Motorola WS5100 Wireless Switch and RFS7000 RF Switch

Security Target

Version 1.5

TABLE OF CONTENTS

SECTION PAGE

Table of Tables

Table **Page**

Document History

Revision	Date	Comment
1.0	3/5/2007	Initial Revision
1.1	4/11/2007	Minor improvements
1.2	9/10/2007	Addressed observation reports
1.3	2/5/2008	Addressed validator comments
1.4	04/14/2009	Minor corrections
1.5	05/20/09	Minor improvement

1 Introduction to the Security Target

1.1 Security Target Identification

TOE Identification:

This Security Target describes two TOEs:

Motorola WS5100 Wireless Switch
Hardware Version: WS5100
Software Version: WS5100-3.0.0.0-022GR

Motorola RFS7000 RF Switch
Hardware Version: RFS7000
Software Version: RFS7000-1.0.0.0-022GR

Document Title: Motorola WS5100 Wireless Switch and RFS7000 RF Switch Security Target, Document Version 1.5, May 20, 2009
CC Version: Common Criteria Version 2.3
Assurance Level: EAL4 augmented with ALC_FLR.2
Strength of Function: SOF-basic
Protection Profile: US Government Wireless Local Area Network (WLAN) Access System Protection Profile for Basic Robustness Environments, Version 1.0, April 2006.

1.2 Security Target Overview

This Security Target (ST) describes Motorola WS5100 Wireless Switch and RFS7000 RF Switch devices. A wireless switch is a hardware device used to control operation of multiple wireless access points and to provide secure Wireless Local Area Network (WLAN) connectivity to a set of wireless client devices.

1.3 Common Criteria Conformance

CC Part 2 extended, Part 3 conformant, and meets the requirements of Evaluation Assurance Level (EAL) 4 from the Common Criteria Version 2.3 augmented with ALC.FLR.2 (Flaw Remediation).

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

1.4 Conventions

The notation, formatting, and conventions used in this ST are consistent with version 2.3 of the Common Criteria (CC).

The CC allows several operations to be performed on functional requirements; refinement, selection, assignment, and iteration are defined in paragraph 2.1.4 of Part 2 of the CC. Each of these operations is used in this ST.

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**. Deleted words are denoted by ~~strike-through text.~~

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *italicized text*.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignment is indicated by showing the value in square brackets, [Assignment_value].

The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing the iteration number in parenthesis following the component identifier, (iteration_number).

The CC paradigm also allows protection profile (PP) and security target authors to create their own requirements. Such requirements are termed 'explicit requirements' and are permitted if the CC does not offer suitable requirements to meet the authors' needs. Explicit requirements must be identified and are required to use the CC class/family/component model in articulating the requirements. In this ST, explicit requirements will be indicated with the "EXP" following the component name.

Application Notes are provided to help the developer, either to clarify the intent of a requirement, identify implementation choices, or to define "pass-fail" criteria for a requirement. For those components where Application Notes are appropriate, the Application Notes will follow the requirement component.

Assumptions: TOE security environment assumptions are given names beginning with "A."-- e.g., A.ADMINISTRATION.

Threats: TOE security environment threats are given names beginning with "T."-- e.g., T.SIGNAL_DETECT.

Policies: TOE security environment policies are given names beginning with "P."—e.g., P.GUIDANCE.

Objectives: Security objectives for the TOE and the TOE environment are given names beginning with "O." and "OE.", respectively,—e.g., O.ACCESS and OE.ADMIN.

2 TOE Description

2.1 Overview

This Security Target describes two TOEs which have the same security functionality, but different performance and hardware characteristics.

Motorola WS5100 Wireless Switch is a rack-mounted hardware device with 1U chassis. It supports up to 48 wireless access points. The device includes two Gigabit Ethernet ports, which provide network connectivity. An RS232 Serial port is used for local administration.

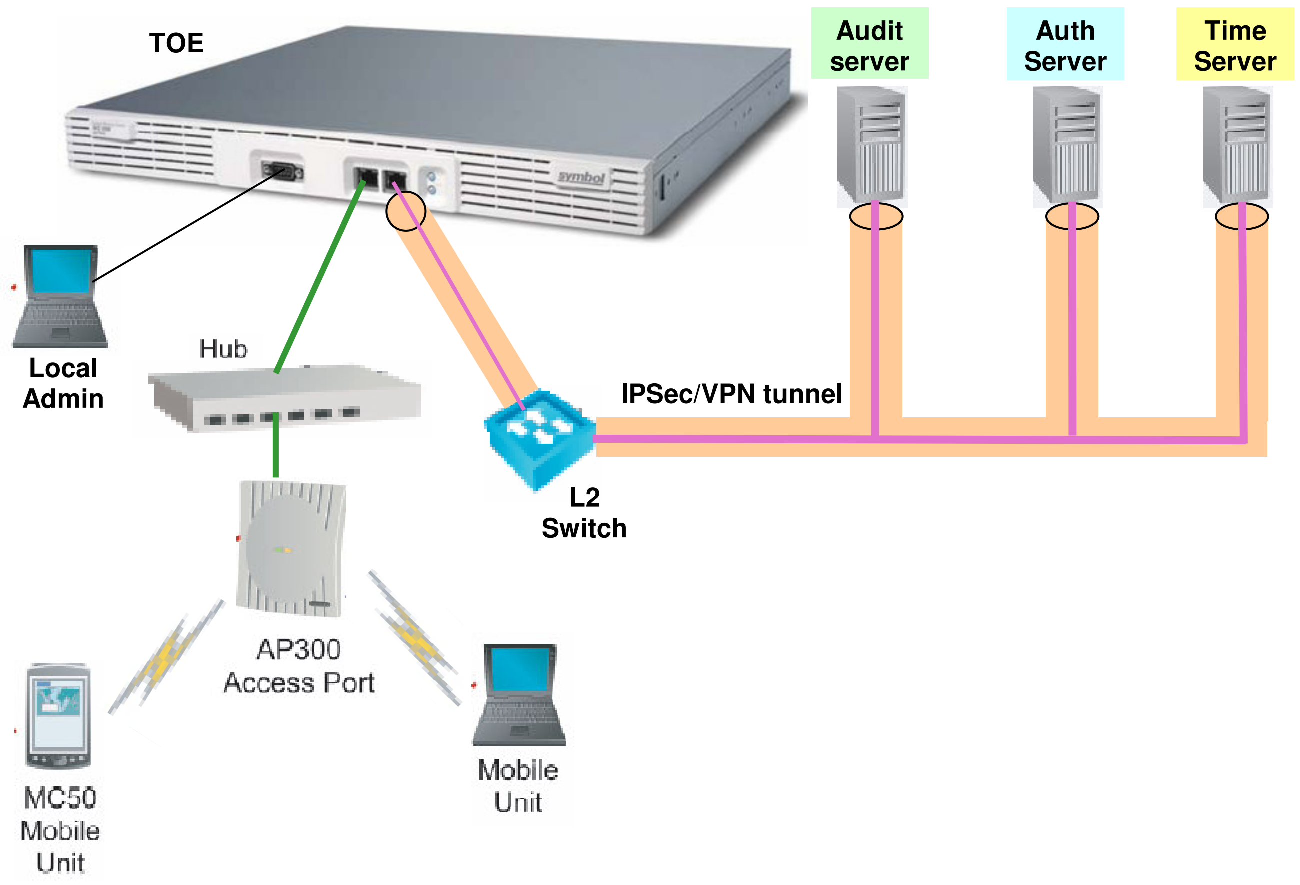
Figure 1. Motorola WS5100 Wireless Switch

Motorola RFS7000 RF Switch is a rack-mounted hardware device with 1U chassis. It supports up to 256 wireless access points. The device includes 8 Gigabit Ethernet ports and one 100Mbit Ethernet port, which provide network connectivity. An RJ45 Serial port is used for local administration. One CompactFlash card slot, two USB ports, and the 100Mbit Ethernet port are not used and are covered by a tamper evident label at the factory.

Figure 2. Motorola RFS7000 RF Switch

In the following, both devices are referred to as “the TOE”.

Figure 3. Typical TOE deployment diagram



The TOE is a device used to control operation of multiple wireless access points and to provide secure Wireless Local Area Network (WLAN) connectivity to a set of wireless client devices. The TOE is installed at a wired network location, and is logically connected to a set of wireless access point devices over a wired Ethernet network. Wireless access point devices are hardware radio devices, which do not provide security functionalities and are used to tunnel wireless network traffic between the TOE and wireless client devices.

The TOE protects data exchanged with wireless client devices using IEEE 802.11i wireless security protocol, which provides data authentication and encryption using the AES-CCM cryptographic algorithm. The TOE uses FIPS 140-2 compliant cryptographic implementations for all cryptographic purposes and is operated in the FIPS 140-2 approved mode of operation.

Wireless users are required to authenticate before access to the wired network is granted by the TOE. The authentication is based on IEEE 802.1X EAP-TLS, EAP-TTLS and PEAP authentication protocols. The TOE acts as the 802.1X authenticator and utilizes services of an external RADIUS authentication server to provide wireless user authentication. During the authentication phase the TOE serves as an intermediary passing authentication messages between the wireless client device and the external authentication server. If the authentication is successful, the authentication server passes to the TOE 802.11i session keys used to establish a 802.11i secure connection between the TOE and the wireless client device. Once the connection is established, the wireless client device may access the protected wired network utilizing the TOE as a gateway. The network connection between the TOE and the external authentication server is protected using the IPSec/IKE security protocol. EAP-TLS authentication protocol uses a client certificate for wireless user authentication, EAP-TTLS and PEAP protocols use password-based authentication.

The TOE provides remote management capabilities using SSH security protocol, as well as local management capabilities via a local serial port connection. The TOE administrators are required to authenticate using a username/password combination. The TOE provides an option to authenticate administrators against an internal administrator database, or against the external authentication server, however only internal administrator database is used in the evaluated configuration.

The TOE provides capabilities to terminate idle wireless user and administrator sessions after the inactivity time limit has been reached, as well as disable a remote administrator account after a pre-defined number of failed authentication attempts had been reached. The account can then be re-enabled using a local serial port administration session.

The TOE provides auditing capabilities which utilize services of an external syslog audit server. The network connection between the TOE and the external audit server is secured using IPSec/IKE security protocol.

The TOE utilizes services of an external Network Time Protocol (NTP) server to obtain reliable time stamps used in audit records. The network connection between the TOE and the external NTP server is secured using IPSec/IKE security protocol.

The TOE provides capabilities to run a set of self-tests on power-on and on demand to verify the integrity and critical functions of the TOE. The security of network data is maintained by zeroizing the memory location corresponding to a network packet, after the packet has been processed by the TOE.

2.2 TOE Hardware

The TOE is a standalone rack-mounted hardware device, which includes a set of general-purpose and network processors that execute the TOE software, as well as volatile and non-volatile storage components. The physical boundary of the TOE is composed of a metal and hard plastic case and meets the physical security requirements of FIPS 140-2 at Security Level 2. Tamper-evident seals are applied to the TOE enclosure to satisfy the tamper evidence requirements of the FIPS 140-2 standard at Security Level 2.

