Aruba 6000 and Aruba 800 Series Mobility Controller

Security Target

Version 1.8

May 28, 2008

Prepared for:

Aruba Networks™
1322 Crossman Ave.
Sunnyvale, CA 94089-1113
Phone: 408-227-4500
Fax: 408-227-4550

Prepared by:

TABLE OF CONTENTS

SECTION **PAGE**

Table of Tables and Figures

Table or Figure **Page**

1 Security Target Introduction

1.1 Security Target Identification

TOE Identification: Aruba 6000 and Aruba 800 series Mobility Controller

Hardware Versions:

a. Aruba 800 series: HW-800-CHAS-SPOE-SX, HW-800-CHAS-SPOE-T

b. Aruba 6000 series: HW-CHASF (3300028 Rev. 01), HW-FTF (3300031 Rev. 01), LC-2G24F (3300026 Rev. 01), LC-2G (3300029-01), LC-2G24FP (3300024 Rev. 01), SC-256-C2 (3300027 Rev. 01), SC-48-C1 (3300025- 01), SC-128-C1 (3300025-01), HW-PSU-200, HW-PSU-400

Software Versions:

a. Aruba 800 series: A800_2.4.8.14-FIPS
b. Aruba 6000 series: A5000_2.4.8.14-FIPS

ST Title: Aruba 6000 and Aruba 800 series Mobility Controller Security Target
ST Version: Version 1.8
ST Date: 05/28/2008
CC Version: Common Criteria Version 2.3 August 2005 CCMB-2005-08-003
Assurance Level: EAL2
Strength of Function: SOF-basic
Keywords: Identification, Authentication, Access Control, Security Target, Security Management, Aruba Mobility Controller, Wireless IDS

1.2 Security Target Overview

This Security Target (ST) defines Information Technology (IT) security requirements for Aruba 6000 and Aruba 800 series Mobility Controllers.

Aruba 6000 and Aruba 800 series Mobility Controllers are wireless LAN (WLAN) switches. A WLAN switch is a gateway device which controls operation of multiple Access Points (APs), processes network data flows between wireless and wired networks, and implements various wired and wireless network and security protocols. Each Aruba Mobility Controller integrates multiple features, such as wireless security protocol processing, policy enforcement firewall, wireless intrusion protection, and VPN server. Aruba Mobility Controllers are hardware devices that run the ArubaOS software suite.

1.3 Common Criteria Conformance

The TOE is Part 2 extended, Part 3 conformant, and meets the requirements of Evaluation Assurance Level (EAL) 2 from the Common Criteria Version 2.3 August 2005, augmented with ACM_SCP.1 (TOE CM Coverage), ALC_FLR.2 (Flaw Remediations) and AVA_MSU.1 (Misuse – Examination of Guidance).

1.4 Document Conventions

The notation, formatting, and conventions used in this security target (ST) are consistent with version 2.3 of the Common Criteria for Information Technology Security Evaluation. All of the components are taken directly from Part 2 of the CC except the ones noted with "_EXP" in the component name. The font style and clarifying information conventions were developed to aid the reader.

The CC permits four functional component operations: assignment, iteration, refinement, and selection to be performed on functional requirements. These operations are defined in CC Part 1 and Part 2, and this ST identifies them as the following:

- Assignment - allows specification of an identified parameter. In this ST the assignments are specified in italicized text (e.g. *assignment*).
- Iteration - allows a component to be used more than once with varying operations. Iterations are identified with a lower case letter following the typical CC requirement naming for each new iteration (e.g. FMT_MTD.1a).
- Refinement - allows addition of details or narrowing of the requirements. In this ST refinements are specified in italicized, bold, underlined text for additional text (e.g. ***additional text***), and strikethrough for deletion text (e.g. ~~deletion text~~).
- Selection - allows specification of one or more elements from a list. Selections are specified in bold text in this ST (e.g. **selection**).
- Explicitly stated requirements will be noted with "_EXP" added to the component name in this ST.

1.5 Document Organization

The main sections of the ST are the ST Introduction, Target of Evaluation (TOE) Description, TOE Security Environment, Security Objectives, IT Security Requirements, TOE Summary Specification, Protection Profile Claims, and Rationale.

Section 2, the TOE Description, describes the product type and the scope and boundaries of the TOE.

Section 3, TOE Security Environment, identifies assumptions about TOE's intended usage and environment and threats relevant to secure TOE operation.

Section 4, Security Objectives, defines the security objectives for the TOE and its environment.

Section 5, IT Security Requirements, specifies the TOE Security Functional Requirements (SFR), Security Requirements for the IT Environment, and the Security Assurance Requirements (SAR).

Section 6, TOE Summary Specification, describes the IT Security Functions and Assurance Measures.

Section 7, Protection Profile (PP) Claims, references the PP to which conformance is claimed and identifies any additional TOE objectives and any tailored or additional IT security requirements.

Section 8, Rationale, presents evidence that the ST is a complete and cohesive set of requirements and that a conformant TOE would provide an effective set of IT security countermeasures within the security environment. The Rationale has three main parts: Security Objectives Rationale, Security Requirements Rationale, and TOE Summary Specification Rationale.

Section 9 provides acronyms, definitions and references.

2 TOE Description

2.1 Product Type

Aruba 6000 and Aruba 800 series Mobility Controllers are wireless LAN (WLAN) switches. A WLAN switch is a gateway device which controls operation of multiple Access Points (APs), processes network data flows between wireless and wired networks, and implements various wired and wireless network and security protocols. All Aruba Mobility Controllers are hardware devices that run the ArubaOS software suite. Aruba 6000 and Aruba 800 series Mobility Controllers have a steel case that physically encloses the complete set of hardware and software components.

2.1.1 Security features included in the evaluation

The following features of the Aruba Mobility Controllers are included in the evaluation:

- Auditing, which utilizes an external audit server
- FIPS 140-2 validated cryptographic processing
- Identification and Authentication, which utilizes an external authentication server
- Wireless Intrusion protection
- Security Management
- Utilizing external Network Time Protocol (NTP) server
- Trusted Path used for remote administrator authentication
- Trusted Path used for wireless user authentication, in the case of open system connection
- Trusted Channels used for connections between the TOE and authentication/audit/NTP servers
- User Data and TSF protection, including Virtual Private Network (VPN) Server and Wireless Security Protocol Processing.

2.1.2 Security features not included in the evaluation

The following features of the Aruba Mobility Controllers are not included in the evaluation:

- Radio Frequency (RF) spectrum monitoring and management.
- Client Integrity module, which enforces secure configuration of wired and wireless devices prior to providing access to network resources.
- Mobility with roaming, which allows wireless devices to move between APs without losing network connectivity.
- WEP, dynamic WEP, WPA, TKIP (WPA-1) protocols are disabled in the FIPS 140-2 approved mode of operation and are outside of the scope of this evaluation. Note: compliance to standards is a vendor assertion and is not tested.
- Policy enforcement firewall.

2.1.3 TOE design and operation

In the evaluated configuration the TOE is used in the FIPS 140-2 approved mode of operation. The Aruba Mobility Controllers utilize the following security protocols in the FIPS 140-2 approved mode of operation:

TLS (RFC 2246), 802.11i (IEEE 802.11i), EAP-TLS, EAP-TTLS (RFC 2716, RFC 3748 and draft-funk-eap-ttls-v1-01), PEAP (draft-josefsson-pppext-eap-tls-eap-05), xSec, IPSec/IKE (RFCs 2401-2412), SSH (RFCs 4251-4254), RADIUS (RFC 2865 and RFC 2866). Note: compliance to standards is a vendor assertion and is not tested.

These protocols are used as follows:

- TLS is used to secure the remote administrator authentication, the HTTPS Web UI administration interface and is also used in EAP-TLS, EAP-TTLS, and PEAP protocols. TLS uses server-side digital certificates during the TLS handshake.

- SSH is used to secure the remote command line administration interface.

- 802.11i is used to secure network traffic to and from wireless users at Layer 2.

- EAP-TLS, EAP-TTLS, PEAP and RADIUS protocols are used as follows: the TOE utilizes an external RADIUS authentication server to provide authentication of wireless users. In particular, when a wireless user connects to the TOE through a wireless access point, the TOE employs the external RADIUS server to authenticate the user. During the authentication phase, the TOE passes EAP protocol authentication messages between the RADIUS authentication server and the wireless client, until the client is authenticated. The following EAP protocol types are supported: EAP-TLS, EAP-TTLS, PEAP. These protocols use the TLS protocol internally to secure authentication data between the RADIUS server and the wireless client and to establish a session key. Once the authentication is completed, the RADIUS server passes the session key to the TOE. The session key is then used to encrypt wireless data traffic between the TOE and the wireless client using the 802.11i or xSec protocols. EAP-TLS, EAP-TTLS, and PEAP use server-side TLS certificates to authenticate the authentication server to the wireless client. EAP-TLS will use a client side certificate to authenticate the wireless client to the authentication server. PEAP and EAP-TTLS will use a username/password to authenticate the wireless client to the authentication server. The server TLS certificates are stored and managed by the RADIUS server. The client TLS certificates are stored on the wireless client.

- xSec is used to secure network traffic to and from wireless network clients at Layer 2. xSec is used to provide a non disruptive 802.11i upgrade overlay solution for legacy infrastructure that is incapable of supporting 802.11i natively.

- IPSec/IKE protocol is used by the VPN Server to secure network traffic between the TOE and wireless network clients, providing also a trusted path for wireless user authentication in the case of non-802.11i user authentication. IPSec/IKE is also used to secure network traffic to wired network hosts, providing trusted channels between the TOE and authentication/audit/NTP servers.

Since the wireless security protocol processing functionality resides on the Aruba Mobility Controller and on the authentication server, access points do not provide security-related functionalities and become dumb devices that do not have to be secured.

In a typical usage scenario, a wireless client attempts to connect to an access point. The access point passes the connection request to the TOE, which in turn passes the request to the authentication server. The authentication server exchanges messages with the wireless client through the TOE and the access point to perform secure session key derivation and secure authentication using EAP-TLS, EAP-TTLS or PEAP protocol. Once the wireless user is successfully authenticated, the authentication server passes the session key and the user role information to the TOE. The TOE establishes a secure connection to the client through the access point using either xSec or 802.11i protocol. The TOE then performs all necessary wireless protocol processing, including encryption, decryption, message authentication code calculation and verification.

The option is also available to use on open system connection. The wireless client connects to the TOE, after which an IPSec/IKE shared key VPN is set up between the wireless client and the TOE. The user then authenticates, to the authentication server passing the authentication details to the server via the TOE. The VPN protects both the user authentication data and the user data.

The TOE uses an external syslog audit server to store audit records. The TOE uses and external Network Time Protocol (NTP) server to obtain reliable time stamps. The TOE utilizes an IPSec/IKE trusted channel to connect to the audit server and NTP server, as well as to the authentication server.

The hardware design of the TOE includes the main processor (control processor), which executes the MontaVista Embedded Linux operating system, the network processor, and the cryptographic processor. The ArubaOS software suite is executed on top of the MontaVista Embedded Linux Linux operating system. The control processor executes all generic tasks necessary for operation of the TOE, except the network packet processing tasks, which are executed by the network processor, and cryptographic acceleration tasks which are executed by the cryptographic processor. The network processor executes a specialized embedded operating system SiByte OS, which handles processing of network packets.

The Aruba 6000 series Mobility Controller can handle up to 512 access points, 8,000 simultaneous wireless connections and up to 7.2 Gbps of encrypted throughput. Aruba 6000 contains the following processors:

- MPC8245 control processor running MontaVista's Embedded Linux as the operating system coupled with LVL7's FASTPATH package. The ArubaOS software suite is executed on the MontaVista Embedded Linux platform.

- BCM1250 network processor executes SOS (SiByte OS). It performs network data frame processing functions. The BCM1250 network processor is connected to the MPC8245 control processor via the PCI and serial interfaces.

- Cavium CN1330 cryptographic processor. The CN1330 processor is used to accelerate cryptographic operations performed by xSec, IPSec/IKE, TLS and 802.11i security protocols. It supports AES, TDES, RSA, SHA-1, and HMAC SHA-1 algorithms. The CN1330 processor is connected to the BCM1250 processor through a serial bus.

The Aruba 800 series Mobility Controller can support up to 16 access points and contains the following processors:

- MPC8241 control processor running MontaVista's Embedded Linux as the operating system coupled with the LVL7's FASTPATH package. The ArubaOS software suite is executed on the MontaVista Embedded Linux platform.

- BCM1125 network processor executes SOS (SiByte OS). It performs network data frame processing functions. The BCM1125 network processor is connected to the MPC8241 control processor via PCI and serial interfaces.

- Cavium CN1001 cryptographic processor. The CN1001 processor is used to accelerate cryptographic operations performed by xSec, IPSec/IKE, TLS and 802.11i security protocols. It supports AES, TDES, RSA, SHA-1, and HMAC SHA-1 algorithms. The CN1001 processor communicates with the BCM1125 processor via the PCI interface.

2.2 TOE Physical Boundary

The TOE consists of the Aruba Mobility Controller hardware device which executes the ArubaOS software suite.

This evaluation includes the Aruba 6000 and Aruba 800 series Mobility Controller hardware devices. Although these devices have different specifications (in terms of performance and capabilities), they both provide the same security functions described in this ST; therefore they have been considered to be the same for the purposes of the ST description.

ArubaOS serves as the software suite for the Aruba 6000 and Aruba 800 series Mobility Controllers. ArubaOS is installed on each Mobility Controller. It is located within the TOE boundary, and is executed on the MontaVista Embedded Linux platform.

The Aruba Mobility Controller works with Aruba and third-party wireless access points. The Access Points (Aruba or third parties) are considered outside the TOE boundary and are outside the scope of this evaluation, therefore, they are considered to be a part of the IT environment.

The Aruba 6000 and Aruba 800 series Mobility Controllers have a steel case that encloses the complete set of hardware and software components and represents the physical boundary of the TOE.

The TOE evaluated configuration and the TOE boundary are illustrated in Figure 2-1.

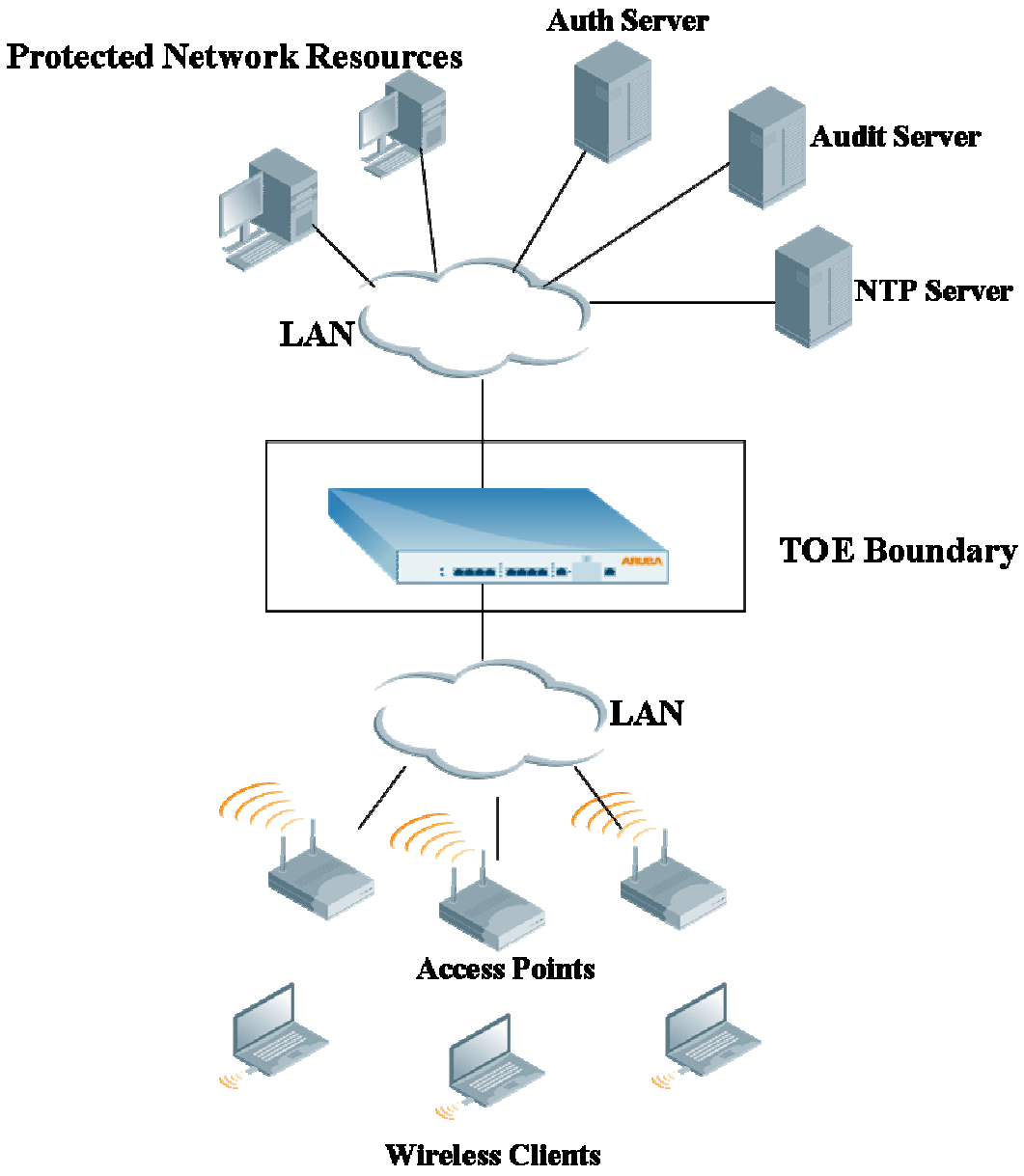

Figure 2-1: The evaluated configuration

2.3 TOE Logical Boundary

The TOE security functions are:

Auditing – The TOE provides a functionality to log security-relevant events. It uses a logging level that can be set for each of the ArubaOS modules. The administrator can configure a logging level (total of eight logging levels) independently for each module. An external syslog

audit server is used to store and review audit records. An external NTP server is used to obtain reliable time stamps.

