP which was validated as acceptable without the inclusion of this dependency.

Rationale for Explicitly Stated SFRs

Table 33 presents the rationale for the inclusion of the explicit requirements found in this ST.

These requirements were all designed to fit into their respective requirement classes: FAU, FCS, FDP, FIA, FPT, and FTP.

Table 33 Rationale for Explicit Requirements for the TOE

Explicit Requirement	Identifier	Rationale
FAU_GEN_EXP.1	Audit Data Generation (WIDS Audit Records)	This explicit requirement is necessary because the FAU_GEN.1 requirement applies to audit functions of the TOE, while this explicit wording applies to the WIDS audit capability for events observed from other products.
FCS_BCM_EXP.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_EXP.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_EXP.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.

Table 33 Rationale for Explicit Requirements for the TOE (continued)

Explicit Requirement	Identifier	Rationale
FCS_COP_EXP.2	Cryptographic Operation	This explicit requirement is necessary because it describes requirements for a crypto module rather that the entire TSF.
FDP_PUD_EXP.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_EXP.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_EXP.5	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_EXP.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_EXP.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.
FPT_TST_EXP.2	Testing of cryptographic modules	This explicit requirement is necessary because the basic self test requirement does not specify the required elements for testing of cryptographic functions, as called out in this explicit requirement.
FTP_ITC_EXP.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.

Rationale for Strength of Function Claim

Part 1 of the CC defines "strength of function" in terms of the minimum efforts assumed necessary to defeat the expected security behavior of a TOE security function. There are three strength of function levels defined in Part 1: SOF-basic, SOF-medium and SOF-high. SOF-basic is the strength of function level chosen for this ST.

SOF-basic states, "a level of the TOE strength of function where analysis shows that the function provides adequate protection casual breach of TOE by attackers possessing a low attack potential." The rationale for choosing SOF-basic was to be consistent with the TOE objective O.VULNERABILITY_ANALYSIS and assurance requirements included in this ST. Specifically, AVA_VLA. 1 requires that the TOE be resistant obvious vulnerabilities, this is consistent with SOF-basic, which is the lowest strength of function metric.

Consequently, security functions with probabilistic or permutational mechanisms chosen for inclusion in this ST were determined to adequately protect information in a Basic Robustness Environment with the low attack potential threat identified in the "Security Environment" section on page 30 of this ST.

Assurance Measures Rationale for TOE Assurance Requirements

The TOE stresses assurance through vendor actions that are within the bounds of current best commercial practice. The TOE provides, primarily via review of vendor-supplied evidence, independent confirmation that these actions have been competently performed.

The general level of assurance for the TOE is:

A. Consistent with current best commercial practice for IT development and provides a product that is competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market.

   The TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL2 from part 3 of the Common Criteria.

Table 34 provides a reference between each TOE assurance requirement and the related vendor documentation that satisfies each requirement. N/A means not applicable because the Assurance Component does not have any dependencies.

Table 34 EAL2 SAR Dependencies

Assurance Component ID	Assurance Component Name	Dependencies	Satisfied
ACM_CAP.2	Configuration items	None	N/A
ACM_SCP.1	TOE CM coverage	ACM_CAP.3	No
ADO_DEL.1	Delivery procedures	None	N/A
ADO_IGS.1	Installation, generation, and start-up procedures	AGD_ADM.1	Yes
ADV_FSP.1	Informal functional specification	ADV_RCR.1	Yes
ADV_HLD.1	Descriptive high-level design	ADV_FSP.1, ADV_RCR.1	Yes
ADV_RCR.1	Informal correspondence demonstration	None	N/A
AGD_ADM.1	Administrator guidance	ADV_FSP.1	Yes

Table 34 EAL2 SAR Dependencies (continued)

Assurance Component ID	Assurance Component Name	Dependencies	Satisfied
AGD_USR.1	User guidance	ADV_FSP.1	Yes
ALC_FLR.2	Flaw reporting procedures	None	N/A
ATE_COV.1	Evidence of coverage	ADV_FSP.1, ATE_FUN.1	Yes
ATE_FUN.1	Functional testing	None	Yes
ATE_IND.2	Independent testing-sample	ADV_FSP.1, AGD_ADM.1, AGD_USR.1, ATE_FUN.1	Yes
AVA_SOF.1	Strength of TOE security function evaluation	ADV_FSP.1, ADV_HLD.1	Yes
AVA_MSU.1	Examination of guidance	AGD_ADM.1, AGD_USR.1, ADO_IGS.1, ADV_FSP.1	Yes
AVA_VLA.1	Developer vulnerability analysis	ADV_FSP.1, ATE_HLD.1 AGD_ADM.1, AGD_USR.1	Yes

Obtaining Documentation, Obtaining Support, and 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