The TOE physical boundary includes a set of network Ethernet ports used to provide network connectivity, a serial console port used for local administration, a set of status LEDs as well as a power port used to provide a source of external electric power.

2.3 Scope of Evaluation

The identification of the TOE is provided in Section 1.1 “Security Target Identification”. The scope of evaluation is comprised by evaluation of TOE security functions specified in Section 6.1 of this document.

The following wireless security protocols are disabled in the FIPS 140-2 mode of operation and are not included in this evaluation: WEP, WPA, TKIP.

The following TOE features are not included in the evaluation: intrusion detection, protection against denial-of-service attacks, roaming of mobile clients across distributed networks, stateful packet analysis, network address translation, 802.11 traffic prioritization and precedence, Wi-Fi multimedia extensions.

2.4 IT Environment

As described in Section 2.1 the TOE uses services of an external RADIUS authentication server for user authentication. The authentication server supports EAP-TLS, EAP-TTLS and PEAP authentication protocols.

Reliable time stamps are provided by an external Network Time Protocol (NTP) server.

Audit records generated by the TOE are transmitted to the external syslog audit server. The audit server provides protected storage for audit records, as well as a capability to view and search audit records.

Network connections between the TOE and external authentication, audit and time servers are protected by a trusted channel, as required by the WLANAS PP. The IPSec/IKE security protocol is used to establish secure network connections for the trusted channel.

3 TOE Security Environment

This section describes the assumptions, threats, and policies that are relevant to both the TOE and the TOE environment.

3.1 Secure Usage Assumptions

Assumptions are limiting conditions that are accepted before developing policy or considering threats. Table 3-1 TOE Assumptions identifies the conditions that are assumed to exist in the operational environment. The TOE Assumptions are identical to those of WLANAS PP.

Table 3-1 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.

3.2 Threats to Security

Threats are actions that may have an adverse affect on the TOE. Exposure of wireless communications in the RF transmission environment introduces unique threats for the WLAN. The WLAN interconnected to a wired network could effectively create a hole in the wired infrastructure boundary because it exposes information to the RF medium where signals can be more readily detected and intercepted. With WLANs, an adversary no longer requires physical access to the network to exploit a wireless system. For basic robustness, the threats identified do not include those that would be considered a sophisticated attack (e.g., intentional jamming, traffic analysis)

The TOE must counter the following threats to security. The threats to security are identical to those of WLANAS PP.

Table 3-2 Threats

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

T.UNAUTH_ADMIN_ACCESS	An unauthorized user or process may gain access to an administrative account.

3.3 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. Table 3-3 Organizational Security Policies identifies the organizational security policies applicable to the TOE. The policies are identical to those of WLANAS PP.

Table 3-3 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_NETWORKS	In accordance with the DOD Wireless Policy, there will be no ad hoc 802.11 or 802.15 networks allowed.

4 Security Objectives

4.1 Security Objectives for the TOE

Table 4-1 Security Objectives for TOE identifies the security objectives of the TOE. These security objectives reflect the stated intent to counter identified threats and/or comply with any organizational security policies identified. The table also shows the corresponding threats and policies that are addressed by the objectives. An explanation of the relationship between the objectives and the threats/policies is provided in the rationale section of this document. The Security Objectives for the TOE are identical to those of WLANAS PP.

Table 4-1 Security Objectives for TOE

Name	TOE Security Objective
O.AUDIT_GENERATION	The TOE will provide the capability to detect and create records of security-relevant events associated with users.
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 140-1/2 validated crypto modules 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.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.

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.ADMIN_GUIDANCE	The TOE will provide administrators with the necessary information for secure management.
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.DOCUMENTED_ DESIGN	The design of the TOE is adequately and accurately documented.
O.PARTIAL_ FUNCTIONAL_TESTING	The TOE will undergo some security functional testing that demonstrates the TSF satisfies some of its security functional requirements.
O.VULNERABILITY_ ANALYSIS	The TOE will undergo some vulnerability analysis demonstrate the design and implementation of the TOE does not contain any obvious flaws.

4.2 Security Objectives for the Environment

The assumptions identified in Section 3.1 are incorporated as security objectives for the environment and listed below. They levy additional requirements on the environment, which are largely satisfied through procedural or administrative measures. Table 4-2 Security Objectives for the IT and Non IT Environment identifies the security objectives for the TOE IT and Non environment. The objectives are identical to those of WLANAS PP.

Table 4-2 Security Objectives for the IT and Non IT Environment

Name	Security Objective

OE.AUDIT_PROTECTION	The IT Environment will provide the capability to protect audit information and the authentication credentials.
OE.AUDIT_REVIEW	The IT Environment will provide the capability to selectively view audit information.
OE.MANAGE	The TOE IT environment will augment the TOE functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
OE.NO_EVIL	Sites using the TOE shall ensure that administrators are non-hostile, appropriately trained and follow all administrator guidance.
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the TOE.
OE.PHYSICAL	The environment provides physical security commensurate with the value of the TOE and the data it contains.
OE.PROTECT_MGMT_COMMS	The 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 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 environment will provide mechanisms that support the TOE in providing a 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.

5 IT Security Requirements

This section provides functional and assurance requirements that must be satisfied by the TOE and the IT environment.

5.1 Strength of Function Claims

The statement of the TOE security requirements must include a minimum strength level for the TOE security functions realized by a probabilistic or permutational mechanism, except for cryptographic functions. For this ST, the overall level will be SoF-basic.

In the event that a probabilistic mechanism, such as a password mechanism for user and/or administrator authentication is used, then the expectation is that for each attempt to use the authentication mechanism, the probability that a random attempt will succeed is less than one in a million. FIA_UAU.1 includes the following probabilistic/permutational mechanisms for which specific SOF metrics are appropriate: password-based authentication.

The strength of function claims in this ST match those of WLANAS PP.

5.2 TOE Security Functional Requirements

The TOE security functional requirements are listed in Table 5-1 Functional Components. The requirement names ending with _EXP correspond to explicitly stated requirements. All other requirements are drawn from CC Part 2.

Table 5-1 Functional Components

Component	Component Name	Dependencies
FAU_GEN.1(1)	Audit data generation	FPT_STM.1
FAU_GEN.2	User identity association	FAU_GEN.1 FIA_UID.1
FAU_SEL.1	Selective audit	FAU_GEN.1; FMT_MTD.1(1)
FCS_BCM_EXP.1	Explicit: baseline cryptographic module	None
FCS_CKM.1	Cryptographic key generation	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4 FMT_MSA.2
FCS_CKM_EXP.2	Cryptographic key establishment	[FTP_ITC.1 or FCS_CKM.1] FMT_MSA.2

FCS_CKM.4	Cryptographic key destruction	FTP_ITC.1 or FCS_CKM.1] FMT_MSA.2
FCS_COP_EXP.1	Explicit: random number generation	[FTP_ITC.1or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2
FCS_COP_EXP.2	Explicit: cryptographic operation	[FTP_ITC.1 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2
FDP_PUD_EXP.1	Protection of user data	None
FDP_RIP.1(1)	Subset residual information protection	None
FIA_AFL.1(1)	Administrator authentication failure handling	FIA_UAU.1
FIA_ATD.1(1)	Administrator attribute definition	None
FIA_UAU.1	Timing of local authentication	FIA_UID.1
FIA_UAU_EXP.5(1)	Multiple authentication mechanisms	None
FIA_UID.2	User identification before any action	None
FIA_USB.1(1)	User-subject binding	FIA_ATD.1(1)
FIA_USB.1(2)	User-subject binding	FIA_ATD.1(1)

FMT_MOF.1(1)	Management of security functions behavior (cryptographic function)	FMT_SMF.1(1)
		FMT_SMR.1(1)

FMT_MOF.1(2)	Management of security functions behavior (audit record generation)	FMT_SMF.1(2)
		FMT_SMR.1(1)

FMT_MOF.1(3)	Management of security functions behavior (authentication)	FMT_SMF.1(3)
		FMT_SMR.1(1)

FMT_MSA.2	Secure security attributes	ADV_SPM.1 [FDP_ACC.1 or FDP_IFC.1] FMT_MSA.1 FMT_SMR.1(1)

FMT_MTD.1(1)	Management of audit data	FMT_SMR.1(1)
		FMT_SMF.1(2)

FMT_MTD.1(2)	Management of authentication data	FMT_SMR.1(1)

	(administrator)	FMT_SMF.1(1)
FMT_SMF.1(1)	Specification of management functions (cryptographic functions)	None
FMT_SMF.1(2)	Specification of management functions (TOE audit record generation)	None
FMT_SMF.1(3)	Specification of management functions (Cryptographic key data)	None
FMT_SMR.1(1)	Security roles	FIA_UID.1
FPT_RVM.1(1)	Non-bypassability of the TOE Security Policy (TSP)	None
FPT_SEP.1(1)	TSF domain separation	None
FPT_STM_EXP.1	Reliable time stamps	None
FPT_TST_EXP.1	TSF testing	FCS_CKM.2, FCS_CKM.4, FCS_COP_EXP.1, FCS_COP_EXP.2
FPT_TST_EXP.2	TSF testing of cryptographic modules	FCS_CKM.2, FCS_CKM.4, FCS_COP_EXP.1, FCS_COP_EXP.2
FTA_SSL.3	TSF-initiated termination	None
FTA_TAB.1	Default TOE access banners	None
FTP_ITC_EXP.1(1)	Inter-TSF trusted channel	None
FTP_TRP.1	Trusted path	None

5.2.1 Security Audit

5.2.1.1 FAU_GEN.1(1) Audit data generation

FAU_GEN.1.1(1) The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;
b) All auditable events for the *minimum* level of audit; and
c) [none].

Table 5-2 TOE Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None	None
FAU_GEN.2	None	None
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_CKM.1	Manual load of a key	The identity of the Administrator performing the function
FCS_CKM_EXP.2	Error(s) detected during cryptographic key transfer	None
FCS_CKM.4	Destruction of a cryptographic key	The identity of the Administrator performing the function
FCS_COP_EXP.1	None	None
FCS_COP_EXP.2	None	None
FDP_PUD.1_EXP	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)	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	None	None

FIA_USB.1(1)
FIA_USB.1(2)
	Unsuccessful binding of user security attributes to a subject	None

FMT_MOF.1(1)	Changing the TOE encryption algorithm including the selection not to encrypt communications	Encryption algorithm selected (or none)
FMT_MOF.1(2)	Start or Stop of audit record generation	None

FMT_MOF.1(3)	Changes to the TOE remote authentication settings; Changes to the threshold of failed authentication attempts; Changes to the session lock timeframe	The identity of the Administrator performing the function.
FMT_MSA.2	All offered and rejected values for security attributes	None
FMT_MTD.1(1)	Changes to the set of rules used to pre-select audit events.	None
FMT_MTD.1(2)	Changing the TOE authentication credentials	None – the TOE SHALL NOT record authentication credentials in the audit log.
FMT_SMR.1(1)	Modifications to the group of users that are part of a role	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.
FTP_ITC_EXP.1(1)	Initiation/Closure of a trusted channel;	Identification of the remote entitywith which the channel was attempted/created; Success of failure of the event
FTP_TRP.1	Initiation of a trusted path	Identification of the remote entity with which the path was attempted/created; Success of failure of the event

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 in FAU_GEN.1.1(1)].