Cryptography - The TOE employs cryptographic functionalities of a FIPS 140-2 validated module for the purposes of wireless and wired security protocol processing as well as for establishment of secure remote administration sessions.

Aruba 6000 and 800 series Mobility Controllers have been validated to meet the FIPS 140-2 Level 2 security requirements. Cryptographic Key Management section of the Cryptographic Module Security Policy (Certificate #649: <***http://csrc.nist.gov/cryptval/140-1/1401val2006.htm#649***>) provides detailed information in regards to the cryptographic key generation, key distribution, and key destruction used in Aruba Mobility Controller 6000 and 800 series.

I&A and TOE Access - The TOE employs an external RADIUS authentication server to provide authentication protocols for wireless users. For wireless users, the authentication protocols include EAP-TLS, EAP-TTLS and PEAP. Additionally wireless users may connect using an open system connection using a VPN. In this case the user authenticates to the RADIUS server using a username and password.

Remote administrators access the TOE via a wired interface. A remote administrator is configured with two user accounts, a specially privileged wired user account and a management user account. The wired user account is privileged to access the management interfaces, which allow a further authentication as a management user to allow management to be performed. The wired user's privilege is assigned by means of the user's role. A remote administrator authenticates first as the wired user against the external RADIUS server and then as a management user against an internal authentication database. For both authentications a username and password is used.

When a user authenticates against the external RADIUS server, information identifying the user's role is passed back from the RADIUS server to the TOE. The user's role determines the access that the user is granted. At the highest level of granularity this is either as a wireless user or as an administrator.

Local administrators, who access the TOE using the serial console interface, are authenticated as management users using the internal authentication database using a username and password.

The TOE terminates a wireless user or remote administrator management user session once the inactivity time exceeds the configurable idle timeout. The RADIUS server will lock out wireless user or remote administrator wired user once a configurable limit of unsuccessful authentication attempts has been reached.

Communications between the TOE and the external authentication server are protected by an IPSec/IKE-based trusted channel.

Security Management - The administrator can configure TOE security settings and policies using the Web User Interface (Web UI) via HTTPS, or the Command Line Interface (CLI) via a remote SSH or local serial console connection.

Trusted Path/Channels - The Mobility Controller provides a TLS based trusted path between itself and the remote administrator. For wireless users using an open system connection, the Mobility Controller provides an IPSec/IKE VPN trusted path between itself and the wireless users. The Mobility Controller provides a trusted channel between itself and external authentication, audit and time servers.

Note: For the authentication of wireless users using 802.11i authentication, the IT environment provides a trusted path. When using the EAP-TTLS and PEAP authentication protocols, the IT environment provides a TLS based trusted path between the authentication server and the wireless user. The trusted path passes through the TOE and is used for authentication, in particular, to pass the wireless user authentication credentials to the authentication server. The TOE participates in the authentication process processes by passing authentication protocol messages between the wireless client and the authentication server. When using the EAP-TLS authentication protocol is used, the authentication is performed by means of certificates and the trusted path is provided by the PKI mechanism.

User Data and TSF Protection - TOE data, executables and Critical Security Parameters are protected inside the FIPS 140-2 Level 2 validated Mobility Controller device. The device enclosure is resistant to probing and is opaque within the visible spectrum. The enclosure was designed and validated to satisfy FIPS 140-2 Level 2 physical security requirements. Tamper-evident seals are used to detect unauthorized access to the internal components of the TOE.

The TOE operational environment is a non-modifiable operational environment, which does not allow unauthorized access to user and TSF data. The primary operating system is Linux, an operating system that supports memory protection for user and TSF data belonging to a particular process. The TOE does not provide user access to the underlying Linux operating system. The user may only utilize well defined external logical interfaces provided by the TOE.

The command line interface, accessible via remote SSH and local serial console, is a restricted interface, which does not permit execution of arbitrary operating system commands, and only provides a restricted command set.

Users must successfully authenticate prior to assumption of the corresponding user role. The TOE enforces separation of user sessions. In particular, data belonging to a particular user session is only accessible by the corresponding user. All Mobility Controller security functions utilize access control and policy enforcement.

As an administrator specified option, user and TSF data is protected by wireless and wired security protocols while in transit. The protocol implementations utilize cryptographic algorithms of a FIPS 140-2 validated module. The TOE supports the following wireless security protocols that protect confidentiality and integrity of wireless data: 802.11i, xSec. The VPN server functionality of the TOE provides support for the IPSec/IKE protocol.

Wireless Intrusion Protection (WIP) – The TOE is capable of analyzing wired and wireless traffic to detect anomalous activity, based on a variety of information including the configuration of valid APs and the characteristics of received wireless frames. The administrator can configure the Aruba Mobility Controller to detect and, where possible, protect the managed networks from specific types of network intrusion attacks.

2.4 IT Environment

The TOE utilizes an external RADIUS authentication server for wireless user and remote administrator authentication, an external NTP server for import of reliable time stamps, and an external syslog audit server for storage of audit records. Communications between the TOE and the external RADIUS, NTP and syslog servers are protected by the IPSec/IKE trusted channel. The IPSec/IKE protocol uses a pre-shared key to provide assured identification of trusted channel endpoints.

The RADIUS authentication server handles authentication of wireless users using EAP-TLS, EAP-TTLS, and PEAP protocols, and communicates success/failure of the authentication attempt to the

TOE. In case of a successful authentication, the authentication server derives a session key which is then provided to the TOE to be used for protection of wireless user data. The authentication server also communicates the wireless user role to the TOE. The IT environment (RADIUS server) stores and manages server certificates used by EAP-TLS, EAP-TTLS, and PEAP protocols, as well as the list of trusted certification authorities used to verify the client certificate in the EAP-TLS protocol. It also stores a user database, including user names, passwords and roles. The authentication server generates audit records of its configuration changes and security-relevant events.

The RADIUS authentication server authenticates remote administrators as wired users using its user database.

The syslog audit server stores records of audit events and provides a capability to review the records. It also generates audit records of its configuration changes, as well as for startup and shutdown of audit functions. The audit server protects the audit records from unauthorized disclosure, modification or deletion.

ArubaOS NTP implementation uses the standard NTP UDP based protocol.

The access points are controlled by the Mobility Controller and serve as dumb devices, delegating security functionalities to the Mobility Controller. The access points are located outside the TOE boundary and outside the scope of this evaluation; therefore they are considered to be part of the IT environment.

3 TOE Security Environment

This section identifies secure usage assumptions, threats to security and organizational security policies.

3.1 Assumptions

This section contains assumptions regarding the security environment and the intended usage of the TOE.

Table 3-1 Assumptions

A.ADMIN	Administrators are non-hostile, appropriately trained and follow all administrator guidance.
A.NO_GENRL	There are no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the TOE.
A.LOCATE	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.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

The assumed level of expertise of the attacker for all the threats is unsophisticated, with access to standard equipment and public information.

The TOE must counter the following threats to security:

Table 3-2 Threats

T.ERROR	An administrator may accidentally incorrectly install or configure the TOE, resulting in ineffective security mechanisms.
T.IMPERSON	A user may gain unauthorized access to data or TOE resources by impersonating an authorized user of the TOE.
T.ACCESS	An unauthorized user or process may gain access to an administrative account.
T.ATTACK	A user may gain access to TSF data, executable code or 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.RESIDUAL	A user or process may gain unauthorized access to data through reallocation of TOE resources from one user or process to another.
T.SESSION	A user may gain unauthorized access to an unattended session
T.CRYPTO	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.INTERNAL	A user or process may cause, through an unsophisticated attack, TSF data, or executable code to be inappropriately accessed (viewed, modified, or deleted).

Application Note: PP Threats T.POOR_DESIGN, T.POOR_IMPLEMENTATION and T.POOR_TEST are not included in this Security Target, as they are not considered to be threats to the TOE, but threats that are applicable to the TOE development, countered by the EAL2 assurance measures.

3.3 Organizational Security Policies

This section identifies applicable organizational security policies.

Table 3-3 Organizational Security Policies

P.BANNER	The TOE shall display an initial banner for administrative logins describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.
P.ACCOUNT	The authorized users of the TOE shall be held accountable for their actions within the TOE.
P.CRYPTO	The TOE shall provide NIST FIPS 140-2 validated cryptographic modules that provide cryptographic functions for its own use, including encryption/decryption operations.
P.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_ADHOC	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

The Security Objectives for the TOE are as follows:

Table 4-1 Security Objectives for TOE

O.AUDIT_GEN	The TOE will provide the capability to detect and create records of security-relevant events, including those associated with users.
O.BANNER	The TOE will display an administrator configurable advisory warning banner regarding use of the TOE prior to establishing an administrator session.
O.CORRECT	The TOE will provide the capability to verify the correct operation of the TSF.
O.CRYPTO	The TOE shall use cryptographic mechanisms of a FIPS 140-2 validated module to protect wireless user data, remote administration sessions, and VPN traffic.
O.INTRUSION	The TOE will detect wireless intrusion attempts, alert administrators and, where possible, prevent or contain the intrusion attempts.
O.MANAGE	The TOE must allow administrators to effectively manage the TOE and its security functions, and must ensure that only authorized administrators are able to access such functionality.
O.RESIDUAL	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_PROTECT	The TOE will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure.
O.TIME	The TOE will obtain reliable time stamps
O.TOE_ACCESS	The TOE will provide mechanisms that control a user's logical access to the TOE.
O.TRAFFIC	The TOE must mediate the flow of information to and from wireless devices in accordance with its security policy.

Application Note: PP TOE security objectives O.ADMIN_GUIDANCE, O.CONFIGURATION, O_ IDENTIFICATION, O.DOCUMENTED_ DESIGN, O.PARTIAL_FUNCTIONAL_TESTING and O.VULNERABILITY_ ANALYSIS are not included in this Security Target, as they are not considered to be security objectives of the TOE, but security objectives that are applicable to the TOE development, countered by the EAL2 assurance measures.

4.2 Security Objectives for the Environment

4.2.1 Security Objectives for the IT Environment

The Security Objectives for the IT Environment are as follows:

Table 4-2 Security Objectives for the IT Environment

OE.AUDIT_PROTECT	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 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.SELF_PROTECT	The IT Environment will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure through its own interfaces.
OE.TIME	The IT Environment shall provide reliable time stamps and the capability for the administrator to set the time used for these time stamps.
OE.TOE_ACCESS	The IT Environment will provide mechanisms that support the TOE in providing a user's logical access to the TOE.
OE.RESIDUAL	The 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.PROTECT_COMMS	The IT Environment shall protect the transport of audit records to the audit server, and authentication server and time server communications with the TOE, and remote network management, in a manner that is commensurate with the risks posed to the network.

4.2.2 Non-IT Security Objectives

The Non-IT security objectives are as follows:

Table 4-3 Security Objectives for Non-IT Environment

OE.ADMIN	Any administrator of the TOE will be competent to manage the TOE and can be trusted not to deliberately abuse their privileges.
OE.NO_GENRL	There are no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the TOE.

OE.PROTECT	The environment provides physical security, commensurate with the value of the TOE and the data it contains.
OE.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 are satisfied by the TOE and the IT environment.

5.1 TOE Security Functional Requirements

The TOE security functional requirements are listed in Table 5-1 Functional Components.

Table 5-1 Functional Components

Item	Component	Component Name	PP Conformance
1	FAU_ARP.1	Security alarms	Additional
2	FAU_SAA.3	Simple attack heuristics	Additional
3	FAU_GEN.1a	Audit data generation	PP Tailored
4	FAU_GEN.2	User identity association	PP
5	FAU_SEL.1	Selective audit	PP Tailored
6	FIA_UAU.1a	Timing of authentication	PP Tailored
7	FIA_UAU_EXP.5a	Multiple authentication mechanisms	PP
8	FIA_UID.2a	User identification before any action	PP
9	FIA_ATD.1a	Administrator attribute definition	PP Tailored
10	FIA_ATD.1b	User attribute definition	PP Tailored
11	FIA_USB.1	User-subject binding	PP Tailored
12	FTA_SSL.3	TSF-initiated termination	PP Tailored
13	FTA_TAB.1	Default TOE access banners	PP Tailored
14	FCS_CKM.1a	Cryptographic key generation	PP Tailored
15	FCS_CKM.2a	Cryptographic key distribution	Additional
16	FCS_CKM_EXP.2	Cryptographic key establishment	PP Tailored
17	FCS_CKM.4a	Cryptographic key destruction	PP Tailored
18	FCS_COP.1a	Cryptographic operation	PP Tailored
19	FDP_PUD_EXP.1	Protection of User Data	PP Tailored
20	FDP_RIP.1a	Subset residual information protection	PP Tailored
21	FPT_RVM.1a	Non-bypassability of the TSP	PP
22	FPT_SEP.1a	TSF domain separation	PP
23	FPT_STM_EXP.1	Reliable time stamps	PP
24	FPT_TST_EXP.1	TSF Testing	PP Tailored
25	FPT_TST_EXP.2	TSF Testing of Cryptographic Modules	PP Tailored

Item	Component	Component Name	PP Conformance
26	FMT_MOF.1a	Management of security functions behavior (Cryptographic Function)	PP
27	FMT_MOF.1b	Management of security functions behavior (Audit Record Generation)	PP
28	FMT_MOF.1c	Management of security functions behavior (Authentication)	PP Tailored
29	FMT_MOF.1d	Management of security functions behavior (Wireless Intrusion Protection)	Additional
30	FMT_MSA.2	Secure security attributes	PP
31	FMT_MTD.1a	Management of Audit data	PP
32	FMT_MTD.1b	Management of Authentication data (Administrator)	PP
33	FMT_MTD.1c	Management of Authentication data (User)	PP
34	FMT_SMF.1a	Specification of management functions (Cryptographic Functions)	PP Tailored
35	FMT_SMF.1b	Specification of management functions (TOE Audit Record Generation)	PP
36	FMT_SMF.1c	Specification of management functions (Cryptographic Key Data)	PP
37	FMT_SMF.1d	Specification of management functions (Wireless Intrusion Protection)	Additional
38	FMT_SMF.1e	Specification of management functions (TOE Authentication Data)	Additional
39	FMT_SMR.1a	Security roles	PP Tailored
40	FTP_ITC_EXP.1a	Inter-TSF trusted channel	PP Tailored
41	FTP_TRP.1a	Trusted path (Remote Administrator)	PP Corrected
42	FTP_TRP.1b	Trusted path (wireless user using open system connection)	PP Corrected

5.1.1 Security Audit

5.1.1.1 FAU_ARP.1 Security alarms

FAU_ARP.1.1 The TSF shall take [the actions specified in column three of Table 5-2 WIP signature events, information and actions] upon detection of a potential security violation.

5.1.1.2 FAU_SAA.3 Simple attack heuristics

FAU_SAA.3.1 The TSF shall be able to maintain an internal representation of the following signature events [the subset of system events specified in column one of Table 5-2 WIP signature events, information and actions] that may indicate a violation of the TSP.

FAU_SAA.3.2 The TSF shall be able to compare the signature events against the record of system activity discernable from an examination of *[the information specified in column two of Table 5-2 WIP signature events, information and actions]*.

FAU_SAA.3.3 The TSF shall be able to indicate an imminent violation of the TSP when a system event is found to match a signature event that indicates a potential violation of the TSP.