Application Note: Event type is defined as the BSD syslog severity level indicator, in the Terminology section of the WLANAS PP.

5.2.1.2 FAU_GEN.2 User identity association

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

5.2.1.3 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].

Application Note: Event type is defined as the BSD syslog severity level indicator, in the Terminology section of the WLANAS PP.

Application Note: The device interface is the physical interface upon which user (or administrative) data is received/sent (e.g. WLAN interface, wired LAN interface, serial port, administrative LAN interface, etc.).

5.2.1.4 FCS_BCM_EXP.1 Explicit: baseline cryptographic module

FCS_BCM_EXP.1.1 All cryptographic modules shall comply with FIPS 140-1/2 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.

5.2.1.5 FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [ANSI X9.31 PRNG] and specified cryptographic key sizes [112-bit Triple DES, 168-bit Triple DES, 128-bit AES, 196-bit AES, 256-bit AES, 1024-bit RSA] that meet the following*:* [FIPS 140-2 standard].

5.2.1.6 FCS_CKM_EXP.2 Explicit: cryptographic key establishment

FCS_CKM_EXP.2.1 The TSF shall provide the following cryptographic key establishment technique: Cryptographic Key Establishment using Manual Loading. The cryptomodule shall be able to accept as input and be able to output keys in the following circumstances [upon issuance of the key input/output command by the administrator] 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.

5.2.1.7 FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a ~~specified key destruction method~~ [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 with an alternating pattern.

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 times with an alternating pattern upon the transfer of the key/CSPs to another location.]

Application Note: Item (d) applies to locations that are used when the keys/parameters are copied during processing, and not to the locations that are used for storage of the keys, which are specified in items (b) and (c). The temporary locations could include memory registers, physical memory locations, and even page files and memory dumps. Configuring the key data may include: setting key lifetimes, setting key length, etc.

5.2.1.8 FCS_COP_EXP.1 Explicit: random number generation

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 cryptomodule running in a FIPS-approved mode.

Application Note: Whenever a referenced standard calls for a random number generation capability, this requirement specifies the subset of random number generators (those that are FIPS-validated) that are acceptable. Although the RNG is required to be implemented in a FIPS cryptomodule, it is not required that it be implemented in the cryptomodule that is performing the cryptographic operations that satisfy FCS_COP_EXP.2. Also note that this requirement is not calling for the RNG functionality to be made generally available (e.g., to untrusted users via an API).

5.2.1.9 FCS_COP_EXP.2(1) Explicit: cryptographic operation

FCS_COP_EXP.2.1(1) A cryptomodule shall perform encryption and decryption using the FIPS-140-1/2 Approved *AES* algorithm and operating in [CCM mode, CBC mode] and supporting FIPS approved key sizes of [128 bits, 196 bits, 256 bits].

5.2.1.10 FCS_COP_EXP.2(2) Explicit: cryptographic operation

FCS_COP_EXP.2.1(2) A cryptomodule shall perform encryption and decryption using the FIPS-140-1/2 Approved *Triple DES* algorithm and operating in [CBC mode] and supporting FIPS approved key sizes of [112 bits, 168 bits].

5.2.1.11 FDP_PUD_EXP.1 Protection of user data

FDP_PUD_EXP.1.1 When the 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 **utilizing 802.11i wireless security protocol**;

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 **utilizing 802.11i wireless security protocol**.

Application Note: This requirement allows the TOE administrator to require that all user data transmitted on the WLAN be encrypted using the cryptographic algorithms specified by FCS_COP.

5.2.1.12 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 *deallocation of the resource from* the following objects: [network packet objects].

Application Note: This requirement ensures that the TOE does not allow data from a previously transmitted packet to be inserted into unused areas or padding in the current packet.

5.2.1.13 FIA_AFL.1(1) Administrator authentication failure handling

FIA_AFL.1.1(1) The TSF shall detect when *an administrator configurable positive integer within the range of [1 to 1024]* **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 Administrator].

Application Note: This requirement applies to remote administrator login and does not apply to the local login of the TOE, since it does not make sense to lock a local administrator's account in this fashion. For the purpose of the WLANAS PP, remote administrator refers to administrators that do not have either Serial cable or local console access to the TOE.

Application Note: This requirement does NOT require that the TOE allow remote administration. However, if the TOE does allow administrators to login to the TOE remotely (e.g. from the wired interface or a management network) then it must provide a mechanism to prevent brute force attacks on the administrative account.

5.2.1.14 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, [no additional attributes]].

5.2.1.15 FIA_UAU.1 Timing of local authentication

FIA_UAU.1.1 The TSF shall allow [identification as provided in FIA_UID.2] on behalf of ~~the user~~ **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.

5.2.1.16 FIA_UAU_EXP.5(1) Explicit: multiple authentication mechanisms

FIA_UAU_EXP.5.1(1) The TSF shall provide local **password-based** authentication **of administrators**, and a remote authentication mechanism to perform user authentication.

FIA_UAU_EXP.5.2(1) The TSF shall, at the option of the administrator, invoke the remote **password-based** authentication mechanism for administrators and **the remote EAP-TLS, EAP-TTLS, or PEAP-based authentication mechanism for** wireless LAN users.

Application Note: This explicit requirement is needed for local administrators because there is disagreement over whether existing CC requirements specifically require the TSF provide authentication. That the TOE provide authentication is implied by other FIA_UAU requirements, and 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 ST, an explicit requirement for authentication has been included. This ST mandates that the TOE provide the client to facilitate remote authentication via an authentication server. The IT environment will provide the authentication server, and 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.

Since FIA_UAU.5.1(1) and 5.2(1) require that the TSF provide authentication mechanisms, this explicit requirement is needed with respect to the remote users to specify that the TSF invoke a remote authentication mechanism rather than provide it.

5.2.1.17 FIA_UID.2 User identification before any action

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

Application Note: This requirement does not refer to management and control packets that must be allowed to pass between the WLAN client and the access system before authentication. It is assumed that this information is not user specific and therefore not covered by this requirement.

Application Note: It is also important to note that the identification credential presented to the authentication server (e.g. a user name) will be related to but not necessarily the same as the identification credential (e.g. MAC address of a remote system) that is used to enforce FDP_PUD_EXP.

5.2.1.18 FIA_USB.1(1) User-subject binding.

FIA_USB.1.1(1) The TSF shall associate the following **wireless** user security attributes with subjects acting on the behalf of that user: [username].

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 identification and authentication the username shall be that of the user that has authenticated successfully].

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: [no changes shall be allowed].

5.2.1.19 FIA_USB.1(2) User-subject binding.

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

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: [upon successful identification and authentication the username shall be that of the user that has authenticated successfully].

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: [no changes shall be allowed].

5.2.1.20 FMT_MOF.1(1) Management of cryptographic security functions behavior

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

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

to [administrators].

5.2.1.21 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 [administrators].

5.2.1.22 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 [administrators].

5.2.1.23 FMT_MSA.2 Secure security attributes

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

5.2.1.24 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 administrator].

5.2.1.25 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] to [administrators].

5.2.1.26 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: [configure administrator authentication, query and set the encryption/decryption of network packets (via FCS_COP_EXP.2) in conformance with the administrators configuration of the TOE].

Application Note: This requirement ensures that those responsible for TOE administration are able to select an encryption algorithm identified in FCS_COP_EXP.2 or no encryption for encrypting/decrypting data transmitted by the WLAN device.

5.2.1.27 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].

Application Note: This requirement ensures that those responsible for TOE administration are able to start or stop the TOE generation of audit records

5.2.1.28 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].

Application Note: The intent of this requirement is to provide the ability to configure the TOE's cryptographic key(s). Configuring the key data may include: setting key lifetimes, setting key length, etc.

5.2.1.29 FMT_SMR.1(1) Security roles

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

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

Application Note: The only user allowed direct access to the TOE is the administrator. Wireless users can pass data through the TOE but do not have direct access. A role of wireless user is included in the TOE, but the scope of that role should be defined only to the extent necessary to support the activities of wireless users passing data through the TOE.

This ST also assumes that the TOE will contain a local authentication mechanism and the capability to use a remote authentication server. Although users are sometimes referred to as local or remote, these references do not imply a role.

5.2.1.30 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.

5.2.1.31 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.

5.2.1.32 FPT_STM_EXP.1 Reliable time stamps

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.

Application Note: The TOE must be capable of obtaining a time stamp via an NTP server.

5.2.1.33 FPT_TST_EXP.1 TSF testing

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, [*temporary files, page files, configuration files, core dumps, data stored in volatile memory*].

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.

5.2.1.34 FPT_TST_EXP.2 TSF testing of cryptographic modules

FPT_TST_EXP.2.1 The TSF shall run the suite of self-tests provided by the FIPS 140-1/2 cryptomodule 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 cryptomodule immediately after the generation of a key.

Application Note: In 2.2 it is required that there be specific functionality IF the TOE generates cryptographic keys. This requirement does not require the TOE to generate keys.

5.2.1.35 FTA_SSL.3 TSF-initiated termination

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

Application Note: This requirement applies to both local administrative sessions and wireless users that pass data through the TOE.

5.2.1.36 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.

5.2.1.37 FTP_ITC_EXP.1(1) Inter-TSF trusted channel

FTP_ITC_EXP.1.1(1) The **TOE** shall provide **an IPSec/IKE encrypted** communication channel between itself **and entities in the 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, *none*].

5.2.1.38 FTP_TRP.1 Trusted path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and ***wireless*** users 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 authentication***, [*none*].

Application Note: This requirement ensures that the initial exchange of authentication information between the wireless client and the access system is protected.

5.3 Security Requirements for the IT Environment.

This ST includes functional requirements for the IT Environment. The IT environment includes an authentication server, a time server and an audit 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 the audit data.

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

It is expected that the 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 IT Environment security functional requirements are listed in Table 5-3 Functional Components.