Table 5-2 WIP signature events, information and actions

Signature Event	Information used to detect event	Action on event
Rogue AP detection	Wireless and wired traffic characteristics	Notify administrator of presence and precise physical location of AP If configured by an administrator, automatically disable the AP
Denial of Service attack	Anomalous rates of 802.11 management frames	Notify administrator
MAC address spoofing	802.11 MAC sequence number analysis	Notify administrator
Station disconnection detection	Anomalies in the 802.11 sequence number on specific 802.11 management frames	Notify administrator
EAP handshake flood DOS attack	Floods of EAPOL messages requesting 802.1x authentication	Notify administrator
Sequence Number Analysis	Anomalies in 802.11 MAC sequence numbers of received frames	Notify administrator
Null-Probe-Response signature detection	Received SSID element of 0 length in a probe response frame	Notify administrator

Signature Event	Information used to detect event	Action on event
AirJack signature detection	Received SSID of “AirJack” in beacon frame	Notify administrator
NetStumbler Generic signature detection	802.11 data packets with specific patterns in the payload	Notify administrator
NetStumbler Version 3.3.0x signature detection	802.11 data packets with specific patterns in the payload	Notify administrator
Deauth-Broadcast signature detection	802.11 deauthentication frames with the broadcast MAC as the destination address	Notify administrator
Misconfigured AP detection	An AP advertising capabilities that do not match known valid AP characteristics	Notify administrator If configured by an administrator, deny access by AP

5.1.1.3 FAU_GEN.1a Audit Data Generation

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

a) Start-up and shutdown of the audit functions;
b) All auditable events for the [**not specified**] level of audit; and
c) [events specified in column two of Table 5-3]

Application note: The ST SFR requires auditable events for the [not specified] level of audit, rather than the PP required [minimum] level of audit – in fact, all of the PP required auditable events are included explicitly in Table 5-3*, and the [not specified] level of audit is selected to apply to additional ST SFRs.*

Table 5-3 TOE Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents
FAU_ARP.1	Actions taken due to imminent security violations	None

Requirement	Auditable Events	Additional Audit Record Contents
FAU_SAA.3	Enabling and disabling of any of the analysis mechanisms Automated responses performed by the tool	None
FAU_GEN.1a	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
FIA_UAU.1a	Use of the authentication mechanism (success or failure)	User identity – the TOE **SHALL NOT** record invalid passwords in the audit log
FIA_UAU_EXP.5a	Failure to receive a response from the remote authentication server	Identification of the Authentication server that did not reply
FIA_UID.2a	None	None
FIA_ATD.1a	None	None
FIA_ATD.1b	None	None
FIA_USB.1	Unsuccessful binding of user security attributes to a subject	None
FTA_SSL.3 See App Note below	TSF Initiated Termination	Termination of an interactive session by the session locking mechanism
FTA_TAB.1	None	None
FCS_CKM.1a	Success or failure of key generation	none
FCS_CKM.2a	Success or failure of key distribution	The identity of the Administrator performing the function
FCS_CKM_EXP.2	Manual load of a key	None
FCS_CKM.4a	Destruction of a cryptographic key	The identity of the Administrator performing the function

Requirement	Auditable Events	Additional Audit Record Contents
FCS_COP.1a	Success or failure of operation	Type of cryptographic operation
FDP_PUD_EXP.1	Enabling or disabling TOE encryption of wireless traffic	The identity of the Administrator performing the function
FDP_RIP.1a	None	None
FPT_RVM.1a	None	None
FPT_SEP.1a	None	None
FPT_STM_EXP.1a	Changes to the time	None
FPT_TST_EXP.1	Execution of self test	Success or failure of the test
FPT_TST_EXP.2	Execution of self test	Success or failure of the test
FMT_MOF.1a	Changing the TOE encryption algorithm including the selection not to encrypt communications	Encryption algorithm selected (or none)
FMT_MOF.1b	Start or Stop of audit record generation	None
FMT_MOF.1c	Changes to the TOE remote authentication settings; Changes to the session lock timeframe	The identity of the Administrator performing the function
FMT_MOF.1d	None	None
FMT_MSA.2	All offered and rejected values for security attributes	None
FMT_MTD.1a	Changes to the set of rules used to pre-select audit events	None
FMT_MTD.1b	Changing the TOE authentication credentials	None – the TOE **SHALL NOT** record authentication credentials in the audit log
FMT_MTD.1c	Changing the TOE authentication credentials	None – the TOE **SHALL NOT** record authentication credentials in the audit log
FMT_SMF.1a	Use of the management functions	None
FMT_SMF.1b	Use of the management functions	None

Requirement	Auditable Events	Additional Audit Record Contents
FMT_SMF.1c	Use of the management functions	None
FMT_SMF.1d	Use of the management functions	None
FMT_SMF.1e	Use of the management functions	None
FMT_SMR.1a	Modifications to the group of users that are part of a role	None
FTP_ITC_EXP.1a	Initiation/Closure of a trusted channel	Identification of the remote entity with which the channel was attempted/created; Success or failure of the event
FTP_TRP.1a	Failure of the trusted path function	None
FTP_TRP.1b	Failure of the trusted path function	None

Application Note: For FTA_SSL.3, wireless user inactivity timeouts are logged. However, inactivity timeouts of the the Web UI and CLI management interfaces are not logged. The most frequent use management interfaces is assumed to be monitoring of the TOE. Monitoring would be performed using the autorefreshed screens of the Web UI, which are not subject to an inactivity timeout. Configuration of the TOE would only be performed by exception. Inactivity timeouts of the management interfaces are therefore not relevant to the normal usage of those interfaces.

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

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, *[information specified in column three of* Table 5-3*]*.

Application note: subject identity is defined as follows. For identified users, the subject identity is represented by the user name. For non-identified subjects, the subject identity is represented by the IP address for wired network subjects, and by the MAC address for wireless network subjects.

5.1.1.4 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.

5.1.1.5 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.

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.).

5.1.2 Identification and authentication

5.1.2.1 FIA_UAU.1a Timing of authentication

FIA_UAU.1.1a The TSF shall allow *[identification as stated in FIA_UID.2a]* on behalf of the user to be performed before the user is authenticated.

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

5.1.2.2 FIA_UAU_EXP.5a Multiple authentication mechanisms

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

FIA_UAU_EXP.5.2a The TSF shall, at the option of the administrator, invoke the remote authentication mechanism for administrators and wireless LAN users.

Application note: Wireless users use an external RADIUS authentication mechanism. Remote administrators are authenticated initially as wired users using the external RADIUS server and then as management users using an internal authentication database. Local administrators are authenticated as management users using the internal authentication database.

Application note: Authentication of management users using the internal authentication database uses a username and password. Authentication of wired users using the RADIUS authentication server uses a username and password. Authentication of wireless users using the RADIUS authentication server may support the PEAP and EAP-TTLS protocols which provide password-based authentication, and the EAP-TLS protocol, which uses client-side certificate authentication in conjunction with a list of trusted certification authorities installed on the authentication server. A client-side certificate used in EAP-TLS contains the username. Configuration of the particular authentication protocol (EAP-TLS, EAP-TTLS, and PEAP) is performed on the RADIUS server. The authentication protocol is transparent to the TOE. The TOE simply passes the authentication protocol messages between the remote administrator or wireless client and the RADIUS server. Additionally, wireless users may authenticate using an open connection with a VPN between the wireless client and mobility controller. In this case the wireless users authenticate using the RADIUS authentication server using a username and password.

5.1.2.3 FIA_UID.2a User identification before any action

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

5.1.2.4 FIA_ATD.1a Administrator attribute definition

FIA_ATD.1.1a The TSF shall maintain the following ***minimum*** list of security attributes belonging to individual ***administrators***: *[password, username]*.

5.1.2.5 FIA_ATD.1b User attribute definition

FIA_ATD.1.1b The TSF shall maintain the following ***minimum*** list of security attributes belonging to individual ***remotely authenticated users***: *[session key, role]*.

5.1.2.6 FIA_USB.1 User-subject binding

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

FIA_USB.1.1 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: *[none]*.

FIA_USB.1.1 The TSF shall enforce the following rules governing changes to the user security attributes associated with the subjects acting on the behalf of users: *[none]*.

5.1.3 TOE Access

5.1.3.1 FTA_SSL.3 TSF-initiated termination

FTA_SSL.3a TSF-initiated termination (wireless user)

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

Application note: The mobility controller assesses user inactivity as the cessation of network traffic arriving from the wireless client. It should be noted that processes acting on behalf of the user may send protocol network packets to the mobility controller, even when the user is not interacting directly, e.g. pressing keys.

FTA_SSL.3b TSF-initiated termination (Command Line Interface)

FTA_SSL.3.1b The TSF shall terminate a **Command Line Interface** interactive session after **an** [administrator configurable time interval of user inactivity].

Application note: The Command Line Interface (CLI) is accessed by local administrators and remote administrators. A local administrator authenticates to the CLI as a management user and accesses the CLI directly via the serial port. Following initial authentication as a privileged wired user, a remote administrator authenticates to the CLI as a management user and accesses the CLI via the wired network. After the configured period of inactivity for the CLI, the management user session of the local administrator or remote administrator is terminated.

FTA_SSL.3c TSF-initiated termination (Web User Interface)

FTA_SSL.3.1c The TSF shall terminate a **Web User Interface** interactive session after a [30 minute period of user inactivity].

Application note: The Web User Interface (Web UI) is accessed by remote administrators. Following initial authentication as a privileged wired user, a remote administrator authenticates to the Web UI as a management user and accesses the Web UI via the wired network. After a 30 minute period of inactivity, the management user session of the remote administrator is terminated. Timeout does not apply to the following screens which are autorefreshed.

5.1.3.2 FTA_TAB.1 Default TOE access banners

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

Application note: In accordance with O.BANNER, the PP requires an access banner to be displayed only for an administrator.

5.1.4 Cryptographic Support

Application note: PP SFR component FCS_BCM_EXP.1 is addressed within TOE SFR components FCS_CKM.1a, FCS_CKM_EXP.2, FCS_CKM.4a and FCS_COP.1a. PP SFR components FCS_COP_EXP.1 and FCS_COP_EXP.2 are addressed within TOE SFR component FCS_COP.1a.

5.1.4.1 FCS_CKM.1a Cryptographic key generation

FCS_CKM.1.1a The TSF shall **use services of a FIPS 140-2 validated cryptographic module to** generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *[listed in Table 5-4 Cryptographic Operation]* and specified cryptographic key sizes *[identified in Table 5-4 Cryptographic Operation]* that meet the following: *[requirements of the standards identified in Table 5-4 Cryptographic Operation]*.

Application note: Cryptographic Module Security Policy [2] was prepared as a part of the FIPS 140-2 Level 2 validation of the Aruba 6000 and 800 series Mobility Controllers. Aruba 6000 and 800 series Mobility Controller Certificate #649 and validation information can be found at : <http://csrc.nist.gov/cryptval/140-1/1401val2006.htm#649>

5.1.4.2 FCS_CKM.2a Cryptographic key distribution

FCS_CKM.2.1a The TSF shall ***use services of a FIPS 140-2 validated cryptographic module to*** distribute cryptographic keys in accordance with a specified cryptographic key distribution method *[Diffie-Hellman key agreement (RFC 2631), RSA PKCS #1 key wrapping]* that meets the following: *[key distribution requirements of the FIPS 140-2 standard]*.

Application note: Cryptographic Module Security Policy [2] was prepared as a part of the FIPS 140-2 Level 2 validation of the Aruba 6000 and 800 series Mobility Controllers. Aruba 6000 and 800 series Mobility Controller Certificate #649 and validation information can be found at : <http://csrc.nist.gov/cryptval/140-1/1401val2006.htm#649>

5.1.4.3 FCS_CKM_EXP.2 Cryptographic key establishment

FCS_CKM_EXP.2.1 The TSF shall ***use services of a FIPS 140-2 validated cryptographic module to*** provide the following cryptographic key establishment technique: Cryptographic Key Establishment using Manual Loading. The cryptomodule shall be able to accept keys as input and be able to output keys in the following circumstances *[none]* in accordance with a specified manual cryptographic key distribution method using FIPS-approved Key Management techniques that meets the FIPS 140-***2*** Key Management Security Levels ***2***, Key Entry and Output.

5.1.4.4 FCS_CKM.4a Cryptographic key destruction

FCS_CKM.4.1a The TSF shall ***use services of a FIPS 140-2 validated cryptographic module to*** destroy cryptographic keys in accordance with a ~~specified cryptographic key destruction method~~ *cryptographic key zeroization method* that meets the following:

- ***Key zeroization requirements of the FIPS 140-2 standard***
- *Zeroization of all private cryptographic keys, plaintext cryptographic keys, key data, and all other critical cryptographic security parameters shall be immediate and complete*
- *The zeroization shall be executed by overwriting the key/critical cryptographic security parameter storage area three or more times with an alternating pattern*
- *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: Cryptographic Module Security Policy [2] was prepared as a part of the FIPS 140-2 Level 2 validation of the Aruba 6000 and 800 series Mobility Controllers. Aruba 6000 and 800 series Mobility Controller Certificate #649 and validation information an be found at : <http://csrc.nist.gov/cryptval/140-1/1401val2006.htm#649>

5.1.4.5 FCS_COP.1a Cryptographic operation

FCS_COP.1.1a The TSF shall ***use services of a FIPS 140-2 validated cryptographic module to*** perform *[cryptographic operations listed in the Table 5-4 Cryptographic Operation]* in accordance with a specified cryptographic algorithm *[listed in the Table 5-4 Cryptographic Operation]* and cryptographic key sizes *[identified in Table 5-4 Cryptographic Operation]* that meet the following: *[requirements of the standards listed in the Table 5-4 Cryptographic Operation]*.

Table 5-4 Cryptographic Operation

Cryptographic operations	Cryptographic algorithm	Key sizes (bits)	Standards	Certificate number
Encryption/decryption of the network traffic	AES–CBC	128, 192, 256	Advanced Encryption Standard (AES) (FIPS PUB 197)	159, 315
	AES-CCM	128	AES-CCM Special Publication 800-38C	4
	Triple DES-CBC	168	ANSI X9.52 Data Encryption Standard (DES), (FIPS PUB 46-3)	261 and 382
Secure Hash	SHA-1	N/A	Secure Hash Standard (SHS) (FIPS PUB 180-2	244 and 386

Cryptographic operations	Cryptographic algorithm	Key sizes (bits)	Standards	Certificate number
Data authentication and verification.	HMAC SHA-1	128, 160	Keyed-Hash Message Authentication Code (HMAC) (FIPS PUB 198)	116 and 118
Key wrapping using asymmetric keys (encryption/decryption)	RSA PKCS #1	1024	RSA PKCS #1	101, 102
Digital signature generation/verification				
Random data generation and key generation	ANSI X9.31 PRNG	64	ANSI X9.31	135
Key agreement	Diffie-Hellman	1024	RFC 2631	vendor affirmed

Application note:

- *AES is used for encryption/decryption of secure WLAN traffic (xSec and 802.11i protocols), IPSec/IKE traffic, SSH traffic and TLS traffic.*
- *SHA-1 and HMAC SHA-1 are used for data authentication in xSec, IPSec/IKE, SSH and TLS, and as a part of the RSA PKCS #1 signature algorithm.*
- *Triple DES is used for encryption/decryption of secure IPSec/IKE traffic, SSH traffic, TLS traffic, and as an internal algorithm of ANSI X9.31 PRNG for random data generation and key generation.*
- *RSA PKCS #1 is used for encryption/decryption of the shared secret during TLS handshake as well as for signature generation/verification during SSH and TLS handshakes.*
- *PRNG (ANSI X9.31) is used to generate random data and cryptographic keys for xSec, 802.11i, TLS, SSH and IPSec/IKE.*

5.1.5 User Data Protection

5.1.5.1 FDP_PUD_EXP.1 Protection of User Data

FDP_PUD_EXP.1.1 When the administrator has enabled encryption, the TSF shall:

a) encrypt authenticated user data transmitted to a wireless client using the cryptographic algorithm(s) specified in FCS_COP.1a;

b) decrypt authenticated user data received from a wireless client using the cryptographic algorithm(s) specified in FCS_COP.1a.

Application Note:

- *Where wireless user authentication uses 802.11i, the TOE encrypts wireless user data using xSec or 802.11i security protocols. xSec and 802.11i protocols operate at the link layer (Layer 2) level. Once the wireless user is authenticated, and an xSec or 802.11i encrypted connection between the TOE*

and the wireless user is established, the wireless user has an option to use IPSec/IKE Layer 3 encryption protocol as an additional security measure on top of xSec/802.11i protocols. For the IPSec/IKE protocol only pre-shared keys are supported, the RSA digital signatures option of IPSec/IKE is not supported.

- *Where wireless user authentication does not use 802.11i, but uses an open system connection, an IPSec/IKE VPN using a pre-shared key is set up between the wireless user and the TOE prior to user authentication. The VPN protects both the authentication and subsequent user data transmissions.*

5.1.5.2 FDP_RIP.1a Subset residual information protection

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

5.1.6 Protection of the TSF

5.1.6.1 FPT_RVM.1a Non-bypassability of the TSP

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

5.1.6.2 FPT_SEP.1a TSF domain separation

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

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

5.1.6.3 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 source,*** for its own use.

Application Note: The TOE obtains time stamps via an NTP server.

5.1.6.4 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 msgs, logs, custom banners, rf plan data.

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.

5.1.6.5 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-***2*** ***validated cryptographic module*** during initial start-up (power on) and upon request, to demonstrate the correct operation of the cryptographic components of the TSF.

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

5.1.7 Security Management

5.1.7.1 FMT_MOF.1a Management of cryptographic security functions behavior

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

- *Crypto: load 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].

5.1.7.2 FMT_MOF.1b Management of audit security functions behavior

FMT_MOF.1.1b 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].

5.1.7.3 FMT_MOF.1c Management of authentication security functions behavior

FMT_MOF.1.1c 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 length of time a session may remain inactive before it is terminated]*

to [administrators].

5.1.7.4 FMT_MOF.1d Management of Wireless Intrusion Protection security functions behavior

FMT_MOF.1.1d The TSF shall restrict the ability to determine the behavior of, enable, disable, and modify the behavior of the functions *[*

- *WIP: signature events (wireless intrusion profiles)*
- *WIP: actions to be taken upon detection of a potential security violation]*

to [administrators].

5.1.7.5 FMT_MSA.2 Secure security attributes

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

Application Note: FMT_MSA.2 was included to meet dependencies in cryptography-related requirements FCS_CKM.1, FCS_CKM.2, FCS_CKM.4 and FCS_COP.1. The security attributes are cryptographic key values. Cryptographic keys are considered secure if generated, distributed and managed by a FIPS 140-2 validated cryptographic module.

5.1.7.6 FMT_MTD.1a Management of Audit pre-selection data

FMT_MTD.1.1a The TSF shall restrict the ability to **query, modify, clear, *[****create****]*** the *[set of rules used to pre-select audit events]* to *[administrators]*.

5.1.7.7 FMT_MTD.1b Management of Authentication data (Administrator)

FMT_MTD.1.1b The TSF shall restrict the ability to **query, modify, delete, clear, *[****create****]*** the *[authentication credentials, user identification credentials]* to *[administrators]*.

Application Note:FMT_MTD.1b applies to user profiles and passwords held in the internal TOE database for use by the TOE username and password based authentication mechanism. Management of authentication data used by the external RADIUS server is managed externally.

5.1.7.8 FMT_MTD.1c Management of Authentication data (User)

FMT_MTD.1.1c The TSF shall restrict the ability to **modify** the *[user authentication credentials]* to *[TOE users]*.

Application Note:FMT_MTD.1c applies to passwords held in the internal TOE database for use by the TOE username and password based authentication mechanism. Management of authentication data used by the external RADIUS server is managed externally. FMT_SMF.1e provides the capability for administrators to modify the user authentication credentials.

5.1.7.9 FMT_SMF.1a Specification of Management Functions (Cryptographic Function)

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

5.1.7.10 FMT_SMF.1b Specification of Management Functions (TOE Audit Record Generation)

FMT_SMF.1.1b The TSF shall be capable of performing the following security management functions: *[query, enable or disable Security Audit]*.

5.1.7.11 FMT_SMF.1c Specification of Management Functions (Cryptographic Key Data)

FMT_SMF.1.1c 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]*.

5.1.7.12 FMT_SMF.1d Specification of Management Functions (Wireless Intrusion Protection)

FMT_SMF.1.1d The TSF shall be capable of performing the following security management functions: *[determine the behavior of, enable, disable, and modify the behavior of WIP signature events and actions in support of FAU_SAA.3 and FAU_ARP.1]*.

5.1.7.13 FMT_SMF.1e Specification of Management Functions (TOE Authentication Data)

FMT_SMF.1.1e The TSF shall be capable of performing the following security management functions: *[query, modify, delete, clear and create the administrator identification and authentication credentials, modify the user authentication credentials]*.

5.1.7.14 FMT_SMR.1a Security roles

FMT_SMR.1.1a The TSF shall maintain the roles *[administrator and wireless user roles]*.

FMT_SMR.1.2a The TSF shall be able to associate users with roles.

Application Note: The administrator role is used to administer the TOE using management interfaces. User roles correspond to wireless users that utilize TOE wireless security protocol processing and VPN server functionalities. The TOE permits creation of multiple wireless user roles.

5.1.8 Trusted path/channels

5.1.8.1 FTP_ITC_EXP.1a Inter-TSF trusted channel

FTP_ITC_EXP.1.1a The ***TOE*** ~~TSF~~ shall provide ***an encrypted*** ~~a~~ communication channel between itself and ***entities in the TOE IT Environment*** ~~a remote trusted IT product~~ 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.1.2a The TSF shall permit **the TSF**, ***or the IT Environment entities*** to initiate communication via the trusted channel.

FTP_ITC_EXP.1.3a The TSF shall initiate communication via the trusted channel for **[***all authentication functions, remote logging, time***]**.

Application Note: The trusted channel is based on the IPSec/IKE protocol with pre-shared keys.

5.1.8.2 FTP_TRP.1a Trusted path (remote administrators)

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

FTP_TRP.1.2a The TSF shall permit ***remote administrator client devices*** to initiate communication via the trusted path.

FTP_TRP.1.3a The TSF shall require the use of the trusted path for ***remote administrator user authentication***.

Application Note: The TOE provides a TLS based trusted path from the remote administrator to the TOE for authentication as a wired user against the external RADIUS authentication server using a username and password.

5.1.8.3 FTP_TRP.1b Trusted path (wireless users)

FTP_TRP.1.1a 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.1.2a The TSF shall permit ***wireless client devices*** to initiate communication via the trusted path.

FTP_TRP.1.3a The TSF shall require the use of the trusted path for ***wireless user authentication***.

Application Note: This SFR applies to the authentication of wireless users using an open system connection. In this case, an IPSec/IKE VPN using a pre-shared key is set up between the wireless user and the TOE prior to user authentication to the external RADIUS server using a username and password. The VPN protects the user authentication.

Application Note: As specified in the requirement FTP_TRP.1c for the IT Environment, the authentication server establishes a trusted path between the authentication server and the wireless client which passes through the TOE. This trusted path is used for wireless user authentication during EAP-TLS, EAP-TTLS or PEAP authentication phase.

5.2 Security Requirements for the IT Environment.

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

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

In support of the authentication server, the environment shall provide implementations of the wireless user authentication protocols as well as facilities to manage and protect authentication information.

The communications between the TOE and audit/time/authentication servers will be protected. In addition, the TOE IT environment is responsible for protecting itself and ensuring that its security mechanisms cannot be bypassed.

The TOE security functional requirements are listed in Table 5-5 Functional Components.

Table 5-5 Functional Components

Item	Component	Component Name	PP Conformance
1	FAU_GEN.1b	Audit data generation	PP Tailored
2	FAU_SAR.1	Audit review	PP
3	FAU_SAR.2	Restricted audit review	PP
4	FAU_SAR.3	Selectable audit review	PP Tailored
5	FAU_STG.1	Protected audit trail storage	PP
6	FAU_STG.3	Action in case of possible audit data loss	PP Tailored
7	FIA_UAU_EXP.5b	Remote authentication mechanism	PP Tailored
8	FIA_UID.2b	User identification before any action	PP
9	FIA_AFL.1	Remote user authentication failure handling	PP Tailored
10	FIA_ATD.1c	User attribute definition	PP Tailored
11	FCS_CKM.1b	Cryptographic key generation	Additional
12	FCS_CKM.2b	Cryptographic key distribution	Additional
13	FCS_CKM.4b	Cryptographic key destruction	Additional
14	FCS_COP.1b	Cryptographic operation	Additional
15	FDP_RIP.1b	Subset Residual Information Protection	PP
16	FPT_RVM.1b	Non-bypassability of the TSP	PP
17	FPT_SEP.1b	TSF domain separation	PP
18	FPT_STM.1	Reliable time stamps	PP
19	FMT_MOF.1e	Management of security functions behavior	PP
20	FMT_MTD.1d	Management of TSF data	PP Tailored
21	FMT_SMF.1f	Specification of Management Functions	Additional
22	FMT_SMR.1b	Security roles	PP
23	FTP_ITC_EXP.1b	Inter-TSF trusted channel	PP Tailored
24	FTP_TRP.1c	Trusted path	Additional

5.2.1 Security Audit

5.2.1.1 FAU_GEN.1b Audit data generation

FAU_GEN.1.1b The ***TOE IT Environment*** ~~TSF~~ shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;
b) All auditable events for the [**not specified**] level of audit; and
c) *[the following events: events specified in column two of Table 5-6 TOE IT Environment Auditable Events].*

Table 5-6 TOE IT Environment Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1b	None	None
FAU_SAR.1	None	None
FAU_SAR.2	Unsuccessful attempt to read 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
FIA_UAU_EXP.5b	Use of the authentication mechanism (success or failure)	User identity – the TOE **SHALL NOT** record invalid passwords in the audit log
FIA_UID.2b	None	None
FIA_ATD.1c	None	None
FCS_CKM.1b	Success or failure of key generation	None
FCS_CKM.2b	Success or failure of key distribution	None
FCS_CKM.4b	Destruction of a cryptographic key	The identity of the Administrator performing the function
FCS_COP.1b	Success or failure of operation	Type of cryptographic operation
FDP_RIP.1b	None	None

Requirement	Auditable Events	Additional Audit Record Contents
FPT_RVM.1b	None	None
FPT_SEP.1b	None	None
FPT_STM.1	Setting time/date	Identity of the administrator that performed the action
FMT_MOF.1e	Changes to audit server settings Changes to authentication server settings Changes to time server settings	None
FMT_MTD.1d	Changes to TSF data	None
FMT_SMF.1f	Use of the management functions	None
FMT_SMR.1b	None	None
FTP_ITC_EXP.1b	Initiation/Closure of a trusted channel	Identification of the remote entity with which the channel was attempted/created; Success or failure of the event
FTP_TRP.1c	Failure of the trusted path function	None

FAU_GEN.1.2b 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, 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 5-6 TOE IT Environment Auditable Events]*.

Application note: for the TOE environment the subject identity is defined as follows. For the audit server and authentication server administrators the subject identity is represented by the user name of the administrator. For wired network subjects the subject identity is represented by the IP address of the subject.

5.2.1.2 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.

5.2.1.3 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.

5.2.1.4 FAU_SAR.3 Selectable audit review

FAU_SAR.3.1 The ***TOE IT Environment*** ~~TSF~~ shall provide the ability to perform **searches, sorting** of audit data based on *[subject identity, event type, event date and time, device interface and wireless client identity]*.

5.2.1.5 FAU_STG.1 Protected audit trail storage

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

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

5.2.1.6 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]* if the audit trail exceeds *[an administrator-settable percentage of storage capacity]*.

5.2.2 User Data Protection

5.2.2.1 FDP_RIP.1b Subset residual information protection

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

5.2.3 Identification and authentication

5.2.3.1 FIA_UAU_EXP.5b Remote authentication mechanism

FIA_UAU_EXP.5.1b The ***TOE IT Environment*** ~~TSF~~ shall provide a remote authentication mechanism to **provide TOE remote** user authentication.

FIA_UAU_EXP.5.2b The ***TOE IT Environment*** ~~TSF~~ shall authenticate any user's claimed identity according to the *EAP-TLS, EAP-TTLS or PEAP authentication mechanisms or username/password, according to the authentication mechanism in use.*

Application Note: EAP-TLS, EAP-TTLS and PEAP are used for wireless users. If authentication is successful, the IT Environment (authentication server) communicates to the TOE the wireless user role and the session key derived during the EAP-TLS/EAP-TTLS/PEAP protocol handshake. If authentication fails, the IT environment reports the authentication failure to the TOE. Additionally, wireless users may authenticate using

an open system connection, in which case a username and password is used. Remote administrators authenticate initially as wired users using a username and password.

5.2.3.2 FIA_UID.2b User identification before any action

FIA_UID.2.1b The ***TOE IT Environment*** ~~TSF~~ shall require each ***TOE remote*** user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.2.3.3 FIA_AFL.1 Remote user authentication failure handling

FIA_AFL.1.1 The **TOE IT Environment** shall detect when **an administrator configurable positive integer within** *[a range from 1 to 65536]* unsuccessful authentication attempts occur related to *[remote user authentication attempts]*.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the **TOE IT Environment** shall *[disable the remote user access]*.

5.2.3.4 FIA_ATD.1c User attribute definition

FIA_ATD.1.1c 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*, *role]*.

Application Note: The TOE maintains a set of user roles. The authentication server maintains a role attribute for each user. This attribute is provided to the TOE after the user is successfully authenticated.

5.2.4 Cryptographic Support

5.2.4.1 FCS_CKM.1b Cryptographic key generation

FCS_CKM.1.1bThe ***TOE IT Environment*** ~~TSF~~ shall ***use services of a FIPS 140-2 validated cryptographic module to*** generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *[listed in Table 5-7 IT Environment Cryptographic Operation]* and specified cryptographic key sizes *[identified in Table 5-7 IT Environment Cryptographic Operation]* that meet the following: *[requirements of the standards identified in Table 5-7 IT Environment Cryptographic Operation]*.

5.2.4.2 FCS_CKM.2b Cryptographic key distribution

FCS_CKM.2.1b The ***TOE IT Environment*** ~~TSF~~ shall ***use services of a FIPS 140-2 validated cryptographic module to*** distribute cryptographic keys in accordance with a specified cryptographic key distribution method *[Diffie-Hellman key agreement (RFC 2631), RSA PKCS #1 key wrapping]* that meets the following: *[key distribution requirements of the FIPS 140-2 standard]*.

5.2.4.3 FCS_CKM.4b Cryptographic key destruction

FCS_CKM.4.1b The ***TOE IT Environment*** ~~TSF~~ shall ***use services of a FIPS 140-2 validated cryptographic module to*** destroy cryptographic keys in accordance with a specified

cryptographic key destruction method *[zeroization upon issuance of the key zeroization command]* that meets the following: *[key zeroization requirements of the FIPS 140-2 standard]*.

5.2.4.4 FCS_COP.1b Cryptographic operation

FCS_COP.1.1b The ***TOE IT Environment*** ~~TSF~~ shall ***use services of a FIPS 140-2 validated cryptographic module to*** perform *[cryptographic operations listed in the Table 5-7 IT Environment Cryptographic Operation]* in accordance with a specified cryptographic algorithm *[listed in the Table 5-7 IT Environment Cryptographic Operation]* and cryptographic key sizes *[identified in Table 5-7 IT Environment Cryptographic Operation]* that meet the following: *[requirements of the standards listed in the Table 5-7 IT Environment Cryptographic Operation]*.

Table 5-7 IT Environment Cryptographic Operation

Cryptographic operations	Cryptographic algorithm	Key sizes (bits)	Standards
Encryption/decryption	AES–CBC	128, 192, 256	Advanced Encryption Standard (AES) (FIPS PUB 197)
	Triple DES-CBC	168	ANSI X9.52 Data Encryption Standard (DES), (FIPS PUB 46-3)
Secure Hash in	SHA-1	N/A	Secure Hash Standard (SHS) (FIPS PUB 180-2)
Data authentication and verification	HMAC SHA-1	128, 160	Keyed-Hash Message Authentication Code (HMAC) (FIPS PUB 198)
Key wrapping using asymmetric keys (encryption/decryption)	RSA PKCS #1	1024	RSA PKCS #1
Digital signature generation/verification			
Random data generation and key generation	Any FIPS-approved PRNG	n/a	n/a
Key agreement	Diffie-Hellman	1024	RFC 2631

Application note:

- *The IT environment uses cryptographic algorithms to establish IPSec/IKE trusted channels between the TOE and audit/authentication servers. Cryptographic algorithms are also used in EAP-TLS, EAP-TTLS and PEAP wireless user authentication protocols implemented by the authentication server.*
- *The IT environment may support a reduced set of cryptographic algorithms, therefore, not all algorithm options of IPSec/IKE, EAP-TLS, EAP-TTLS and PEAP protocols may be available. It is required to support at least one algorithm/key size combination for IPSec/IKE and the authentication protocols.*
- *AES, Triple-DES, Diffie-Hellman, SHA-1 and HMAC SHA-1 are used in IPSec/IKE, EAP-TLS, EAP-TTLS and PEAP*
- *RSA is used in EAP-TLS, EAP-TTLS and PEAP*

- *A FIPS-approved PRNG shall be used by the IT environment for random data generation and key generation purposes.*

5.2.5 Protection of the TSF

5.2.5.1 FPT_RVM.1b Non-bypassability of the TOE IT Environment Security Policy

FPT_RVM.1.1b 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.