Table 5-3 Functional Components

Component	Component Name	Dependencies
FAU_GEN.1(2)	Audit data generation	FPT_STM.1
FAU_SAR.1	Audit review	FAU_GEN.1
FAU_SAR.2	Restricted audit review	FAU_SAR.1
FAU_SAR.3	Selectable audit review	FAU_SAR.1
FAU_STG.1	Protected audit trail storage	FAU_GEN.1
FAU_STG.3	Action in case of possible audit data loss	FAU_STG.1

FDP_RIP.1(2)	Subset residual information protection	None
FIA_AFL.1(2)	Remote user authentication failure handling	FIA_UAU.1
FIA_ATD.1(2)	User attribute definition	None
FIA_UAU_EXP.5(2)	Remote authentication mechanisms	FIA_UID.1
FIA_UID.1	Timing of identification	None
FMT_MOF.1(4)	Management of security functions Behavior	FMT_SMF.1(1)(2)(3) FMT_SMR.1

FMT_MTD.1(3)	Management of identification data (user)	FMT_SMF.1(4)
		FMT_SMR.1(2)

FMT_MTD.1(4)	Management of authentication data (user)	FMT_SMF.1(4)
		FMT_SMR.1(2)

FMT_MTD.1(5)	Management of time data	FMT_SMF.1(5)
		FMT_SMR.1(2)

FMT_SMR.1(2)	Security roles	FIA_UID.1
FMT_SMF.1(4)	Specification of management functions (user identification and authentication)	None
FMT_SMF.1(5)	Specification of management functions (time stamps)	None
FTP_ITC_EXP.1(2)	Inter-TSF trusted channel	None
FPT_RVM.1(2)	Non-bypassability of the TOE Security Policy (TSP)	None
FPT_SEP.1(2)	TSF domain separation	None
FPT_STM.1	Reliable time stamps	None

5.3.1.1 FAU_GEN.1(2) Audit data generation

FAU_GEN.1.1(2) The **TOE IT Environment** shall be able to generate an audit record of the following auditable events:

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

b. All auditable events for the [*minimum*] level of audit; and

c. [none].

Table 5-4 TOE IT Environment Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1(2)	None	None
FAU_SAR.1	None	None
FAU_SAR.2	Unsuccessful attempt to read the audit records	The identity of the user attempting to perform the function
FAU_SAR.3	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(2)	None	None
FIA_UAU_EXP.5(2)	Use of the authentication mechanism (success or failure)	User identity - the TOE **SHALL NOT** record invalid passwords the audit log.
FIA_UID.1	None	None
FMT_MOF.1(4)	Changes to audit server settings Changes to authentication server settings Changes to time server settings	None

FMT_MTD.1(3)
FMT_MTD.1(4)
	Changing the authentication credentials	None – the IT environment SHALL NOT record authentication credentials in the audit log.

FMT_MTD.1(5)	Changes to the time data	None
FMT_SMR.1(2)	None	None
FTP_ITC_EXP.1(2)	Initiation/Closure of a trusted channel;	Identification of the 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, 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 in FAU_GEN.1.1(2)].

Application Note: Event type is defined as the BSD syslog severity level indicator in the Terminology section of the WLANAS PP.

5.3.1.2 FAU_SAR.1 Audit review

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

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

Application Note: This requirement ensures that the TOE IT environment provides the administrator with functionality necessary for the administrator to review the audit records generated by the TOE.

5.3.1.3 FAU_SAR.2 Restricted audit review

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

Application Note: This requirement ensures that access to audit records generated by the TOE is limited to those authorized to view the information.

5.3.1.4 FAU_SAR.3 Selectable audit review

FAU_SAR.3.1 The **TOE IT environment** ~~TSF~~ shall provide the ability to perform *searches* of audit data based on [event type, date, time and/or [no additional criteria]].

5.3.1.5 FAU_STG.1 Protected audit trail storage

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

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

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

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

5.3.1.7 FDP_RIP.1(2) Subset residual information protection

FDP_RIP.1.1(2) The **TOE IT Environment** ~~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]

Application Note: This requirement ensures that the TOE environment does not allow data from a previously transmitted packet to be inserted into unused areas or padding in the current packet. Since operations on requirement for the IT environment must be completed, the selection "allocation of resources to" has been made because it is encompassing of the two options (e.g. a system that make the information contents of resource unavailable when the resource is freed can also claim to meet the requirement that the content of the resource be freed prior to reallocation).

5.3.1.8 FIA_AFL.1(2) Remote user authentication failure handling

FIA_AFL.1.1(2) The **TOE IT Environment** ~~TSF~~ shall detect when *an administrator configurable positive integer within [1 to 1024]* **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].

Application Note: This requirement ensures that the TOE IT Environment has the capability to detect multiple authentication attempts and take action to disable subsequent authentication attempts.

5.3.1.9 FIA_ATD.1(2) User attribute definition

FIA_ATD.1.1(2) The **TOE IT Environment** ~~TSF~~ shall maintain the following **minimum** list of security attributes belonging to individual **remotely authenticated** users: [password for users authenticating using EAP-TTLS and PEAP authentication protocols].

5.3.1.10 FIA_UAU_EXP.5(2) Remote authentication mechanisms

FIA_UAU_EXP.5.1(2) The **TOE IT Environment** ~~TSF~~ shall provide [a remote authentication mechanism] **to provide TOE remote** user authentication.

FIA_UAU_EXP.5.2(2) The **TOE IT Environment** ~~TSF~~ shall authenticate any user's claimed identity according to the [EAP-TLS, EAP-TTLS, or PEAP authentication protocols].

5.3.1.11 FIA_UID.1 Timing of identification

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

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

Application Note: This requirement does not refer to management and control packets that must be allowed to pass between the wlan client and the access system before authentication. It is assumed that this information is not user specific and therefore not covered by this requirement.

5.3.1.12 FMT_SMF.1(4) Specification of management functions (user identification and authentication)

FMT_SMF.1.1(1) The **TOE IT environment** ~~TSF~~ shall be capable of performing the following security management functions: [configure user identification and authentication].

5.3.1.13 FMT_SMF.1(5) Specification of management functions (time stamps)

FMT_SMF.1.1(2) The **TOE IT environment** ~~TSF~~ shall be capable of performing the following security management functions: [configure time stamps].

5.3.1.14 FMT_MOF.1(4) Management of security functions behavior

FMT_MOF.1.1(4) The **TOE IT environment** ~~TSF~~ shall restrict the ability to *determine the behavior of* the functions: [

- Audit,
- Remote Authentication
- Time service]

to [the administrator].

Application Note: The TOE IT environment must be managed in conjunction with the TOE.

5.3.1.15 FMT_MTD.1(3) Management of identification data (user)

FMT_MTD.1.1(3) The **TOE IT environment** ~~TSF~~ shall restrict the ability to *query, modify, delete, clear*, [create] the [user identification credentials] to [administrators].

5.3.1.16 FMT_MTD.1(4) Management of authentication data (user)

FMT_MTD.1.1(4) The **TOE IT environment** ~~TSF~~ shall restrict the ability to *modify* the [user authentication credentials] to [administrators].

5.3.1.17 FMT_MTD.1(5) Management of time data

FMT_MTD.1.1(5) The **TOE IT environment** shall restrict the ability to [set] the [time and date used to form the time stamps in FPT_STM.1] to [the Security Administrator or authorized IT entity].

5.3.1.18 FMT_SMR.1(2) Security roles

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

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

Application Note: The TOE IT environment must include an administrative role for its own management.

5.3.1.19 FTP_ITC_EXP.1(2) Inter-TSF trusted channel

FTP_ITC_EXP.1.1(2) The **TOE IT environment** ~~TSF~~ shall provide **an IPSec/IKE 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** ~~TSF~~ 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** ~~TSF~~ shall initiate communication via the trusted channel for [all authentication functions, remote logging, time, *none*].

Application Note: For FTP_ITC_EXP.1.1(2) it is expected that the environment be able to provide and encrypted channel between the environment and the TOE. This is to provide for communications between itself and the TOE, as end points, to protect the communications between the TOE and the IT environment.

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

FPT_RVM.1.1(2) The **TOE IT Environment** ~~TSF~~ shall ensure that **IT environment** ~~TSP~~ enforcement functions are invoked and succeed before each function within the **IT environmental scope of control** ~~TSC~~ is allowed to proceed.

5.3.1.21 FPT_SEP.1(2) TSF domain separation

FPT_SEP.1.1(2) The **TOE IT Environment** ~~TSF~~ 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** ~~TSF~~ shall enforce separation between the security domains of subjects in the **IT environmental scope of control**.

5.3.1.22 FPT_STM.1 Reliable time stamps

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

Application Note: The TOE IT environment must provide reliable time stamps (for example: an NTP server). It is also acceptable for the TOE to satisfy this requirement by providing its own time stamp.

5.4 TOE Security Assurance Requirements

The Security Assurance Requirements for the TOE are the assurance components of Evaluation Assurance Level 4 (EAL4) augmented with ALC_FLR.2 (Flaw Remediation). The components are taken from Part 3 of the Common Criteria. None of the assurance components are refined. The assurance components are listed in Table 5-5 Assurance Components below. The components meet or exceed the requirements of WLANAS PP.

Table 5-5 Assurance Components

Assurance class	Assurance components
Configuration management	ACM_AUT.1 Partial CM automation
	ACM_CAP.4 Generation support and acceptance procedures
	ACM_SCP.2 Problem tracking CM coverage
Delivery and operation	ADO_DEL.2 Detection of modification
	ADO_IGS.1 Installation, generation, and start-up procedures
Development	ADV_FSP.2 Fully defined external interfaces
	ADV_HLD.2 Security enforcing high-level design
	ADV_IMP.1 Subset of the implementation of the TSF
	ADV_LLD.1 Descriptive low-level design
	ADV_RCR.1 Informal correspondence demonstration
	ADV_SPM.1 Informal TOE security policy model
Guidance documents	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
Life cycle support	ALC_DVS.1 Identification of security measures
	ALC_FLR.2 Flaw remediation
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: high-level design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
Vulnerability assessment	AVA_MSU.2 Validation of analysis

	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.2 Independent vulnerability analysis

6 TOE Summary Specification

This chapter describes the security functions and associated assurance measures.

6.1 TOE Security Functions

The following security functions are implemented by the TOE

a) Security Audit

b) Cryptographic Support

c) User Data Protection

d) Identification and Authentication

e) Security Management

f) Protection of the TSF

g) TOE Access

h) Trusted Path/Channels

6.1.1 Security Audit

The Security Audit function includes generation of audit events for startup/shutdown of audit functions, modifications to the audit configuration, manual load of a key, cryptographic key transfer errors, cryptographic key destruction, enabling/disabling wireless encryption, reaching of the unsuccessful authentication attempts threshold and re-enabling the user, user authentication attempts, authentication server failures, configuration of security functions, execution of self tests, initiation/closure of a trusted channel, and initiation of a trusted path. The specific events are listed as a part of FAU_GEN.1(1) definition. Audit events include at least date and time of the event, type of event, subject identify (if applicable), and outcome (success or failure) of the event. For some events additional information is included, as specified in FAU_GEN.1(1). For each identified user, the username is included in the audit event record. The TOE provides an ability to include/exclude events based on username, threshold syslog level, device interface and wireless client MAC address.

The following syslog levels are supported:

Syslog level	Description
LOG_EMERG	An emergency condition. The system is unusable
LOG_ALERT	This message warrants an immediate action
LOG_CRIT	Critical Condition
LOG_ERR	Error
LOG_WARNING	Warning
LOG_NOTICE	Normal but a significant condition
LOG_INFO	Information only
LOG_DEBUG	This message appears only during debug mode

The audit events records are transmitted to the external audit server over a secure IPSec/IKE connection.

Reliable time stamps are used for audit records.