5.2.5.2 FPT_SEP.1b TOE IT Environment domain separation

FPT_SEP.1.1b 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.1.2b The ***TOE IT Environment*** ~~TSF~~ shall enforce separation between the security domains of subjects in the ***IT environmental scope of control*** ~~TSC~~.

5.2.5.3 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.

5.2.6 Security Management

5.2.6.1 FMT_MOF.1e Management of security functions behavior

FMT_MOF.1.1e The ***TOE IT Environment*** ~~TSF~~ shall restrict the ability to **determine the behavior of** the functions *[audit, remote authentication, time service]* to *[the administrator]*.

5.2.6.2 FMT_MTD.1d Management of TSF data

FMT_MTD.1.1d The ***TOE IT Environment*** ~~TSF~~ shall restrict the ability to **modify, set initial value of** the *[date and time used for time stamps in FPT_STM.1b, user names, user passwords, user roles, EAP-TLS/EAP-TTLS/PEAP server certificates, list of trusted certificate authorities for EAP-TLS client certificates, IPSec/IKE pre-shared keys used for trusted channel]* to *[the administrator]*.

5.2.6.3 FMT_SMF.1f Specification of Management Functions

FMT_SMF.1.1f The ***TOE IT Environment*** ~~TSF~~ shall be capable of performing the following security management functions: *[as specified in FMT_MOF.1e, FMT_MTD.1d]*.

5.2.6.4 FMT_SMR.1b Security roles

FMT_SMR.1.1b The ***TOE IT Environment*** ~~TSF~~ shall maintain the roles *[administrator]*.

FMT_SMR.1.2b 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.

5.2.7 Trusted path/channels

5.2.7.1 FTP_ITC_EXP.1b Inter-TSF trusted channel

FTP_ITC_EXP.1.1b The ***TOE IT Environment*** ~~TSF~~ shall provide ***an encrypted*** ~~a~~ communication channel between itself ***and the TOE*** ~~a remote trusted IT product~~ 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.1.2b 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.1.3b The ***TOE IT Environment*** ~~TSF~~ shall initiate communication via the trusted channel for **all authentication functions***,* **remote logging, time**.

Application Note: The trusted channel is based on the IPSec/IKE protocol with pre-shared keys.

5.2.7.2 FTP_TRP.1c Trusted path

FTP_TRP.1.1c The ***TOE IT Environment*** ~~TSF~~ shall provide a communication path between itself and ***remote*** users ***passing through the TOE*** 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.1.2c The TSF shall permit ***remote users*** to initiate communication via the trusted path.

FTP_TRP.1.3c The TSF shall require the use of the trusted path for [**wireless user authentication using EAP-TLS, EAP-TTLS, or PEAP protocols**].

Application Note: When a wireless client connects to the TOE, the wireless client establishes a connection to the authentication server through the TOE in such a way that the TOE passes EAP-TLS, EAP-TTLS or PEAP protocol messages between the client and the authentication server. The authentication server establishes an EAP-TLS, EAP-TTLS or PEAP-based trusted path to the wireless user, which is used for authentication. Once the wireless user is authenticated, the authentication server passes to the TOE a session key which was derived during the EAP-TLS, EAP-TTLS or PEAP handshake. The session key is then used by the TOE to establish an encrypted data connection with the wireless client using the 802.11i or xSec protocol. The authentication server also passes to the TOE the wireless user role attribute.

5.3 TOE Security Assurance Requirements

The Security Assurance Requirements for the TOE are the assurance components of Evaluation Assurance Level 2 (EAL2) taken from Part 3 of the Common Criteria, augmented with ACM_SCP.1 (CM Coverage), ALC_FLR.2 (Flaw Remediation) and AVA_MSU.1 (Misuse – Examination of guidance). None of the assurance components are refined. The assurance components are listed in Table 5-8 TOE Assurance Components below.

Table 5-8 TOE Assurance Components

Assurance class	Assurance components
Configuration management	ACM_CAP.2 Configuration items ACM_SCP.1 TOE CM Coverage
Delivery and operation	ADO_DEL.1 Delivery procedures
	ADO_IGS.1 Installation, generation, and start-up procedures
Development	ADV_FSP.1 Informal functional specification
	ADV_HLD.1 Descriptive high-level design
	ADV_RCR.1 Informal correspondence demonstration
Guidance documents	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
Life-Cycle Support	ALC_FLR.2 Flaw Reporting Procedures
Tests	ATE_COV.1 Analysis of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
Vulnerability assessment	AVA_MSU.1 Examination of guidance
	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.1 Developer vulnerability analysis

Further information on these assurance components can be found in the Common Criteria for Information Technology Security Evaluation Part 3.

5.4 Strength of Function

The overall strength of function requirements claim for all of these IT security functions is SOF-basic.

Note: the SOF claim does not apply to the strength of cryptographic algorithm implementations, which is outside the scope of the CC.

FIA_UAU.1a includes the following probabilistic/permutational mechanisms for which specific SOF metrics are appropriate: password-based authentication of users.

FDP_PUD_EXP.1 and FTP_ITC_EXP.1a include the following probabilistic/permutational mechanisms for which specific SOF metrics are appropriate: a pre-shared key is used in the IPSec/IKE protocol.

6 TOE Summary Specification

6.1 IT Security Functions

Section 6.1 describes the specific security functions that are implemented by the TOE.

The following sections describe the IT Security Functions of the Aruba 6000 and Aruba 800 series Mobility Controller. This section includes a bi-directional mapping between functions and requirements that clearly shows which functions satisfy which requirements and that all requirements are met.

Table 6-1 Security Functional Requirements mapped to Security Functions

Security Class	SFR	Sub-function	Security function
Security audit	FAU_ARP.1	WIP-1	Wireless Intrusion Protection
	FAU_SAA.3	WIP-1	
	FAU_GEN.1a	SA-1	Auditing
	FAU_GEN.2	SA-2	
	FAU_SEL.1	SA-3	
TOE access	FTA_SSL.3	TA-1	I&A and TOE access
	FTA_TAB.1	TA-2	
Identification and authentication	FIA_UAU.1a FIA_UAU_EXP.5a	IA-1	
	FIA_UID.2a	IA-2	
	FIA_ATD.1a FIA_ATD.1b	IA-4	
	FIA_USB.1	IA-5	
Cryptographic support	FCS_CKM.1a	CY-1	Cryptography
	FCS_CKM.2a FCS_CKM_EXP.2	CY-2	
	FCS_CKM.4a	CY-3	
	FCS_COP.1a	CY-4	
User data protection			User Data and TSF Protection

	FDP_PUD_EXP.1 FDP_RIP.1a	UDP-1 UDP-2	
Protection of the TSF	FPT_RVM.1a FPT_SEP.1a	PT-1	
	FPT_STM_EXP.1 FPT_TST_EXP.1 FPT_TST_EXP.2	PT-2 PT-3 PT-4	
Security management	FMT_SMF.1a FMT_SMF.1b FMT_SMF.1c FMT_SMF.1d FMT_SMF.1e	SM-2 SM-2, SM-4	Security Management
	FMT_SMR.1a	SM-1	
	FMT_MOF.1a FMT_MOF.1b FMT_MOF.1c FMT_MOF.1d	SM-1, SM-2	
	FMT_MSA.2	SM-3	
	FMT_MTD.1a FMT_MTD.1b FMT_MTD.1c	SM-2, SM-4	
Trusted path/channels	FTP_TRP.1a FTP_TRP.1b FTP_ITC_EXP.1a	TP-1 TP-2	Trusted Path/Channels

6.1.1 Wireless Intrusion Protection

Wireless Intrusion Protection (WIP) involves analysis of wired and wireless traffic to detect anomalous activity, based on a variety of information including the configuration of valid APs and the characteristics of received wireless frames. The administrator can configure the Aruba Mobility Controller to detect and, where possible, protect the managed networks from specific types of network intrusion attacks.

WIP-1 The Aruba Mobility Controller can be configured to detect and, where possible, protect the managed networks from the following types of network intrusion attacks:

Rogue AP, using the Configuration-> WLAN Intrusion Detection-> Rogue AP panel of the Web UI

Denial of Service, using the Configuration-> WLAN Intrusion Detection-> Denial of Service panel of the Web UI, including:
- Rate Analysis

Man-in-the-Middle, using the Configuration-> WLAN Intrusion Detection-> Man-in-the-Middle panel of the Web UI, including:
- MAC Spoofing
- Station Disconnection Detection
- EAP Handshake Analysis
- Sequence Number Analysis

Signature Detection, using the Configuration-> WLAN Intrusion Detection-> Signatures panel of the Web UI, including:
- Null-Probe-Response
- AirJack
- NetStumbler Generic
- NetStumbler Version 3.3.0x
- Deauth-Broadcast

WLAN Policies, using the Configuration-> WLAN Intrusion Detection-> Policies panel of the Web UI, including:

- Misconfigured AP Protection.

6.1.2 Auditing

Auditing involves recognizing, recording, storing, and analyzing information related to security relevant events. The resulting audit records can be examined to determine which security relevant events took place and which subject is responsible for them.

The Aruba Mobility Controller uses a logging level that can be set for each of the modules of the ArubaOS. The administrator can configure the logging levels for each of these modules. There are a total of eight BSD syslog logging levels:

Emergency - Panic conditions that occur when the system becomes unstable.

Alert - Any condition requiring immediate attention and correction.

Critical - Any critical conditions such as, physical memory errors.

Errors - Error conditions.

Warning - Warning messages.

Notice - Significant events of non-critical and normal nature.

Informational - Messages of general interest to system users.

Debug - Messages containing information useful for debugging purposes.

SA-1 The TOE generates audit records for auditable events. The audit function is integrated into each module of ArubaOS. In particular, when an auditable event occurs, the module executes a logging API call that records event information to the external audit server. The following event sources are supported:

"AAA" – wireless user authentication events
"Management AAA" – administrator authentication events
"Configuration Manager" - changes to the TOE configuration
"User" – wireless user events other than authentication
"VPN Server" – IPSec/IKE VPN-related events
"WIP" - Wireless Intrusion Protection events
"Switch" – internal TOE events, such as startup/shutdown of various services, including audit services, internal errors and warnings.

For each event the following information is recorded:

Event Type – The BSD syslog logging level.

Subject Identity – The identity of the subject involved in the event. For identified users, the subject identity is represented by the user name. For other subjects, the subject identity is represented by the IP address for wired network subjects, and by the MAC address for wireless network subjects.

Date and Time of the Event - The date and time when the event occurred. The date and time are represented by the month, day, hour, minute and second, e.g. "May 05 10:24:07".

Outcome of the Event - success or failure of the event.

The following events are auditable

1) Unsuccessful login by a wireless user or administrator.
2) Creation/deletion of an administrator, setting and modifying the password for the administrator.
3) Creation/deletion of a new wireless user role.
4) Setting/modifying IPSec/IKE pre-shared keys. Setting IPSec/IKE encryption algorithms. Changes to the VPN configuration.
5) Setting the RSA server certificate used by the HTTPS Web UI.
6) Startup and shutdown of audit functions, changes to the types of audited events
7) Setting IP addresses of the authentication and audit servers as well as IPSec/IKE pre-shared keys used by trusted channels established between the TOE and authentication/audit servers. Initiation/closure of a trusted channel.
8) Enabling and disabling of any of the WIP analysis mechanisms, automated responses performed by the WIP mechanisms and actions taken due to imminent security violations.

The audit records are transmitted to the audit server over a trusted channel and stored on the audit server. The audit server protects the records, and provides a capacity to

review them to the administrator.

Note: Reliable time stamps described in PT-2 are used to provide time for audit records.

SA-2 After a user is identified, the TOE will keep an in-memory session object for this user and associate each auditable event with the identity of the user that caused the event using an in-memory pointer to the username string. The user is identified by the username in the audit record.

SA-3 The TOE provides the ability to include or exclude auditable events from the set of audited events based on the user identity, event type, device interface and wireless client identity. The inclusion and exclusion of audited events for the event type (syslog level) is performed by using the "*logging*" command of the command line interface. Similar functionality is provided by the *Monitoring->Management->Logging* panel of the Web UI. For user identity, device interface and wireless client, selection is provided using a separate mechanism, the "aaa user debug" command.

6.1.3 I&A and TOE Access

I&A and TOE access defines the types of user authentication mechanisms supported by the TSF, as well as the attributes on which the user authentication mechanisms are based. It also specifies how the TOE controls establishment of a user session.

IA-1 The TOE supports role-based authentication.

Wireless users and remote administrators use different authentication mechanisms.

Wireless users

Wireless users are authenticated using an external RADIUS authentication server. A trusted channel is established between the TOE and the authentication server.

For wireless users using 802.11i authentication, when a user client connects to the TOE, the TOE passes authentication protocol messages between the client and the authentication server, until the user is authenticated, or authentication is denied. The following authentication protocols are supported: EAP-TLS, EAP-TTLS, PEAP. As a part of the initial handshake the authentication server presents to the client a TLS server certificate. Communications between the client and the server are then encrypted by the TLS protocol.

For EAP-TTLS and PEAP protocols, the user will authenticate to the server over a TLS-encrypted connection using a username and password.

For EAP-TLS, the user will use a TLS client certificate to authenticate. The certificate will contain the username of the user, and may contain other user-specific information. The authentication server will maintain a list of trusted certification authorities to verify the client certificate.

If the authentication fails, the authentication server will communicate the authentication failure to the TOE. Otherwise, the authentication server will communicate the authentication success to the TOE and send to the TOE the session key, which was derived during the EAP-TLS/EAP-TTLS/PEAP handshake, as well as the user role

attribute. The session key may be used by the TOE to encrypt further communications with a wireless client.

For wireless users using an open system connection with VPN, the IPSec/IKE VPN is established between the TOE and the wireless client prior to the user authentication using pre-shared keys. The user authenticates to the RADIUS server using a username and password. The RADIUS server communicates success or failure of the authentication to the TOE.

Remote Administrators

Remote administrators are configured as users who have privileges to access the CLI and WebUI administration interfaces. Following user authentication the remote administrators must authenticate further as an administrator in order to perform administrative tasks.

Remote administrators are authenticated as wired users using an external RADIUS authentication server. A trusted channel is established between the TOE and the authentication server. The remote administrators authenticate as wired users using a username and password via Captive Portal. The Captive Portal interface provides a trusted path to connect to the TOE via HTTPS. The HTTPS interface uses a server RSA certificate which is stored on the TOE. The authentication and lockout after unsuccessful authentication attempts is applied to this logon.

The further authentication as an administrator as a management user, which is required to perform administrative tasks, uses an internal database on the TOE, which stores a list of management users and their passwords.

Local Administrators

Local administrators are authenticated as management users using the internal database using a username and password.

IA-2 The TSF requires each wireless user or administrator to be successfully identified before allowing any other TSF-mediated actions on behalf of that user. Wireless users and administrators are identified by using a username. The TOE will not allow the wireless user or the administrator to perform any TSF-mediated actions except identification before the authentication process completes successfully. In particular, a wireless user has no access to the protected wired network until he/she is authenticated. The administrator has no access to management functions until he/she is authenticated.

IA-4 The TOE maintains a username and password for each management user, set for each new user using the *Configuration-> Management-> Access Control* panel of the Web UI, and clicking the *Add* button. A new password for a particular local administrator can be set by using the *Configuration-> Management-> Access Control* panel of the Web UI, and clicking the *Edit* button next to the administrator name. A similar functionality is provided by the *"mgmt-user"* command of the CLI.

The TOE maintains remotely authenticated wireless user and remote administrator attributes for the duration of each remotely authenticated user session, including session key and role.

IA-5 The TSF associates the username of a logged on user with the user's sessions and any processes acting on behalf of that user.

TA-1 The TSF terminates a wireless user session or a management user CLI session (for a local or remote administrator) after the inactivity time exceeds a configurable session idle timeout.

The TSF terminates a management user Web UI session for a remote administrator after the inactivity time exceeds a session idle timeout of 30 minutes. Timeout does not apply to the following screens which are autorefreshed.

Monitoring > Network > All Access Points
Monitoring > Network > All Air Monitor
Monitoring > Network > Wired Access Points
Monitoring > Network > All WLAN Clients
Monitoring > Controller > Access Points
Monitoring > Controller > Air Monitor
Monitoring > Controller > Wired Access Points
Monitoring > Controller > Clients
Monitoring > WLAN > [ESSID_NAME] > Access Points
Monitoring > WLAN > [ESSID_NAME] > Clients
Monitoring > Debug > Local Clients
Monitoring > Debug > Process Logs
Maintenance > WLAN > Program AP
Maintenance > WLAN > Reboot AP.

The session idle timeout is the maximum amount of time a wireless user or a management user may remain idle.
The TSF assesses wireless user inactivity as the cessation of network traffic arriving from the wireless client. It should be noted that processes acting on behalf of the user may send protocol network packets to the mobility controller, even when the user is not interacting directly, e.g. pressing keys.