6.1.2 Cryptographic Support

The TOE utilizes cryptographic functions for the purposes of wireless data protection using 802.11i protocol, for SSH trusted path used for the TOE administration, as well as for IPSec/IKE trusted channel established between the TOE and external authentication, audit and time servers.

The cryptographic module implemented by the TOE complies with FIPS 140-2 requirements at Security Level 2. The module implements cryptographic algorithms as specified in FCS_CKM.1, FCS_COP_EXP.2(1), and FCS_COP_EXP.2(2). A key zeroization function implemented by the module zeroizes all cryptographic keys and critical security parameters by overwriting the storage area three times with an alternating pattern. All intermediate storage areas for cryptographic keys and critical security parameters are zeroized upon the transfer of the key or CSP to another location. The module implements an administrator command to manually input/output cryptographic keys, including the IPSec/IKE pre-shared keys and RADIUS authentication key.

The module employs ANSI X9.31 FIPS 140-2 approved random number generator for key generation purposes.

6.1.3 User Data Protection

The TOE implements a capability to protect authenticated user data exchanged with a wireless client using 802.11i wireless security protocol, which utilizes AES-CCM encryption with 128-bit keys. The keys are dynamically established by the external authentication server during EAP-TLS, EAP-TTLS or PEAP authentication phase, and then transferred from the authentication server to the TOE over a protected IPSec/IKE channel.

The memory locations corresponding to 802.11i and IP network packets processed by the TOE are zeroized when the packet is processed.

6.1.4 Identification and Authentication

The TOE keeps a local database of administrator usernames and passwords and utilizes password-based authentication to authenticate administrators connecting remotely using SSH protocol, or locally using a serial console connection. The TOE also provides a capability to authenticate administrator against an external RADIUS authentication server, however only internal administrator database is used in the evaluated configuration. When a pre-defined number of unsuccessful authentication attempts for a remote administrator has been reached, the administrator user is disabled until re-enabled using a local console connection.

The TOE authenticates wireless users utilizing an external RADIUS authentication server, which implements EAP-TLS, EAP-TTLS and PEAP protocols. The trusted channel between the TOE and the external authentication server is protected using IPSec/IKE security protocol with pre-shared keys. EAP-TLS uses a client certificate for user authentication, the username is embedded in the certificate. EAP-TTLS and PEAP use a password for user authentication.

No services are provided by the TOE until the user is successfully identified and authenticated.

6.1.5 Security Management

The TOE provides remote management using SSH protocol, as well as local management utilizing a serial console connection.

The management interfaces provide capabilities to add, view and remove IPSec/IKE and RADIUS cryptographic keys and key lifetime, create/delete administrator users and set administrator passwords, set maximum number of unsuccessful administrator authentication attempts, re-enable administrators, set maximum session idle time for administrators and wireless users, enable/disable wireless encryption, enable/disable the use of an authentication server, set IP addresses of remote authentication, audit and time servers, execute self-tests, set cryptographic algorithms used by IPSec/IKE, zeroize cryptographic keys and CSPs, start and stop audit functions, execute self-tests, select events which trigger an audit record, enable/disable verification of cryptographic key testing, as well as view the corresponding settings.

All management functions require assumption of the administrator role upon successful authentication of the administrator.

6.1.6 Protection of the TSF

The TOE provides for non-bypassability of the TOE Security Policy, and TSF domain separation. The TSP enforcement functions are invoked and succeed before security functions in the TSC are allowed to proceed. Each wireless user is authenticated before access is provided, and for authenticated wireless users, each wireless user network packet is authenticated as a part of 802.11i security protocol before the packet is processed by the TOE. Each administrator is authenticated before management access is provided and each network message coming from an authenticated administrator is authenticated as a part of the SSH protocol.

For each authenticated wireless user and remote administrator the TOE associates the user with a session object. The session object is then used to enforce domain separation for authenticated wireless users and administrators. All enforcement operations are performed within the physical boundary of the TOE. Connection to the remote authentication server is protected using an IPSec/IKE-based trusted channel, which authenticates each incoming and outgoing network packet.

The TOE maintains an IPSec/IKE trusted channel to a remote network time protocol server, which provides time used in reliable time stamps.

The TOE implements a set of FIPS 140-2 self-tests, which are executed during initial start-up and upon administrator request. The TOE provides an option to run self-tests immediately after a key is generated.

The TOE implements a set of critical self-tests, which are executed during initial start-up and upon administrator request. The tests include an integrity check for TSF data and executable code.

If the self-tests fail, the TOE security functionalities and data output are disabled.

6.1.7 TOE Access

The TOE terminates a local serial console administrator or a wireless user session after a configurable time interval of user inactivity is reached. A default banner regarding unauthorized access is displayed before establishing a user session.

6.1.8 Trusted Path/Channels

The TOE maintains a trusted channel with audit, authentication, and network time protocol servers. The channel is protected by IPSec/IKE protocol with pre-shared keys and can be initiated by the TOE or the servers.

The TOE maintains a trusted path with wireless users during the wireless user authentication phase. The trusted path is based on EAP-TLS, EAP-TTLS and PEAP protocols and can be established by wireless client devices with the help of the external authentication server, which performs authentication and cryptographic key derivation operations required by the EAP-TLS, EAP-TTLS and PEAP protocols.

6.2 Assurance Measures

The assurance requirements for this TOE are for Evaluation Assurance Level EAL4. The following items are provided as evaluation evidence to satisfy the EAL4 assurance requirements:

Table 6-1 Assurance Measures

Security Assurance Requirement	Evaluation Evidence Documentation
ACM_AUT.1 Partial CM automation	Motorola Wireless Switch Configuration Management Plan and Procedures
ACM_CAP.4 Generation support and acceptance procedures	Motorola Wireless Switch Configuration Management Plan and Procedures
ACM_SCP.2 Problem tracking CM coverage	Motorola Wireless Switch Configuration Management Plan and Procedures
ADO_DEL.2 Detection of modification	Motorola Wireless Switch Delivery and Operation Plan and Procedures
ADO_IGS.1 Installation, generation, and start-up procedures	Motorola Wireless Switch Installation Guide
ADV_FSP.2 Fully defined external interfaces	Motorola Wireless Switch Functional Specification
ADV_HLD.2 Security enforcing high-level design	Motorola Wireless Switch High-Level Design Specification

ADV_IMP.1 Subset of the implementation of the TSF	A subset of the source code and hardware diagrams used to generate the TOE
ADV_LLD.1 Descriptive low-level design	Motorola Wireless Switch Low-Level Design Specification
ADV_RCR.1 Informal correspondence demonstration	Motorola Wireless Switch Informal Correspondence Demonstration
ADV_SPM.1 Informal TOE security policy model	Motorola Wireless Switch Security Policy Model
AGD_ADM.1 Administrator guidance	Motorola Wireless Switch CLI Reference Guide Motorola Wireless Switch Installation Guide
AGD_USR.1 User guidance	Motorola Wireless Switch CLI Reference Guide Motorola Wireless Switch Installation Guide
ALC_DVS.1 Identification of security measures	Motorola Wireless Switch Life Cycle Management Plan and Procedures
ALC_FLR.2 Flaw Remediation	Motorola Wireless Switch Life Cycle Management Plan and Procedures
ALC_LCD.1 Developer defined life-cycle model	Motorola Wireless Switch Life Cycle Management Plan and Procedures
ALC_TAT.1 Well-defined development tools	Motorola Wireless Switch Life Cycle Management Plan and Procedures
ATE_COV.2 Analysis of coverage	Motorola Wireless Switch Test Coverage Analysis
ATE_DPT.1 Testing: high-level design	Motorola Wireless Switch Testing Plan and Procedures
ATE_FUN.1 Functional testing	Motorola Wireless Switch Testing Plan and Procedures
ATE_IND.2 Independent testing - sample	TOE for testing Authentication Server Audit Server Time Server Motorola Wireless Switch Testing Plan and Procedures
AVA_MSU.2 Validation of analysis	Motorola Wireless Switch Misuse Analysis Motorola Wireless Switch CLI Reference Guide Motorola Wireless Switch Installation Guide
AVA_SOF.1 Strength of TOE security function evaluation	Motorola Wireless Switch Strength of Function Analysis

AVA_VLA.2 Independent vulnerability analysis	Motorola Wireless Switch Vulnerability Analysis

7 PP Claims

The TOE conforms to the US Government Wireless Local Area Network (WLAN) Access System Protection Profile for Basic Robustness Environments, Version 1.0, April 2006.

Please see Section 8.10, PP Claims Rationale, for a detailed discussion of PP compliance.

8 Rationale

This section describes the rationale for the Security Objectives, Security Functional Requirements and TOE Summary Specification. Additionally, this section describes the rationale for not satisfying all of the dependencies and the rationale for the strength of function (SOF) claim. Table 8-1 illustrates the mapping from Security Objectives to Threats and Policies. It is identical to that of the WLANAS PP.

8.1 Rationale for Security Objectives

Table 8-1 Security Objectives to Threats and Policies Mappings

Threat/Policy	**Objectives Addressing the Threat**	**Rationale**
T.ACCIDENTAL_ADMIN_ ERROR An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.	O.ADMIN_GUIDANCE The TOE will provide administrators with the necessary information for secure management. O.MANAGE The TOE will provide those functions and facilities necessary to support the administrators in their management of the security of the TOE. 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.	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 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 by ensuring that there can be no accidental errors due to the introduction of unauthorized software or data, by ensuring that there are no general-purpose or storage repository applications available on the TOE.
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.	O.RESIDUAL_INFORMATION The TOE will ensure that any information contained in a protected resource is not released when the resource is reallocated. 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. O.SELF_PROTECTION The TOE will maintain a domain for itself and the TOE's own execution that protects them and their resources from external interference, tampering, or unauthorized disclosure through their interfaces. OE.SELF_PROTECTION The 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.	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 ensuring that cryptographic material is not accessible once it is no longer needed. O.SELF_PROTECTION ensures that the TOE will have adequate protection from external sources and that all TSP functions are invoked. OE.SELF_PROTECTION ensures that the TOEIT environment will have protection similar to that of the TOE.

T.MASQUERADE A user may masquerade as an authorized user or the authentication server to gain access to data or TOE resources.	O.TOE_ACCESS The TOE will provide mechanisms that control a user's logical access to the TOE. OE.TOE_ACCESS The environment will provide mechanisms that support the TOE in providing users 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.	O.TOE_ACCESS mitigates this threat by controlling 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 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 can not be flowing between a wireless client and another client or other host on the network without passing through the TOE.

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.	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.DOCUMENTED_ DESIGN The design of the TOE is adequately and accurately documented. O.VULNERABILITY_ ANALYSIS The TOE will undergo vulnerability analysis demonstrate the design and implementation of the TOE does not contain any obvious flaws.	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 ensures 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 a TOE claiming conformance to this ST.

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.	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.PARTIAL_FUNCTIONAL_ TESTING The TOE will undergo some security functional testing that demonstrates the TSF satisfies some of its security functional requirements. O.VULNERABILITY_ ANALYSIS The TOE will undergo vulnerability analysis to demonstrate the design and implementation of the TOE does not contain any obvious flaws.	O.CONFIGURATION_IDENTIFICATION plays a role in countering this threat by requiring the developer to provide control of the changes made to the TOE's design. This ensures that changes to the TOE are performed in structure manner and tracked. O.PARTIAL_FUNCTIONAL_TESTING ensures that the developers provide evidence and demonstration that all security functions perform as specified through independent sample testing. O.VULNERABILITY_ANALYSIS_TEST ensures that the TOE has been analyzed and tested to demonstrate that it is resistant to obvious vulnerabilities.
T.POOR_TEST 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.	O.CORRECT_ TSF_OPERATION The TOE will provide the capability to test the TSF to ensure the correct operation of the TSF at a customer's site. O.PARTIAL_FUNCTIONAL_ TESTING The TOE will undergo some security functional testing that demonstrates the TSF satisfies some of its security functional requirements. O.VULNERABILITY_ ANALYSIS The TOE will undergo some vulnerability analysis demonstrate the design and implementation of the TOE does not contain any obvious flaws.	O.CORRECT_ TSF_OPERATION provides assurance that the TSF continues to operate as expected in the field. O.PARTIAL_FUNCTIONAL_TESTING increases the likelihood that any errors that do exist in the implementation will be discovered through testing. O.VULNERABILITY_ANALYSIS_TEST addresses this concern by requiring a vulnerability analysis be performed in conjunction with testing that goes beyond functional testing. This objective provides a measure of confidence that the TOE does not contain security flaws that may not be identified through functional testing.

	O.DOCUMENTED_DESIGN The design of the TOE is adequately and accurately documented.	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 A user or process may gain unauthorized access to data through reallocation of TOE resources from one user or process to another.	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. 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.	O.RESIDUAL_INFORMATION and TOE.RESIDUAL_INFORMATION contributes to the mitigation of this threat by ensuring that any residual data is removed from network packet objects and ensuring that cryptographic material is not accessible once it is no longer needed.

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).	O.MANAGE The TOE will provide functions and facilities necessary to support the administrators in their management of the security of the TOE. 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. 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. 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. 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 interfaces. OE.SELF_PROTECTION The environment will maintain a domain for its own execution that protects itself	O.MANAGE mitigate this threat by restricting access to administrative functions and management of TSF data to the administrator. OE.MANAGE ensures that the administrator can view security relevant audit events. O.RESIDUAL_INFORMATION and OE.RESIDUAL_INFORMATION contributes to the mitigation of this threat by ensuring that any residual data is removed from network packet objects and ensuring that cryptographic material is not accessible once it is no longer needed. O.SELF_PROTECTION requires that the TOE environment 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.

	and its resources from external interference, tampering, or unauthorized disclosure through its own interfaces.	
T.UNATTENDED_SESSION A user may gain unauthorized access to an unattended session.	O.TOE_ACCESS The TOE will provide mechanisms that control a user's logical access to the TOE.	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.

T.UNAUTH_ADMIN_ACCESS An unauthorized user or process may gain access to an administrative account.	O.ADMIN_GUIDANCE The TOE will provide administrators with the necessary information for secure management. 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. 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. O.TOE_ACCESS The TOE will provide mechanisms that control a user's logical access to the TOE. OE.TOE_ACCESS The environment will provide mechanisms that support the TOE in providing user's logical access to the TOE. OE.NO_EVIL Sites using the TOE shall ensure that administrators are non-hostile, appropriately trained and follow all administrator guidance.	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 not secure. 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 helps to mitigate this threat by ensuring that the TOE administrators have guidance that instructs them in how to administer the TOE in a secure manner.

P.ACCESS_BANNER The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.	O.DISPLAY_BANNER The TOE will display an advisory warning regarding use of the TOE.	O.DISPLAY_BANNER satisfies this policy by ensuring that the TOE displays an administrator configurable banner that provides all users with a warning about unauthorized use of the TOE. A banner will be presented for all TOE services that allow direct access to the TOE. 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.
P.ACCOUNTABILITY The authorized users of the TOE shall be held accountable for their actions within the TOE.	O.AUDIT_GENERATION The TOE will provide the capability to detect and create records of security-relevant events associated with users. 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. 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. OE.MANAGE The TOE IT environment will	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

	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. O.TIME_STAMPS The TOE shall obtain reliable time stamps and the capability for the administrator to set the time used for these time stamps. 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. O.TOE_ACCESS The TOE will provide mechanisms that control a user's logical access to the TOE. OE.TOE_ACCESS The environment will provide mechanisms that support the TOE in providing user's logical access to the TOE.	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 The TOE shall provide cryptographic functions for its own use, including encryption/decryption operations.	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.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	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 TSF data while in transit to remote parts of the TOE. O.RESIDUAL_INFORMATION satisfies this policy by ensuring that cryptographic data are cleared according to FIPS 140-1/2.

	is reallocated.	
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).	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 140-1/2 validated cryptomodules for cryptographic services implementing NIST-approved security functions and random number generation services used by cryptographic functions.	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 TSF data while in transit to remote parts of the TOE. O.CRYPTOGRAPHY_VALIDATED satisfies this policy by requiring that all cryptomodules for cryptographic services be NIST 140-1/2 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 140-1/2

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.	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 140-1/2 validated cryptomodules for cryptographic services implementing NIST-approved security functions and random number generation services used by cryptographic functions. 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. OE.PROTECT_MGMT_COMMS The environment shall protect the transport of audit records to the audit server, remote network management, and authentication server communications with the TOE in a manner that is commensurate with the risks posed to the network.	O.CRYPTOGRAPHY and O.CRYPTOGRAPHY_VALIDATED satisfy this policy by requiring the TOE to implement NIST FIPS validated cryptographic services. These services will provide confidentiality and integrity protection of TSF data while in transit to wireless clients that are authorized to join the network. O.MEDIATE further allows the TOE administrator to set a policy to encrypt all wireless traffic. OE.PROTECT_MGMT_COMMS provides that the audit records, remote network management information and authentication data will be protected by means of a protected channel in the environment.

P.NO_AD_HOC_NETWORKS In concordance with the DOD Wireless Policy, there will be no ad hoc 802.11 or 802.15 networks allowed.	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. 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	O.MEDIATE works to support 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 policies.

8.2 Rationale for Security Objectives in the TOE Environment

Four of the security objectives for the TOE are simply restatements of an assumption found in Section 3.1. Therefore, these four objectives for the environment, OE.NO_EVIL, OE.PHYSICAL, OE.NO_GENERAL_PURPOSE, and OE.TOE_NO_BYPASS trace to the assumptions trivially.

The remainder of the security objectives for the IT environment have been included in this ST in order to support the TOE IT environment security functions. The rationale support is documented in Table 8-1 Security Objectives to Threats and Policies Mappings along with the rationale for security objectives for the TOE.

8.3 Rationale for TOE Security Requirements

Table 8-2 Rationale for TOE Security Requirements

Objective	Requirements Addressing the Objective	Rationale
O.ADMIN_GUIDANCE The TOE will provide administrators with the necessary information for secure management.	ADO_DEL.1 ADO_IGS.1 AGD_ADM.1 AGD_USR.1 AVA_MSU.1	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 set up and use the auditing features of the TOE. The 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 misconfigured in an insecure state due to confusing guidance.

O.AUDIT_GENERATION
The TOE will provide the capability to detect and create records of security-relevant events associated with users.
	FAU_GEN.1(1)
	FAU_GEN.2
	FAU_SEL.1
	FIA_USB.1(1),(2)
	FPT_STM_EXP.1
	FTP_ITC_EXP.1(1)
		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. This requirement also places a requirement on the level of detail that is recorded on any additional security functional requirements an ST author adds to this ST.
		FAU_GEN.2 ensures that the audit records associate a user identity with the auditable event. In the case ofauthorized users, the association is accomplished with the user ID. In all other cases, the association is based on the source network identifier, which is presumed to be the correct identity, but cannot be confirmed since these subjects are not authenticated.
		FAU_SEL.1 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 criterion for the events to be audited.
		FIA_USB.1(1),(2) play a role is satisfying this objective by requiring a binding of security attributes associated with users 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 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.	ACM_CAP.2 ACM_SCP.1 ALC_FLR.2	ACM_CAP.1 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 discovery by others. The flaw remediation process used by the developer corrects any discovered flaws and performs an analysis to ensure new flaws are not created while fixing the discovered flaws.

O.CORRECT_ TSF_OPERATION The TOE will provide the capability to test the TSF to ensure the correct operation of the TSF at a customer's site.	FPT_TST_EXP.1 FPT_TST_EXP.2	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 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.	FCS_BCM_EXP.1 FCS_CKM.1 FCS_CKM_EXP.2 FCS_CKM.4 FCS_COP_EXP.1 FCS_COP_EXP.2	The FCS requirements satisfy this objective by levying requirements that ensure the cryptographic standards include the NIST FIPS publications (wherepossible) and NIST approved ANSI standards. The intent is to have the satisfaction of the cryptographic standards be validated through a NIST FIPS 140-1/2 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 extensively the module is tested. FCS_CKM.1 ensures that, if necessary, the TOE is capable of generating cryptographic keys. FCS_CKM_EXP.2 Cryptographic Key Handling and Storage requires that FIPS PUB 140-1/2 be satisfied when performing key entry and output. FCS_CKM.4 mandates the standards (FIPS 140-1/2) 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 for data decryption and encryption that a NIST approved algorithm is used, and that the algorithm meets the FIPS PUB 140-1/2 standard.

O.CRYPTOGRAPHY_VALIDATED The TOE will use NIST FIPS 140-1/2 validated cryptomodules for cryptographic services implementing NIST-approved security functions and random number generation services used by cryptographic functions.	FCS_BCM_EXP.1 FCS_CKM.1 FCS_CKM_EXP.2 FCS_CKM.4 FCS_COP_EXP.1 FCS_COP_EXP.2	The FCS requirements satisfy this objective by levying requirements that ensure the cryptographic standards include the NIST FIPS publications (wherepossible) and NIST approved ANSI standards. The intent is to have the satisfaction of the cryptographic standards be validated through a NIST FIPS 140-1/2 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 extensively the module is tested. FCS_CKM.1 ensures that, if necessary, the TOE is capable of generating cryptographic keys. FCS_CKM_EXP.2 Cryptographic Key Handling andStorage requires that FIPS PUB 140-1/2 be satisfied when performing key entry and output. FCS_CKM.4 mandates the standards (FIPS 140-1/2) 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 for data decryption and encryption that a NIST approved algorithm is used, and that the algorithm meets the FIPS PUB 140-1/2 standard.
O.DISPLAY_BANNER The TOE will display an advisory warning regarding use of the TOE prior to permitting the use of any TOE services that require authentication.	FTA_TAB.1	FTA_TAB.1 meets this objective by requiring that the TOE display an administrator defined banner before a user can establish an authenticated session. This banner is under complete control of the administrator, who can 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	ADV_FSP.1, ADV_HLD.1, and 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 accidentaldesign errors will be discovered. ADV_RCR.1 ensures that the TOE design is consistent across the High Level Design and the Functional Specification.