The TSF assesses management user inactivity as the cessation of direct interaction, e.g. pressing keys and using the mouse.

To change the wireless user session idle timeout, the administrator shall use the *"config aaa timers"* command of the CLI. The default value of the wireless user session idle timeout is 10 minutes.

To change the management user CLI session idle timeout, the administrator shall use the *"loginsession timeout*" command of the CLI. The default value of the management user session idle timeout is 15 minutes.

TA-2 The TSF displays an advisory warning banner regarding use of the TOE prior to establishing an administrator session. The administrator can configure the warning message displayed in the banner.

6.1.4 Cryptography

The TOE employs cryptographic functionalities of a FIPS 140-2 validated module for the purposes of wireless and wired security protocol processing as well as for the establishment of secure remote administration sessions.

Aruba 6000 and 800 series Mobility Controllers have been validated to meet FIPS 140-2 Level 2 security requirements. Cryptographic Key Management section of the Cryptographic Module Security Policy (Certificate #649: <http://csrc.nist.gov/cryptval/140-1/1401val2006.htm#649>) provides detailed information in regards to the cryptographic key generation, key distribution, and key destruction used in Aruba Mobility Controller 6000 and 800 series.

CY-1 The TSF generates cryptographic keys in accordance with the cryptographic key generation methods identified in Table 5-4 Cryptographic Operation. In particular, the TSF uses the ANSI X9.31 random number generator to generate cryptographic keys internally. Cryptographic key sizes and the corresponding standards are also identified in Table 5-2.

The TOE generates an SSH RSA public-private key pair during the initial configuration of the TOE. This public-private key pair is used to provide SSH-based remote administration access to the TOE.

The TOE generates Diffie-Hellman session parameters used during TLS and IPSec/IKE handshakes.

IPSec/IKE pre-shared keys are not generated by the TOE. They are set by the administrator using the management interface.

CY-2 The cryptographic keys are distributed in accordance with FIPS-approved key distribution techniques. In particular, the following techniques are utilized:

- TLS uses RSA key wrapping to perform key transport.

- SSH and TLS use the Diffie-Hellman algorithm to perform key agreement.

- IKE protocol with a pre-shared key option is used to establish IPSec session keys. IKE utilizes the Diffie-Hellman algorithm to derive the session keys.

The RSA server certificate, which is used to provide HTTPS for the management interface, is generated as a self-signed certificate during the TOE installation phase, and can also be updated later through the management interface.

The static IPSec/IKE key is set the administrator using the management interface. 802.11i and xSec use dynamically derived session keys provided by the authentication server.

Note: 802.11i and xSec session keys are established by the authentication server and the wireless client using EAP-TLS, EAP-TTLS and PEAP protocol handshakes. In this case, key establishment is performed by the IT Environment. After the session key is established, it is provided by the authentication server to the TOE.

CY-3 The cryptographic keys will be zeroized upon issuance of the key zeroization command by the administrator as prescribed in the FIPS 140-2 standard. The Cryptographic Module Security Policy for the Aruba Mobility Controller (certificate #649) provides more information on cryptographic key zeroization.

CY-4 The TSF uses FIPS-approved cryptographic algorithms and key sizes identified in Table 5-4 Cryptographic Operation to perform cryptographic operations. In particular,

- AES is used for encryption of secure WLAN traffic (xSec and 802.11i protocols), IPSec/IKE traffic, SSH traffic and TLS traffic. AES-CCM mode is used by the 802.11i to provide both encryption and data authentication.

- SHA-1 and HMAC SHA-1 are used for data authentication in xSec, IPSec/IKE, SSH and TLS protocols.

- Triple DES is used for encryption of secure IPSec/IKE traffic, SSH traffic, TLS traffic, and, as a part of ANSI X9.31 PRNG, for random data generation and key generation.

- RSA PKCS #1 is used for encryption/decryption of shared secret during TLS

handshake as well as for signature generation/verification during SSH and TLS handshakes.

- PRNG (ANSI X9.31) is used to generate random data and cryptographic keys for xSec, 802.11i, TLS, SSH and IPSec/IKE.

The TOE relies on the environment (authentication server) to implement cryptographic handshakes used in EAP-TLS, EAP-TTLS and PEAP protocols.

6.1.5 User Data and TSF Protection

The User Data and TSF Protection security function protects the user and TSF data against unauthorized disclosure, modification or deletion. It also protects the integrity of mechanisms that provide the TSF.

UDP-1 Where the wireless user authenticates using 801.11i, the TSF will encrypt user data transmitted to wireless users using xSec or 802.11i Layer 2 protocols. The administrator sets the protocol to be used by the TOE. Both of the protocols utilize AES for encryption. In addition to that, once the wireless user is authenticated to the TOE and is connected to the IP network, the administrator has an option to enforce additional Layer 3 encryption using the IPSec/IKE protocol, which employs either Triple-DES or AES algorithms. The xSec and 802.11i protocols may use for encryption the session keys derived by the authentication server using EAP-TLS, EAP-TTLS or PEAP protocols during the wireless user authentication phase.

IPSec/IKE uses session keys which are derived during the IKE handshake using the Diffie-Hellman key agreement algorithm. The IKE handshake uses a pre-shared key set by the administrator. The IPSec/IKE protocol with pre-shared keys represents a probabilistic/permutational security mechanism.

The wireless user may authenticate without using 802.11i. In this case, an IPSec/IKE VPN is set up prior to user authentication. The user authenticates using a username and password. The authentication and subsequent data traffic are protected by the VPN. As above, IPSec/IKE uses a pre-shared and represents a probabilistic/permutational security mechanism.

UDP-2 Network packets are received in memory buffers pre-allocated at boot time. The buffers are populated in the network interface receive ring. When CPU receives network packets from the network interface, CPU allocates a free buffer from the pre-allocated pool and replenishes the receive ring. When CPU has finished packet processing, CPU adds the memory buffer associated with this network packet to the free buffer pool. Packets read from the buffers are always the same size as those written, so no explicit zeroing or overwriting of buffers on allocation is required.

PT-1 The TOE data and executables are protected inside the FIPS 140-2 Level 2 certified cryptographic module. The enclosure of the Mobility Controller has been designed to satisfy FIPS 140-2 Level 2 physical security requirements; in particular the hard steel case of the Mobility Controller is resistant to probing and is opaque within the visible spectrum. The Mobility Controller employs tamper-evident seals to detect unauthorized physical access to the internal components and data of the TOE.

The TOE operational environment is non-modifiable. Firmware updates are not allowed. The control plane operating system is MontaVista's Embedded Linux, a real-time, multi-threaded operating system that supports memory protection among

processes. Access to the underlying Linux implementation is not provided to the users. The command line interface utilizes a restricted command set. The TOE does not provide uncontrolled management interfaces.

The TOE's critical data is protected against unauthorized disclosure, modification, and substitution by controlling access to the management functions via authentication and through the access control mechanism. Only an authenticated administrator is authorized to access TOE management functions. The TOE is only accessible through its specified interfaces.

Wireless user roles and traffic policies form the cornerstone of all functionality of the Mobility Controller. Traffic policies can be associated with wireless user roles, giving differential treatment to different wireless users and providing protection of the TSF data.

The TOE provides only well-defined session interfaces. Administrators and wireless users use different types of sessions. Administrators use management user session to perform management functions. Administrators can access the TOE locally and remotely. Local administrators logon directly as a management user. A remote administrator requires an initial logon as a wired user, privileged to access the management interfaces for a further logon. A remote administrator utilizes the SSH protocol to access the CLI functionality, and the HTTPS protocol to access the Web UI. A local administrator administrator utilizes the CLI functionality through the local serial console interface. Wireless users utilize the TOE to establish secure wireless connections to the protected wired network. Wireless users do not have access to management interfaces. The functionalities described above are completely disjoint with regards to operators, and thus, the separation between operators based on these lines is clearly established.

Sessions of authenticated wireless users are kept separate based on a session table which is maintained by the TOE for each wireless security protocol. Each session object contains username and session id information, as well as the session key. The session object is used to enforce separation of sessions belonging to different wireless users.

The TOE maintains an IPSec/IKE VPN connections table in memory. Each VPN connection is maintained in the table along with information about the identity of the user of that connection, the session id and the session key being used.

The TOE maintains a table of SSH connections in memory. Each SSH management connection is stored in the table along with the username and session id information for that session, as well as the session key. The table maintains separation between SSH management sessions. Additionally, the maximum of five concurrent SSH sessions are supported. If more than one session is running simultaneously, only one session can perform the configuration change, and the other sessions would be blocked until the configuration change in progress is completed.

The HTTPS management interface uses the OpenSSL library, which allocates a unique session context for each HTTPS management session, which includes the session id and the session key. The TOE maintains a table mapping HTTPS administrative sessions to administrator users.

PT-2 The Mobility Controller has an internal hardware clock that provides reliable time stamps used for auditing. The internal clock is synchronized with a time signal

obtained from an external NTP server.

PT-3 The Mobility Controller runs a suite of self tests during power-up which includes demonstration of the correct operation of the hardware and the use of cryptographic functions to verify the integrity of TSF executable code and static data. An administrator can choose to reboot the TOE to perform power-up self test.

PT-4 The Mobility Controller runs the suite of FIPS 140-2 validated cryptographic module self tests during start-up or on request from the administrator, including immediately after generation of a key.

6.1.6 Security Management

The Security Management security function provides the administrator role and enables management of security attributes, TSF data and functions.

The administrator can configure TOE security settings and policies using the Web User Interface via HTTPS, or the Command Line Interface via serial console.

SM-1 The TOE supports role-based authentication. There are two types of roles: the administrator role and the wireless user role.

Administrators manage the TOE using HTTPS Web UI or command line interface (CLI). The remote administrator first authenticates with a username and password to the internal authentication database, using the Captive Portal interface via an HTTPS connection. The local administrator first authenticates with a username and password to the internal authentication database, via the interactive command line. Once the administrator is authenticated, the TOE provides management interfaces which can be used by the administrator to configure the TOE security functions. Local administrators use the CLI via a serial console connection to the TOE. Remote administrators may use the Web UI interface from the browser. Remote administrators may also use the CLI interface via an SSH protocol connection from an SSH client.

Wireless users can not access the TOE through the Web UI or CLI interfaces and, therefore, do not have access to the management functionalities of the TOE.

SM-2 The administrator is able to configure the following security functions:

a) Wireless security protocols, including choosing between xSec and 802.11i for wireless data encryption. This functionality is provided by the *WLAN->Network* panel of the Web UI.

b) VPN server, including setting up IPSec/IKE connections and setting the pre-shared keys. This functionality is provided by the *Security-> VPN Settings -> IPSec* panel of the Web UI.

c) WIP, including setting signature events (wireless intrusion profiles) and actions to be taken upon detection of a potential security violation

d) Identification and Authentication. This includes configuring the IP address of the authentication server, which is performed by utilizing the *Security->AAA Servers -> Radius Servers* panel of the Web UI, configuring management user usernames and passwords (which is performed by utilizing the *Management->Access Control* panel of the Web UI), setting the CLI idle timeout for management users (which is

performed utilizing the CLI *loginsession timeout* command) and setting the idle timeout for wireless users (which is configured by utilizing the *Security->AAA Servers -> Internal Servers-> General* panel of the Web UI for local administrators and the *Security->AAA Servers* panel of the Web UI or the CLI *config aaa timers* command).

e) Auditing. This includes starting and stopping of audit event logging, setting the IP address of the audit server and setting the types of audit events to selectively log. The configuration is performed by utilizing the *Management->Logging* panel of the Web UI.

SM-3 To meet FMT_MSA.2, which is included as a dependency in cryptography-related requirements FCS_CKM.1a, FCS_CKM.2a, FCS_CKM.4a and FCS_COP.1a, the TSF shall ensure that only secure values are accepted for security attributes. The security attributes are cryptographic keys. The keys are considered secure if they are generated, distributed and managed by a FIPS 140-2 approved cryptographic module. In particular, running the TOE in FIPS mode of operation enforces this requirement.

SM-4 The TOE provides to the administrator capabilities to query, modify, delete, clear and create management users, including usernames and passwords, using the *Configuration-> Management-> Access Control* panel of the Web UI.

The TOE provides to the administrator capabilities to query, modify, clear, create the set of audit event types to selectively log using the *Configuration-> Management-> Logging* panel of the Web UI and the “aaa user debug” command of the CLI.

The TOE also provides to the administrator capabilities to modify and set initial value of:

a) management user session idle timeout, using the *“loginsession timeout”* command of the command line interface

d) audit server IP address, using the *Management->Logging* panel of the Web UI.

f) authentication server IP address, using the *Security->AAA Servers -> Radius Servers* panel of the Web UI.

g) TLS Web UI server certificate used for TOE administration, using the *Wireless Network Management -> Import Certificate For Web Server* panel of the Web UI.

h) NTP server IP address, using the *Configuration->Switch->General* panel of the Web UI.

6.1.7 Trusted Path/Channels

The TOE provides trusted paths for remote administrator authentication as a wired user and for wireless user authentication using an open system connection. The TOE provides a trusted channel between itself and the IT environment authentication, audit and NTP servers.

TP-1 For remote administrators, the TOE provides a TLS based trusted path from the TOE to the remote administrators for authentication as wired users to the external authentication server.

For wireless users using an open system connection, the TOE provides an IPSec/IKE VPN trusted path from the TOE to the wireless users for authentication of the

wireless users to the external authentication server.

Note: As specified in the requirement FTP_TRP.1c for the IT Environment, for wireless user authentication using EAP-TLS, EAP-TTLS or PEAP protocols, the authentication server establishes a trusted path between the authentication server and the wireless user which passes through the TOE.

TP-2 The TOE uses the IPSec/IKE protocol with pre-shared keys to establish a trusted channel between itself and the external authentication, logging and NTP servers. IPSec/IKE with pre-shared keys represents a probabilistic/permutational security mechanism. To configure the channels the administrator uses the *Security -> VPN Settings -> IPSec* panel of the Web UI to create the host-to-host IPSec/IKE connections. The administrator then sets a pre-shared IPSec/IKE key for each IPSec/IKE connection using the *Security -> VPN Settings -> IPSec -> Add IKE Secret* panel of the Web UI.

6.2 Assurance Measures

The assurance requirements for this TOE are for Evaluation Assurance Level EAL2, augmented with ACM_SCP.1 (CM Coverage), ALC_FLR.2 (Flaw Remediation) and AVA_MSU.1 (Misuse – Examination of guidance). The following items are provided as evaluation evidence to satisfy the assurance requirements:

Table 6-2 Assurance Measures

Item	Security Assurance Requirement	How Satisfied
1	ACM_CAP.2 Configuration items	Aruba Mobility Controller Configuration Management Plan and Procedures
2	ACM_SCP.1 CM Coverage	Aruba Mobility Controller Configuration Management Plan and Procedures
3	ADO_DEL.1 Delivery procedures	Aruba Mobility Controller Delivery and Operation Plan and Procedures
4	ADO_IGS.1 Installation, generation, and start-up procedures	Aruba 5000/6000 Series Mobility Controller Installation Guide Aruba 800 Series Mobility Controller Installation Guide Aruba Quick Start Guide
5	ADV_FSP.1 Informal functional specification	Aruba Mobility Controller Functional Specification
6	ADV_HLD.1 Descriptive high-level design	Aruba Mobility Controller High-Level Design Specification
7	ADV_RCR.1 Informal correspondence demonstration	Aruba Mobility Controller Informal Correspondence Demonstration

Item	Security Assurance Requirement	How Satisfied
8	AGD_ADM.1 Administrator guidance	ArubaOS 2.4 Reference Guide ArubaOS 2.4 Management Reference Guide Aruba Quick Start Guide
9	AGD_USR.1 User guidance	ArubaOS 2.4 User Guide
10	ALC_FLR.2 Flaw Remediation	Aruba Mobility Controller Flaw Remediation
11	ATE_COV.1 Evidence of coverage	Aruba Mobility Controller Test Coverage Analysis
12	ATE_FUN.1 Functional testing	Aruba Mobility Controller Functional Testing Plan and Procedures
13	ATE_IND.2 Independent testing - sample	TOE for testing Authentication Server Audit Server Aruba Mobility Controller High-Level Design Testing Plan and Procedures Aruba Mobility Controller Functional Testing Plan and Procedures
14	AVA_MSU.1 Misuse – Examination of guidance	Guidance documents supplied to satisfy ADO_IGS.1, AGD_ADM.1 and AGD_USR.1
15	AVA_SOF.1 Strength of TOE security function evaluation	Aruba Mobility Controller Strength of Function Analysis
16	AVA_VLA.1 Independent vulnerability analysis	Aruba Mobility Controller Vulnerability Analysis

7 PP Claims

7.1 PP Reference

This TOE is in conformance with the Wireless Local Area Network (WLAN) Access System Protection Profile for Basic Robustness Environments [3].