O.MANAGE
The TOE will provide all the 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.
	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_SMR.1(1)
	FMT_SMF.1(1)
	FMT_SMF.1(2)
	FMT_SMF.1(3)
		The FMT requirements are used to satisfy this management objective, as well as other objectives that specify the control of functionality. The requirements' rationale for this objective focuses on the administrator's capability to perform management functions in order to control the behavior of security functions.
		FMT_MOF.1(1)(2) and (3) ensure that the administrator has the ability manage the cryptographic, audit, and authentication functions.
		FMT_MSA.2 provides the administrator the ability to accept only secure values and modify security attributes.
		FMT_MTD.1(1) (2) and (3) ensure that the administrator can manage TSF data. This ST specifically identifies audit preselection, 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 by identifying the management functions for cryptographic data, audit records, and cryptographic key data.

O.MEDIATE The TOE must mediate the flow of information to and from wireless clients communicating via the TOE RF Transmitter/Receiver	FIA_UAU.1 FIA_UAU_EXP.5(1) FIA_UID.2 FDP_PUD_EXP.1	FIA_UAU.1, FIA_UAU_EXP.5(1) and FIA_UID.2 ensure that the TOE has the ability to mediate packet flow based upon the authentication credentials of the wireless user. FDP_PUD_EXP.1 allows the administrator to control whether or not unencrypted data will be

interface in accordance with its security policy.		allowed to pass through the TOE.
O.PARTIAL_FUNCTIONAL_TESTING The TOE will undergo some security functional testing that demonstrates the TSF satisfies some of its security functional requirements.	ATE_COV.1 ATE_FUN.1 ATE_IND.2	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 that 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 ofthese requirements, the TOE's conformance to the specified security functional requirements will have been demonstrated.

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.	FDP_RIP.1(1) FCS_CKM_EXP.2 FCS_CKM.4	FDP_RIP.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
The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure.
	FPT_SEP.1(1)
	FPT_RVM.1(1)
		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 onsubjects and objects that are within the scope of 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.

O.TIME_STAMPS The TOE shall obtain reliable time stamps from the IT Environment and the capability for the administrator to set the time used for these time stamps.	FPT_STM_EXP.1	FPT_STM_EXP.1 requires that the TOE be able to obtain reliable time stamps for its own use and therefore, partially satisfies this objective. Time stamps include date and time and are reliable in that they are always available to the TOE, and the clock must be monotonically increasing.
O.TOE_ACCESS The TOE will provide mechanisms that control a user's logical access to the TOE.	FIA_AFL.1(1) FIA_ATD.1(1) FIA_UAU.1 FIA_UAU_EXP.5(1) FIA_UID.2 AVA_SOF.1 FTA_SSL.3 FTP_TRP1 FTP_ITC_EXP.1(1)	FIA_UID.2 plays a 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 that specified in the data packet. AVA_SOF.1 requires that any permutational or probabilistic mechanism in the TOE be analyzed and 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) contribute to thisobjective by ensuring that administrators and users are authenticated before they are provided access to the TOE or its services. In order to control logical access to the TOE an authentication mechanism is required. The local administrator authentication mechanism is necessary to ensure an administrator has the ability to login to the TOE regardless of network connectivity (e.g., it would be unacceptable if an administrator could not login to the TOE because the authentication server was down, or that the network path to the authentication server was unavailable). FIA_AFL.1(1) ensures that the TOE can protect itself and its users from brute force

		attacks on their authentication credentials. FIA_ATD.1(1) Management requirements provides additional control to supplement the authentication requirements. FTA_SSL.3 ensures that 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(1) provides a trusted channel for services provided by the TOE IT environment (the remote authentication server)
O.VULNERABILITY_ ANALYSIS The TOE will undergo some vulnerability analysis demonstrate the design and implementation of the TOE does not contain any obvious flaws.	AVA_VLA.1 AVA_SOF.1	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 security mechanisms vulnerable to guessing type attacks are resistant to casual attack.

8.4 Rationale for TOE IT Environment Security Requirements

Table 8-3 Rationale for Requirements on the TOE IT Environment

Objective	Requirements Addressing the Objective	Rationale

OE.AUDIT_PROTECTION The IT Environment will provide the capability to protect audit information and the authentication credentials.	FAU_SAR.2 FAU_STG.1 FAU_STG.3 FMT_MOF.1(4) FMT_SMR.1(2)	FAU_SAR.2 restricts the ability to read the audit records to only the administrator. The exception to this is that all administrators have access to the audit record information presented in the alarm indicating a potential security violation. FAU_STG.1restricts 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) specify 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 The IT Environment will provide the capability to selectively view audit information.	FAU_GEN.1(2) FAU_SAR.1 FAU_SAR.3	FAU_SAR.1 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 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 ensures that the TOE IT environment will generate appropriate audit events to support the TOE.

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.
	FMT_MOF.1(4)
	FMT_SMR.1(2)
	FMT_MTD.1(3),(4),(5)
	FMT_SMF.1(4),(5)
		FIA_USB.1 ensures that the TOE IT environment includes a mechanism to associate processes with roles. This ensures that both the TOE and its IT environment can identify
		FMT_MOF.1(4) ensures that the TOE IT environment limits access to TSF management functions to the administrator. FMT_SMR.1(2), FMT_MTD.1(3),(4), (5) FMT_SMF.1(4),(5) ensure that the TOE IT environment provides an administrative role and management functions that may be used

		to manage the IT environment.
OE.NO_EVIL Sites using the TOE shall ensure that administrators are non-hostile, appropriately trained and follow all administrator guidance.	AGD_ADM.1	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.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.NO_GENERAL_PURPOSE	It is assumed that there will be no general-purpose computing or storage capabilities available on the TOE therefore no SFR is necessary.
OE.PHYSICAL The IT environment provides physical security, commensurate with the value of the TOE and the data it contains.	A.Physical	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the IT environment. Therefore, an explicit requirement is not necessary.
OE.PROTECT_MGMT_COMMS The environment shall protect the transport of audit records to the audit server, remote network management, and authentication server communications with the	FTP_ITC_EXP.1(2)	FTP_ITC_EXP.1(2) provides a trusted channel for services provided by the TOE IT environment to the TOE (the remote authentication server, syslog serverand time server)

TOE 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.	FDP_RIP.1(2)	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 insert into new packets.

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.
	FPT_SEP.1(2)
	FPT_RVM.1(2)
		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.

OE.TOE_ACCESS
The environment will provide mechanisms that support the TOE in providing user’s logical access to the TOE.
	FIA_AFL.1(2)
	FIA_ATD.1(2)
	FIA_UAU_EXP.5(2)
	FIA_UID.1
		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.1 ensure that users are identified and authenticated.
		FIA_ATD.1(2) 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 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.	FIA_UAU.1 FIA_UAU_EXP.5(2) FIA_UID.1	FIA_UAU.1, FIA_UAU_EXP.5(2), and FIA_UID.1 ensure that the TOE has the ability to mediate packet flow based upon the authentication credentials of the wireless user.

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.	FPT_STM.1 FMT_MTD.1(5)	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(5) helps satisfy this objective by providing that there be a management function of the Security Administrator or an authorized IT entity that will set the time and date used to provide reliable time stamps to the TOE.

8.5 Rationale for Assurance Requirements

CC part 3 states:

"EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line."

"EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs."

Evaluation Assurance Level EAL4 augmented with ALC_FLR.2 in this ST was chosen based on the security environment and the security objectives defined in this ST. Due to the nature of wireless communications the TOE interacts with potentially hostile wireless environment, where any malicious entity can potentially attack the TOE. Compared to wired networks, where physical access to the network is usually limited to some extent, this amounts to an additional degree of risk and justifies evaluating the TOE at EAL4.

The explicitly stated TOE security functional requirements in this ST are those of the WLANAS PP. All assurance requirements specified in the WLANAS PP have been included in this ST. Therefore, the assurance requirements of this ST cover the explicitely stated TOE security functional requirements stated in this ST.

Evaluating the TOE at EAL4 is consistent with the current best IT security practices and provides a degree of assurance matching that of other evaluated competitive products.

ALC_FLR.2 (Flaw Remediation) was added to EAL4 requirements to match the WLANAS PP. Therefore, the assurance requirements of this ST match or exceed the requirements of WLANAS PP in all assurance areas.

8.6 Satisfaction of Dependencies

Each functional requirement, including explicit requirements was analyzed to determine that all dependencies were satisfied. All requirements were then analyzed to determine that no additional dependencies were introduced as a result of completing each operation. With the exception of dependencies related to FMT_MSA.2, all dependencies in this ST have been satisfied.

FMT_MSA.2 is included in this ST as a dependency of the Cryptographic Support family (FCS_COP and FCS_CKM). It is used there to ensure that security attributes related to cryptographic objects (e.g. cryptographic keys) are protected. However, FMT_MSA family is also used to ensure the protection of security attributes related to access control policies (FDP_IFC and FDP_AFC) and includes a dependency upon those Security Functional Requirements. However, this ST and WLANAS PP do not require that the TOE implement an access control policy and those requirements have not been included in the ST.

FCS_CKM.1 depends on FCS_CKM.2 or FCS_COP.1, which are not included in this ST. Instead, FCS_CKM_EXP.2 and FCS_COP_EXP.2 are included, which cover the requirements of FCS_CKM.2 and FCS_COP.1. FAU_GEN.1 depends on FPT_STM.1, which is not included in this ST. Instead, FPT_STM.1_EXP.1 is included, which covers the requirements of FPT_STM.1.

The satisfaction of dependencies in this ST is identical to the satisfaction of dependencies in WLANAS PP.

8.7 Rationale for Strength of Function Claims

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 against casual breach of TOE security 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 to 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.

The password used for administrator authentication is the only probabilistic or permutational mechanism implemented by the TOE. This mechanism is associated with the Identification and Authentication security function. The TOE requires the administrator password to be at least 8 characters long. Numeric, alphabetic, and extended characters can be used, which gives a total of 95 characters. Therefore, the number of potential eight-character passwords is very significant.

The SOF claims of this ST match those of WLANAS PP.

8.8 Rationale for Explicit requirements

Table 8-4 Rationale for Explicit Requirements presents the rationale for the inclusion of the explicit requirements found in this ST. The rationale matches that of WLANAS PP. The explicit requirements are reproduced from the WLANAS PP and are left unchanged to maintain compliance to the protection profile.

Table 8-4 Rationale for Explicit Requirements

Explicit Requirement	Identifier	Rationale
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. FCS_COP_EXP.1 requires FIPS approved random number generation to be used for all cryptographic functionalities, while FCS_CKM.1 is limited to cryptographic key generation.
FCS_COP_EXP.2	Cryptographic Operation	This explicit requirement is necessary because it describes requirements for a cryptomodule rather than 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(1), (2)	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 ST, an explicit requirement for authentication has been included. This ST 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_TST_EXP.1	TSF Testing	This explicit requirement is necessary because, as identified in the US Government PP Guidance for Basic Robustness, 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 Basic Robustness TOEs. Therefore, the explicit requirements are 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(1), (2)	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.