7.2 PP Tailoring

All PP SFRs except FTP_TRP.1 are satisfied by the TOE, either without tailoring or with permitted operations carried out. PP SFR FTP_TRP.1 is considered to be in error and has been corrected in ST SFRs FTP_TRP.1a, FTP_TRP.1b and FTP_TRP.1c (for a justification, please see the entry for FTP_TRP.1 in Table 8-8).

Those TOE SFRs that satisfy the corresponding PP SFRs by tailoring are identified as “PP Tailored” in the fourth columns of Table 5-1 Functional Components and Table 5-5 Functional Components. In Table 5-1 Functional Components the TOE SFR component names identified in the second column match the corresponding PP SFR component names, with the following exceptions:

- PP SFR component FCS_BCM_EXP.1 is addressed within TOE SFR components FCS_CKM.1a, FCS_CKM_EXP.2, FCS_CKM.4a and FCS_COP.1a
- PP SFR components FCS_COP_EXP.1 and FCS_COP_EXP.2 are addressed within TOE SFR component FCS_COP.1a.

In Table 5-5 Functional Components the IT Environment SFR component names identified in the second column match the corresponding PP SFR component names.

7.3 PP Additions

The TOE has an additional IT Objective, O.INTRUSION, which is implemented by the TOE’s Wireless Intrusion Protection features.

TOE SFRs that are additional to those required by the PP are identified as “Additional” in the fourth columns of Table 5-1 Functional Components and Table 5-5 Functional Components.

8 Rationale

8.1 Security Objectives Rationale

This section provides evidence demonstrating coverage of the TOE security environment by the IT security objectives. The security objectives were derived from statements of threats, assumptions and organizational security policies. The following table demonstrates that the mapping of the assumptions, threats and organizational security to the security objectives is complete. The rationales in the following sections provide evidence of coverage for each statement of TOE security environment.

Table 8-1 Mapping of Security Environment to Security Objectives, shows that:

- Each threat, assumption and organizational security policy is addressed by at least one security objective, and
- Each security objective addresses at least one threat, assumption or policy.

Table 8-1 Mapping of Security Environment to Security Objectives

Security Environment \ Security Objectives	O.MANAGE	O.AUDIT_GEN	O.SELF_PROTECT	O.BANNER	O.TOE_ACCESS	O.RESIDUAL	O.CORRECT	O.TIME	O.TRAFFIC	O.CRYPTO	O.INTRUSION	OE.AUDIT_PROTECT	OE.AUDIT_REVIEW	OE.MANAGE	OE.SELF_PROTECT	OE.TIME	OE.TOE_ACCESS	OE.RESIDUAL	OE.PROTECT_COMMS	OE.ADMIN	OE.PROTECT	OE.BYPASS	OE.NO_GENRL
T.ERROR	X						X													X			
T.IMPERSON					X					X							X					X	
T.ACCESS	X				X					X				X						X			
T.ATTACK	X		X		X	X			X	X	X			X	X		X	X	X	X		X	
T.RESIDUAL						X												X					
T.SESSION					X																		
T.CRYPTO			X			X									X			X					X
T.INTERNAL	X		X			X								X	X			X					X
A.ADMIN																				X			
A.NO_GENRL																							X
A.LOCATE																					X		
A.BYPASS																						X	
P.BANNER				X																			
P.ACCOUNT	X	X			X			X				X	X	X		X	X						
P.CRYPTO						X				X													
P.CHANNEL									X	X									X				
P.NO_ADHOC									X													X	

8.1.1 Threats

T.ERROR

An administrator may accidentally incorrectly install or configure the TOE, resulting in ineffective security mechanisms.

Coverage Rational:

O.MANAGE provides that administrators will be able to effectively manage the TOE and its security functions. **O.CORRECT** provides assurance to the administrators that the TSF continues to operate as expected. They will be competent to manage the TOE, including initial installation and configuration, and the security of the information it contains, and will be trusted not to deliberately abuse their privileges (**OE.ADMIN**).

T.IMPERSON

A user may gain unauthorized access to data or TOE resources by impersonating an authorized user of the TOE.

Coverage Rational:

O.TOE_ACCESS mitigates this threat by controlling the logical access to the TOE and its resources. By constraining how and when authorized users can access the TOE, and by mandating the type and strength of the authentication mechanism, this objective helps mitigate the possibility of a user attempting to login and masquerade as an authorized user. **OE.TOE_ACCESS** supports wireless user authentication by providing an authentication server in the TOE IT environment. In addition, this objective provides the administrator means to control the number of failed login attempts a wireless user or remote administrator can generate before an account is locked out, further reducing the possibility of a user gaining unauthorized access to the TOE. **OE.BYPASS** contributes to mitigating this threat by ensuring that all information that flows between a wireless client and any other wireless client or host networked to the TOE must pass through the TOE. **O.CRYPTO** contributes to mitigating this threat by requiring the TOE to utilize cryptographic services of a FIPS 140-2 validated module. These services will provide confidentiality and integrity protection of the TSF data while in transit.

T.ACCESS

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

Coverage Rational:

O.TOE_ACCESS mitigates this threat by including mechanisms to authenticate the TOE administrators and placing controls on administrator sessions. **O.MANAGE** and **OE.MANAGE** mitigate this threat by restricting access to administrative functions and management of TSF data to the administrator. **OE.ADMIN** requires that the administrators are competent to securely manage the TOE, are not hostile and can be trusted not to disclose authentication credentials to unauthorized users. **O.CRYPTO** contributes to mitigating this threat by requiring the TOE to utilize cryptographic services of a FIPS 140-2 validated module. These services will provide confidentiality and integrity protection of administrative data while in transit.

T.ATTACK

A user may gain access to TSF data, executable code or services (either on the TOE or by sending data through the TOE) for which they are not authorized according to the TOE security policy.

Coverage Rational:

O.MANAGE and **OE.MANAGE** mitigate this threat by restricting access to administrative functions and management of the TSF data to the administrator. **OE.ADMIN** provides that administrators are not hostile and competent to manage the TOE security functions. **O.TOE_ACCESS** and **OE.TOE_ACCESS** provide that the TOE requires successful authentication prior to gaining access to certain services on or mediated by the TOE.

O.TRAFFIC works to mitigate this threat by ensuring that all network packets that flow through the TOE are subject to the information flow policies.

O.INTRUSION works to mitigate this threat by detecting, informing the administrator and, if possible, containing wireless intrusion attacks.

OE.BYPASS contributes to mitigating this threat by ensuring that wireless clients must be configured so that all information that flows between a wireless client and any other wireless client or host networked to the TOE must pass through the TOE.

O.CRYPTO contributes to mitigating this threat by requiring the TOE to utilize cryptographic services of a FIPS 140-2 validated cryptographic module. These services will provide confidentiality and integrity protection of TSF data while in transit.

O.SELF_PROTECT and **OE.SELF_PROTECT** mitigate this threat by ensuring that all configured enforcement functions must be invoked prior to allowing a user to gain access to the TOE or TOE mediated services.

O.RESIDUAL and **OE.RESIDUAL** contribute to the mitigation of this threat by ensuring any residual data is removed from network packet objects and ensuring that cryptographic material is not accessible once it is no longer needed.

OE.PROTECT_COMMS provides that the authentication data will be protected by means of a protected channel in the environment.

T.RESIDUAL

A user or process may gain unauthorized access to data through reallocation of TOE resources from one user or process to another.

Coverage Rational:

O.RESIDUAL and **OE.RESIDUAL** contribute to the mitigation of this threat by ensuring any residual data is removed from network packet objects and ensuring that cryptographic material is not accessible once it is no longer needed.

T.SESSION

A user may gain unauthorized access to an unattended session.

Coverage Rational:

The TSF will uniquely identify all users, and will authenticate the claimed identity before granting a user access to the TOE services. When a user is idle, user

sessions are dropped after an administrator-defined time period of inactivity. (**O.TOE_ACCESS**).

T.CRYPTO

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.

Coverage Rational:

O.RESIDUAL and **OE.RESIDUAL** contribute 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_PROTECT and **OE.SELF_PROTECT** ensure that the TOE will have adequate protection from external sources and that all TSP functions are invoked.

OE.NO_GENRL contributes to the mitigation of this threat by ensuring that no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) are available on the TOE.

T.INTERNAL

A user or process may cause, through an unsophisticated attack, TSF data, or executable code to be inappropriately accessed (viewed, modified, or deleted).

Coverage Rational:

O.MANAGE mitigates 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 and **OE.RESIDUAL** contribute 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_PROTECT and **OE.SELF_PROTECT** ensure that the TOE will have adequate protection from external sources and that all TSP functions are invoked.

OE.NO_GENRL contributes to the mitigation of this threat by ensuring that no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) are available on the TOE.

8.1.2 Assumptions

A.ADMIN

Administrators are non-hostile, appropriately trained and follow all administrator guidance.

Coverage Rational:

OE.ADMIN provides that the administrator of the TOE will be competent to manage the TOE and can be trusted not to deliberately abuse their privileges.

A.NO_GENRL

There are no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the TOE.

Coverage Rational:

> **OE. NO_GENRL** specifies that the TOE provides no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications).

A.LOCATE

Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.

Coverage Rational:

> **OE.PROTECT** specifies that the environment provides physical security, commensurate with the value of the TOE and the data it contains.

A.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.

Coverage Rational:

> **OE.BYPASS** provides that the wireless clients are configured such that information cannot flow between a wireless client and any other wireless client or host networked to the TOE without passing through the TOE.

8.1.3 Organizational Security Policies

P.BANNER

The TOE shall display an initial banner for administrative logins describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.

Coverage Rational:

> **O.BANNER** satisfies this policy by ensuring that the TOE displays an administrator configurable banner that provides all administrators with a warning about unauthorized use of the TOE.

P.ACCOUNT

The authorized users of the TOE shall be held accountable for their actions within the TOE.

Coverage Rational:

> **O.AUDIT_GEN** addresses this policy by providing a capability to detect and record security–relevant events, including events related to actions of a specific user.
>
> **OE.AUDIT_PROTECT** provides protected storage of audit data in the environment.

OE.AUDIT_REVIEW supports accountability by providing mechanisms for viewing and sorting the audit logs.

O.MANAGE provides that the TSF allows only administrators to manage the TOE and its security functions, and ensures that only authorized administrators will be able to access such functionality. Therefore, the access to TOE administration and management functions is restricted to the administrators. **OE.MANAGE** ensures that the administrator can manage audit functionality in the TOE IT environment. **O.TOE_ACCESS** and **OE.TOE_ACCESS** support this policy by controlling logical access to the TOE and its resources. Users are identified and authenticated so that their actions may be tracked by the administrator.

A reliable time stamp will be included in the event audit record (**O.TIME** and **OE.TIME**).

P.CRYPTO

The TOE shall provide NIST FIPS 140-2 validated cryptographic modules that provide cryptographic functions for its own use, including encryption/decryption operations.

Coverage Rational:

O.CRYPTO satisfies this policy by requiring the TOE to implement the cryptographic services of a FIPS 140-2 validated module. These services will provide confidentiality and integrity protection of TSF data while in transit to remote parts of the TOE.

O.RESIDUAL satisfies this policy by ensuring that cryptographic data are cleared according to FIPS 140-2.

P.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.

Coverage Rational:

O.CRYPTO satisfies this policy by requiring the TOE to implement the cryptographic services of a FIPS 140-2 validated module. 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.TRAFFIC further allows the TOE administrator to set a policy to encrypt all wireless traffic.

O.PROTECT_COMMS provides that audit records and authentication data will be protected by means of a protected channel in the environment.

P.NO_ADHOC

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

Coverage Rational:

O.TRAFFIC works to support this policy by ensuring that all network packets that flow through the TOE are subject to the information flow policies.

O.BYPASS supports this policy by ensuring that wireless clients must be configured to use the wireless access system for all information flowing between a wireless client and any other host on the network. If the clients are properly configured, any

information passing through the TOE will be inspected to ensure it is authorized by TOE polices.

8.2 Security Requirements Rationale

This section provides evidence demonstrating that the security objectives for the TOE and the IT environment are satisfied by the security requirements.

8.2.1 Rationale for TOE Security Requirements

Table 8-2 Mapping of TOE Security Requirements to Security Objectives for the TOE

TOE security Objectives / Security Functional Requirements	O.MANAGE	O.AUDIT_GEN	O.SELF_PROTECT	O.BANNER	O.TOE_ACCESS	O.RESIDUAL	O.CORRECT	O.TIME	O.TRAFFIC	O.CRYPTO	O.INTRUSION
FAU_ARP.1											X
FAU_SAA.3											X
FAU_GEN.1a		X									
FAU_GEN.2		X									
FAU_SEL.1		X									
FIA_UAU.1a					X						
FIA_UAU_EXP.5a					X						
FIA_UID.2a					X						
FIA_ATD.1a					X						
FIA_ATD.1b					X						
FIA_USB.1		X									
FTA_SSL.3					X						
FTA_TAB.1				X							
FCS_CKM.1a										X	
FCS_CKM.2a						X				X	
FCS_CKM_EXP.2						X				X	
FCS_CKM.4a						X				X	
FCS_COP.1a										X	
FDP_PUD_EXP.1									X		

TOE security Objectives / Security Functional Requirements	O.MANAGE	O.AUDIT_GEN	O.SELF_PROTECT	O.BANNER	O.TOE_ACCESS	O.RESIDUAL	O.CORRECT	O.TIME	O.TRAFFIC	O.CRYPTO	O.INTRUSION
FDP_RIP.1a						X					
FPT_RVM.1a			X		X				X		
FPT_SEP.1a			X		X				X		
FPT_STM_EXP.1		X						X			
FPT_TST_EXP.1							X				
FPT_TST_EXP.2							X				
FMT_MOF.1a	X										
FMT_MOF.1b	X										
FMT_MOF.1c	X										
FMT_MOF.1d	X										
FMT_MSA.2	X										
FMT_MTD.1a	X										
FMT_MTD.1b	X										
FMT_MTD.1c	X										
FMT_SMF.1a	X										
FMT_SMF.1b	X										
FMT_SMF.1c	X										
FMT_SMF.1d	X										
FMT_SMF.1e	X										
FMT_SMR.1a	X										
FTP_ITC_EXP.1a		X			X						
FTP_TRP.1a					X						
FTP_TRP.1b					X						

O.AUDIT_GEN

The TOE will provide the capability to detect and create records of, security-relevant events, including those associated with users.

Coverage Rational:

FAU_GEN.1a, Audit data generation, specifies that the TOE will be able to generate audit records of security-relevant events. The list of the events is specified in **FAU_GEN.1a**. For each event, date and time of the event, type of the event, subject identity, and the outcome (success or failure) of the event are recorded. Subject identity is defined as follows. For identified users, the subject identity is represented by the user name **(FIA_USB.1)**. For non-identified subjects, the subject identity is represented by the IP address for wired network subjects, and by the MAC address for wireless network subjects. Audit records use reliable time stamps (**FPT_STM_EXP.1a**).

For audit events resulting from actions of identified users, each event will be associated with the identity of the user that caused the event (**FAU_GEN.2**).

FAU_SEL.1, Selective audit, requires that the TSF will be able to include or exclude auditable events from the set of audited events based on user identity, event type, device interface and wireless client identity.

FTP_ITC_EXP.1a, Inter-TSF trusted channel, provides a trusted channel for services provided by the TOE IT environment (the audit server).

O.CRYPTO

The TOE shall use cryptographic services of a FIPS 140-2 validated cryptographic module to protect wireless user data, remote administration sessions, and VPN traffic.

Coverage Rational:

The FCS requirements satisfy this objective by ensuring that the cryptographic requirements include FIPS 140-2 compliance. **FCS_CKM.1a**, **FCS_CKM.2a**, **FCS_CKM_EXP.2** and **FCS_CKM.4a** mandate usage of services of a FIPS 140-2 validated cryptographic module when the TOE generates, distributes and destroys cryptographic keys. TSF will use services of a FIPS 140-2 validated cryptographic module, including specific cryptographic algorithms and cryptographic key sizes, to perform cryptographic operations **(FCS_COP.1a).**

O.MANAGE

The TOE must allow administrators to effectively manage the TOE and its security functions, and must ensure that only authorized administrators are able to access such functionality.

Coverage Rational:

The FMT requirements are used to satisfy this objective. **FMT_SMR.1a**, Security Roles, requires the TSF to maintain administrator and user roles. The administrator has unrestricted privileges and is responsible for all management functions within the TOE. The administrator will be capable of performing security management functions **(FMT_SMF.1a, FMT_SMF.1b, FMT_SMF.1c, FMT_SMF.1d, FMT_SMF.1e)**. The ability to manage the behavior of the TOE security functions is to be restricted to the administrator**(FMT_MOF.1a, FMT_MOF.1b, FMT_MOF.1c, FMT_MOF.1d)**. The ability to manage TSF data is to be restricted to the administrator (**FMT_MTD.1a, FMT_MTD.1b, FMT_MTD.1c**).