8.9 TOE Summary Specification Rationale

The TOE Summary Specification describes security functions of the TOE. The security functions considered together satisfy all of the TSFRs and security assurance requirements. All of the security functions are required in order for the TOE to support the required security functionalities.

The table below demonstrates the relationship of TSFRs to security functions.

Table 8-5 Mapping of Security Functions to TSFRs

	Security Audit	Cryptographic Support	User Data Protection	Identification and Authentication	Security Management	Protection of the TSF	TOE Access	Trusted Path/Channels
FAU_GEN.1(1)	X							
FAU_GEN.2	X							
FAU_SEL.1	X							
FCS_BCM_EXP.1		X						
FCS_CKM.1		X						
FCS_CKM_EXP.2		X						
FCS_CKM.4		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_UAU.1				X				
FIA_UAU_EXP.5(1)				X				
FIA_UID.2				X				
FIA_USB.1				X				

FMT_MOF.1(1)					X			
FMT_MOF.1(2)					X			
FMT_MOF.1(3)					X			
FMT_MSA.2					X			
FMT_MTD.1(1)					X			
FMT_MTD.1(2)					X			
FMT_SMF.1(1)					X			
FMT_SMF.1(2)					X			
FMT_SMF.1(3)					X			
FMT_SMR.1(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

The table below demonstrates suitability of Security Functions to meet TSFRs.

Table 8-6 Suitability of Security Functions to meet TSFRs

Security Functions	SFRs	Rationale
Security Audit	FAU_GEN.1(1) FAU_GEN.2 FAU_SEL.1	The Security Audit function enables TOE to generate audit events (FAU_GEN.1(1)) that contain the username for an identified user (FAU_GEN.2), and allows inclusion/exclusion of events (FAU_SEL.1).
Cryptographic Support	FCS_BCM_EXP.1 FCS_CKM.1 FCS_CKM_EXP.2 FCS_CKM.4 FCS_COP_EXP.1 FCS_COP_EXP.2(1) FCS_COP_EXP.2(2)	The Cryptographic Support function ensures that the TOE cryptographic module complies with FIPS 140-2 at Level 2 (FCS_BCM_EXP.1). The module generates cryptographic keys and random numbers (FCS_CKM.1 and FCS_COP_EXP.1), supports cryptographic key establishment (FCS_CKM_EXP.2), allows cryptographic key destruction (FCS_CKM.4), and performs cryptographic operations (FCS_COP_EXP.1, FCS_COP_EXP.2(1), and FCS_COP_EXP.2(2)).
User Data Protection	FDP_PUD_EXP.1 FDP_RIP.1(1)	The User Data Protection function ensures protection of the TOE wireless user data (FDP_PUD_EXP.1) and network packet residual information (FDP_RIP.1(1)).

Identification and Authentication	FIA_AFL.1(1)
	FIA_ATD.1(1)
	FIA_UAU.1
	FIA_UAU_EXP.5(1)
	FIA_UID.2
	FIA_USB.1(1)
	FIA_USB.1(2)
		The Identification and Authentication function ensures that the TOE prevents remote administrator login when a configurable number of unsuccessful remote administrator authentication attempts occur (FIA_AFL.1(1)), and maintains administrator passwords (FIA_ATD.1(1)).
		The TOE enforces user

		authentictation before any actions other than identification (FIA_UAU.1). The TOE authenticates administrators using passwords while wireless LAN users are authenticated using the EAP protocol (FIA_UAU_EXP.5(1)). The TOE requires that each user must be successfully identified before allowing TSF-mediated actions (FIA_UID.2). The TOE associates a username with a subject acting on the user's behalf upon successful identification and authentication of the wireless or administrator user (FIA_USB.1(1) and FIA_USB.1(2)).

Security Management	FMT_MOF.1(1)
	FMT_MOF.1(2)
	FMT_MOF.1(3)
	FMT_MSA.2
	FMT_MTD.1(1)
	FMT_MTD.1(2)
	FMT_SMF.1(1)
	FMT_SMF.1(2)
	FMT_SMF.1(3)
	FMT_SMR.1(1)
		The TOE limits the management of cryptographic, audit, and authentication security functions behavior to administrators (FMT_MOF.1(1), FMT_MOF.1(2) and FMT_MOF.1(3)) and ensures that only secure values are accepted for security attributes (FMT_MSA.2).
		The TOE limits the management of audit pre-selection data and authentication credentials to administrators (FMT_MTD.1(1) and FMT_MTD.1(2)).
		The TOE is capable of performing the management of the network packets encryption status, security audit, and cryptographic key data (FMT_SMF.1(1), FMT_SMF.1(2) and FMT_SMF.1(3)).
		The TOE maintains administrator and wireless user roles and is able to associate

		users with roles (FMT_SMR.1(1)).
Protection of the TSF	FPT_RVM.1(1) FPT_SEP.1(1) FPT_STM_EXP.1 FPT_TST_EXP.1 FPT_TST_EXP.2	The TOE provides for non-bypassability of the TOE Security Policy (FPT_RVM.1(1)) and TSF domain separation (FPT_SEP.1(1)). The TOE implements a set of FIPS 140-2 and critical self-tests executed during initial start-up and upon administrator request, or upon key generation (FPT_TST_EXP.1 and FPT_TST_EXP.2).
TOE Access	FTA_SSL.3 FTA_TAB.1	The TOE terminates a local administrator session or a wireless user session after a configurable user inactivity time interval (FTA_SSL.3). The TOE displays a default banner regarding unauthorized use of the TOE (FTA_TAB.1).
Trusted Path/Channels	FTP_ITC_EXP.1(1) FTP_TRP.1	The TOE maintains a trusted IPSec/IKE channel with the servers, which can be initiated by the TOE or the servers (FTP_ITC_EXP.1(1)). The TOE uses an EAP trusted path for wireless user authentication. The path can be initiated by wireless client devices (FTP_TRP.1).

The minimum strength level for the TOE security functions in this ST is SoF-basic. FIA_UAU.1 includes the following probabilistic/permutational mechanism for which specific SOF metrics are appropriate: password-based administrator authentication. The administrator passwords must be eight characters or longer in length and are case sensitive, resulting in 95^8 possible combinations. The password-based authentication mechanism also enforces the FIPS 140-2 requirement that for multiple attempts to use the authentication mechanism during a one-minute period, the probability is less than one in 100,000 that a random attempt will succeed or a false acceptance will occur. If one tries one million passwords per second, the exploit time is still more than 100 years, which satisfies the requirements of SoF-basic.

Mapping of assurance measures to assurance requirements is provided in Table 6-1 Assurance Measures.

8.10 PP Claims Rationale

The TOE conforms to the US Government Wireless Local Area Network (WLAN) Access System Protection Profile for Basic Robustness Environments, Version 1.0, April 2006.

The following IT security requirements statements included in this ST contain completed WLANAS PP operations:

FAU_GEN.1, FCS_CKM_EXP.2, FCS_COP_EXP.2, FDP_RIP.1, FIA_AFL.1, FIA_ATD.1, FIA_UAU.1, FIA_USB.1, FPT_TST_EXP.1, FTP_ITC_EXP.1, FTP_TRP.1, FAU_SAR.3, FAU_STG.3, FIA_UAU_EXP.5, FIA_UID.1

Except as noted earlier in this section, this ST does not contain any security objectives or TOE security functional requirements that are additional to the security objectives and the IT security requirements of WLANAS PP. Additional SFRs for the TOE IT environment have been defined to provide a more detailed description of the TOE environment - this does not impact the conformance of this ST to the PP.

The PP includes the requirement FMT_MTD.1(3), which specifies that the TOE users can only change their own authentication credentials. Since the TOE and the wireless authentication protocols implemented by the TOE do not allow non-administrator users to change their authentication credentials, the requirement FMT_MTD.1(3) would need to be refined to specify "administrators" instead of "TOE Users". Such a refined requirement would then be a duplicate of FMT_MTD.1(2), which is already included in the ST. Therefore, both the requirements FMT_MTD.1(2) and FMT_MTD.1(3) of the PP are covered by the requirement FMT_MTD.1(2) of the ST.

9 Appendix

Table 9-1 Abbreviations and Acronyms

AES	Advanced Encryption Standard
CC	Common Criteria
CBC	Cipher Block Chaining
CCM	Counter with CBC-MAC
EAL	Evaluation Assurance Level
EAP	Extensible Authentication Protocol
EAP-TLS	EAP-Transport Layer Security Protocol
EAP-TTLS	EAP-Tunneled Transport Layer Security Protocol
FIPS 140-2	Federal Information Processing Standard Publication 140-2
IKE	Internet Key Exchange Protocol
IP	Internet Protocol
IPSec	IP Security Protocol
IT	Information Technology
LAN	Local Area Network
NTP	Network Time Protocol
MAC	Media Access Control
PEAP	Protected Extensible Authentication Protocol
PP	Protection Profile
SOF	Strength of Function
SF	Security Function
SFP	Security Function Policy
SSH	Secure Shell Protocol
ST	Security Target
TOE	Target of Evaluation
TLS	Transport Layer Security Protocol
Triple DES	Triple Data Encryption Standard
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
WLAN	Wireless Local Area Network
WLANAS PP	US Government Wireless Local Area Network (WLAN) Access System Protection Profile for Basic Robustness Environments, Version 1.0, April 2006.

Table 9-2 References

[1] Common Criteria for Information Technology Security Evaluation, Part 1, Version 2.3, August 2005, CCMB-2005-08-001
[2] Common Criteria for Information Technology Security Evaluation, Part 2, Version 2.3, August 2005, CCMB-2005-08-002
[3] Common Criteria for Information Technology Security Evaluation, Part 3, Version 2.3, August 2005, CCMB-2005-08-003
[4] Common Methodology for Information Technology Security Evaluation, Version 2.3, August 2005, CCMB-2005-08-004
[5] US Government Wireless Local Area Network (WLAN) Access System Protection Profile For Basic Robustness Environments, Version 1.0, April 2006

[6] FIPS PUB 140-2, Security Requirements for Cryptographic Modules, May 2001

[7] Motorola Wireless Switch Configuration Management Plan and Procedures

[8] Motorola Wireless Switch Delivery and Operation Plan and Procedures

[9] Motorola Wireless Switch Installation Guide

[10] Motorola Wireless Switch Functional Specification

[11] Motorola Wireless Switch High-Level Design Specification

[12] Motorola Wireless Switch Low-Level Design Specification

[13] Motorola Wireless Switch Informal Correspondence Demonstration

[14] Motorola Wireless Switch Security Policy Model

[15] Motorola Wireless Switch CLI Reference Guide

[16] Motorola Wireless Switch Life Cycle Management Plan and Procedures

[17] Motorola Wireless Switch Test Coverage Analysis

[18] Motorola Wireless Switch Testing Plan and Procedures

[19] Motorola Wireless Switch Misuse Analysis

[20] Motorola Wireless Switch Strength of Function Analysis

[21] Motorola Wireless Switch Vulnerability Analysis