The TSF will enforce the secure values for cryptographic keys (**FMT_MSA.2**).

O.SELF_PROTECT

The TOE will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure.

Coverage Rational:

FPT_SEP.1a, TSF domain separation, 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.1a, Non-bypassability of the TOE Security Policy, ensures that the TSF makes policy decisions on all interfaces that perform operations on subjects 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

The TOE will obtain reliable time stamps.

Coverage Rational:

FPT_STM_EXP.1, Reliable time stamps, addresses this objective by requiring the TOE to obtain reliable time stamps.

O.TOE_ACCESS

The TOE will provide mechanisms that control a user's logical access to the TOE.

Coverage Rational:

FIA_UID.2a, User identification before any action, specifies that user identification is required before any TSF-mediated action is performed. **FIA_UAU.1a**, Timing of authentication, specifies that user authentication is required before any TSF-mediated action is performed, except for identification as per **FIA_UID.2a. FIA_UAU_EXP.5a,** multiple authentication mechanisms, specifies that the TSF will provide two mechanisms to support administrator and wireless user authentication: an internal password-based authentication mechanism and an external RADIUS server-based authentication mechanism . **FIA_ATD.1a**, Administrator attribute definition, specifies that as a minimum a username and password is maintained for each administrator. **FIA_ATD.1b**, User attribute definition, specifies that as a minimum a session key and role is maintained for each remotely authenticated user. **FTA_SSL.3** supports the objective by requiring the TOE to terminate an interactive session after the idle time limit is exceeded.

FPT_SEP.1a, TSF domain separation, protects the TSF from unauthorized users during execution and enforces separation between the security domains of authorized users in the TSC.

FPT_RVM.1a, Non-bypassability of the TSP, ensures that for each user the TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

FTP_TRP.1a ensures that remote administrators utilize a trusted path for authentication with the TOE.

FTP_TRP.1b ensures that wireless users authentication using an open system connection utilize a trusted path for authentication with the TOE.

FTP_ITC_EXP.1a, Inter-TSF trusted channel, provides a trusted channel for services provided by the TOE IT environment (the authentication server).

O.TRAFFIC

The TOE must mediate the flow of information to and from wireless devices in accordance with its security policy.

Coverage Rational:

FPT_SEP.1a, TSF domain separation, provides a distinct protected domain for the TSF and provides separation between subjects within the TSC, whereas

FPT_RVM.1a, Non-bypassability of the TSP, ensures that all actions requiring policy enforcement are validated by the TSF against the SFP.

FDP_PUD_EXP.1 allows the administrator to protect the flow of data on the wireless LAN by requiring all data to be encrypted.

O.BANNER

The TOE will display an administrator configurable advisory warning banner regarding use of the TOE prior to establishing an administrator session.

Coverage Rational:

FTA_TAB.1 addresses this objective by requiring the TOE to display a warning banner to an administrator prior to authentication.

O.RESIDUAL

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.

Coverage Rational:

FDP_RIP.1a addresses this objective by requiring the TOE to ensure that the contents of resources are not available once the resource is reallocated. For this TOE this is critical for resources used in handling network packet objects.

FCS_CKM.2a, FCS_CKM_EXP.2 and FCS_CKM.4a place requirements on how cryptographic keys are managed by a FIPS 140-2 validated cryptographic module, which ensures memory is immediately cleared after use.

O.CORRECT

The TOE will provide the capability to verify the correct operation of the TSF.

Coverage Rational:

> **FPT_TST_EXP.1** addresses this objective by requiring the TOE to provide facilities to verify the correct operation of TSF hardware and to verify that TSF software and data has not been corrupted.
>
> **FPT_TST_EXP.2** addresses this objective by requiring the TOE to make use of the suite of self-tests provided by the FIPS 140-2 validated cryptographic module, during initial start-up and on request, including immediately after generation of a key.

O.INTRUSION

The TOE will detect wireless intrusion attempts, alert administrators and, where possible, prevent or contain the intrusion attempts.

Coverage Rational:

> **FAU_SAA.3** addresses the first part of this objective by requiring the TOE detect a defined set of wireless intrusion attempts. **FAU_ARP.1** addresses the remainder of this objective by taking appropriate action on the detection of an intrusion attempt, including alerting an administrator and, if possible, preventing or containing the attempted intrusion.

8.2.2 Rationale for Security Requirements for the IT Environment

Table 8-3 Mapping of Security Requirements for the IT Environment to Security Objectives for the IT Environment

Security Objectives for IT Environment / Security Functional Requirements	OE.AUDIT_PROTECT	OE.AUDIT_REVIEW	OE.MANAGE	OE.SELF_PROTECT	OE.TIME	OE.TOE_ACCESS	OE.RESIDUAL	OE.PROTECT_COMMS
FAU_GEN.1b		X						
FAU_SAR.1		X						
FAU_SAR.2	X							
FAU_SAR.3		X						
FAU_STG.1	X							
FAU_STG.3	X							
FIA_UAU_EXP.5b						X		

Security Objectives for IT Environment / Security Functional Requirements	OE.AUDIT_PROTECT	OE.AUDIT_REVIEW	OE.MANAGE	OE.SELF_PROTECT	OE.TIME	OE.TOE_ACCESS	OE.RESIDUAL	OE.PROTECT_COMMS
FIA_UID.2b						X		
FIA_AFL.1						X		
FIA_ATD.1c						X		
FCS_CKM.1b						X		X
FCS_CKM.2b						X		X
FCS_CKM.4b						X		X
FCS_COP.1b						X		X
FDP_RIP.1b							X	
FPT_RVM.1b				X				
FPT_SEP.1b				X				
FPT_STM.1			X		X			
FMT_MOF.1e	X		X					
FMT_MTD.1d			X		X			
FMT_SMF.1f			X					
FMT_SMR.1b	X		X					
FTP_ITC_EXP.1b								X
FTP_TRP.1c						X		

OE.AUDIT_PROTECT

The IT Environment will provide the capability to protect audit information and the authentication credentials.

Coverage Rational:

FAU_SAR.2 restricts the ability to read the audit records to the administrator.

FAU_STG.1 restricts the ability to delete or modify audit information to the administrator. The environment will prevent unauthorized 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.1e and **FMT_SMR.1b** specify the ability of the administrator to control the security functions associated with audit and alarm generation.

OE.AUDIT_REVIEW

The IT Environment will provide the capability to selectively view audit information.

Coverage Rational:

The administrator will be able to read all the events and will be able to interpret the information (**FAU_SAR.1).** The TSF will provide the ability to perform searches and sorting of audit data events based on subject identity, event type, event date and time, device interface and wireless client identity (**FAU_SAR.3**). **FAU_GEN.1b** ensures that the TOE IT environment will generate appropriate audit events to support the TOE.

OE.MANAGE

The 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.

Coverage Rational:

FMT_MOF.1e ensures that the TOE IT environment limits access to the TSF management functions to the administrator.

The administrator will be capable of performing security management functions **(FMT_SMF.1f)**.

FMT_SMR.1b ensures that the TOE IT environment provides an administrative role that may be used to manage the IT environment.

Only the administrator will be able to modify and set date and time used for time stamps in **FPT_STM.1**, user passwords, user roles, EAP-TLS/TTLS/PEAP server certificates, list of trusted certificate authorities for EAP-TLS client certificates, IPSec/IKE pre-shared keys used for trusted channel/path **(FMT_MTD.1d)**.

OE.SELF_PROTECT

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.

Coverage Rational:

FPT_SEP.1b, IT Environment domain separation, 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.1b, Non-bypassability of the TOE IT Environment Security Policy, ensures that the environment makes policy decisions on all interfaces that perform operations on subjects and objects that are scoped by the policies.

OE.TIME

The IT Environment shall provide reliable time stamps and the capability for the administrator to set the time used for these time stamps.

Coverage Rational:

FPT_STM.1, Reliable time stamps, addresses this objective by requiring the IT environment to provide reliable time stamps.

The IT environment will provide to the administrator an interface that can be used to set the time used for the time stamps (**FMT_MTD.1d**).

OE.TOE_ACCESS

The IT Environment will provide mechanisms that support the TOE in providing a user's logical access to the TOE.

Coverage Rational:

The TOE IT environment will provide an authentication mechanism in order to support authentication of remote users. **FIA_UAU_EXP.5b** and **FIA_UID.2b** ensure that remote users are identified and authenticated prior to obtaining logical access to the TSF-mediated actions. **FTP_TRP.1c** provides a trusted path between the authentication server and the remote user passing through the TOE, which is used during EAP-TLS, EAP-TTLS or PEAP authentication. The FCS requirements satisfy this objective by ensuring that the cryptographic requirements include FIPS 140-2 compliance. **FCS_CKM.1b**, **FCS_CKM.2b**, and **FCS_CKM.4b** and **FCS_COP.1b** mandate usage of a FIPS 140-2 validated cryptographic module when the IT Environment (authentication server) authenticates a remote user using EAP-TLS, EAP-TTLS or PEAP protocols or manages corresponding cryptographic keys. **FIA_AFL.1** supports the objective by requiring that a remote user that reaches a predefined number of unsuccessful authentication attempts will be denied access to the TOE. **FIA_ATD.1c** ensures that the proper attributes are associated with users.

OE.PROTECT_COMMS

The IT Environment shall protect the transport of audit records to the audit server, and authentication server and time server communications with the TOE, and remote network management, in a manner that is commensurate with the risks posed to the network.

Coverage Rational:

FTP_ITC_EXP.1b provides a trusted channel for services provided by the IT environment to the TOE. **FCS_CKM.1b**, **FCS_CKM.2b**, and **FCS_CKM.4b** and **FCS_COP.1b** mandate usage of a FIPS 140-2 validated cryptographic module for the trusted channel encryption, as well as for the management of the corresponding cryptographic keys.

OE.RESIDUAL

The 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.

Coverage Rational:

> **FDP_RIP.1b** addresses this objective by requiring the IT environment to provide the same protection for residual information in network packet objects that the TOE provides.

8.2.3 Security Functional Requirements Dependencies

Table 8-4 shows the dependencies between the functional requirements. All dependencies are satisfied.

Table 8-4 Security Functional Requirements Dependencies Satisfied

Item #	SFR	Dependencies	
		SFR	Included
TOE Security Functional Requirements			
1	FAU_ARP.1 Security alarms	FAU_SAA.1	2
2	FAU_SAA.3 Simple attack heuristics	none	-
3	FAU_GEN.1a Audit data generation	FPT_STM.1	24
4	FAU_GEN.2 User identity association	FAU_GEN.1	3
		FIA_UID.1	8
5	FAU_SEL.1 Selective audit	FAU_GEN.1	3
		FMT_MTD.1	32
6	FIA_UAU.1a Timing of authentication	FIA_UID.1	8
7	FIA_UAU_EXP.5a Multiple authentication mechanisms	none	-
8	FIA_UID.2a User identification before any action	none	-
9	FIA_ATD.1a Administrator attribute definition	none	-
10	FIA_ATD.1b User attribute definition	none	-
11	FIA_USB.1 User-subject binding	FIA_ATD.1	11, 12
12	FTA_SSL.3 TSF-initiated termination	none	-

Item #	SFR	Dependencies	
		SFR	Included
13	FCS_CKM.1a Cryptographic key generation	FCS_CKM.2 or FCS_COP.1	16, 17 19
		FCS_CKM.4	18
		FMT_MSA.2	31
14	FCS_CKM.2a Cryptographic key distribution	FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1	19
		FCS_CKM.4	18
		FMT_MSA.2	31
15	FCS_CKM_EXP.2 Cryptographic key establishment	FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1	19
		FCS_CKM.4	18
		FMT_MSA.2	31
16	FCS_CKM.4a Cryptographic key destruction	FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1	19
		FMT_MSA.2	31
17	FCS_COP.1a Cryptographic operation	FDP_ITC.1 or FCS_CKM.1	19
		FCS_CKM.4	18
		FMT_MSA.2	31
18	FDP_PUD_EXP.1 Protection of User Data	none	-
19	FDP_RIP.1a Subset residual information protection	none	-
20	FPT_RVM.1a Non-bypassability of the TSP	none	-
21	FPT_SEP.1a TSF domain separation	none	-
22	FPT_STM_EXP.1 Reliable time stamps	none	-
23	FPT_TST_EXP.1 TST testing	FCS_COP.1	19
24	FPT_TST_EXP.2 TST testing of Cryptographic Modules	none	-
25	FMT_MOF.1a Management of security functions behavior (Cryptographic Functions)	FMT_SMF.1	35, 37
		FMT_SMR.1	40

Item #	SFR	Dependencies	
		SFR	Included
26	FMT_MOF.1b Management of security functions behavior (Audit Record Generation)	FMT_SMF.1	36
		FMT_SMR.1	40
27	FMT_MOF.1c Management of security functions behavior (Authentication)	FMT_SMF.1	39
		FMT_SMR.1	40
28	FMT_MOF.1d Management of security functions behavior (Wireless Intrusion Protection)	FMT_SMF.1	38
		FMT_SMR.1	40
29	FMT_MSA.2 Secure security attributes	ADV_SPM.1	
		FDP_ACC.1 or FDP_IFC.1	
		FMT_MSA.1	
		FMT_SMR.1	40
30	FMT_MTD.1a Management of Audit data	FMT_SMF.1	36
		FMT_SMR.1	40
31	FMT_MTD.1b Management of Authentication data (Administrator)	FMT_SMF.1	39
		FMT_SMR.1	40
32	FMT_MTD.1c Management of Authentication data (User)	FMT_SMF.1	39
		FMT_SMR.1	40
33	FMT_SMF.1a Specification of management functions (Cryptographic Functions)	none	-
34	FMT_SMF.1b Specification of management functions (TOE Audit Record Generation)	none	-
35	FMT_SMF.1c Specification of management functions (Cryptographic Key Data)	none	-
36	FMT_SMF.1d Specification of management functions (Wireless Intrusion Protection)	none	-
37	FMT_SMF.1e Specification of management functions (TOE Authentication Data)	none	-
38	FMT_SMR.1a Security roles	FIA_UID.1	8
39	FTP_ITC_EXP.1a Inter-TSF trusted channel	none	-
40	FTP_TRP.1a Trusted path (Remote Administrator)	none	-
41	FTP_TRP.1b Trusted path (Wireless User open system)	none	-
Security Requirements for IT Environment			
41	FAU_GEN.1b Audit data generation	FPT_STM.1	59

Item #	SFR	Dependencies	
		SFR	Included
42	FAU_SAR.1 Audit review	FAU_GEN.1	1, 43
43	FAU_SAR.2 Restricted audit review	FAU_SAR.1	44
44	FAU_SAR.3 Selectable audit review	FAU_SAR.1	44
45	FAU_STG.1 Protected audit trail storage	FAU_GEN.1	1, 43
46	FAU_STG.3 Prevention of audit data loss	FAU_STG.1	47
47	FIA_UAU_EXP.5b Remote authentication mechanism	FIA_UID.1	50
48	FIA_UID.2b User identification before any action	none	-
49	FIA_ATD.1c User attribute definition	none	-
50	FCS_CKM.1b Cryptographic key generation	FCS_CKM.2 or FCS_COP.1	53 55
		FCS_CKM.4	54
		FMT_MSA.2	31
51	FCS_CKM.2b Cryptographic key distribution	FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1	52
		FCS_CKM.4	54
		FMT_MSA.2	31
52	FCS_CKM.4b Cryptographic key destruction	FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1	52
		FMT_MSA.2	31
53	FCS_COP.1b Cryptographic operation	FDP_ITC.1 or FCS_CKM.1	52
		FCS_CKM.4	54
		FMT_MSA.2	31
54	FDP_RIP.1b Subset residual information protection	none	-
55	FPT_RVM.1b Non-bypassability of the TSP	none	-
56	FPT_SEP.1b TSF domain separation	none	-
57	FPT_STM.1 Reliable time stamps	none	-
58	FMT_MOF.1e Management of security functions behavior	FMT_SMF.1	62
		FMT_SMR.1	63

Item #	SFR	Dependencies	
		SFR	Included
59	FMT_MTD.1d Management of TSF data	FMT_SMF.1	62
		FMT_SMR.1	63
60	FMT_SMF.1f Specification of Management Functions	none	-
61	FMT_SMR.1b Security roles	FIA_UID.1	50
62	FTP_ITC_EXP.1b Inter-TSF trusted channel	none	-
63	FTP_TRP.1a Trusted path	none	-
63	FTP_TRP.1b Trusted path	none	-

Note: Since FAU_SAA.3 is hierarchical to FAU_SAA.1, the dependency of FAU_ARP.1 on FAU_SAA.1 is satisfied. Similarly, since FIA_UID.2 is hierarchical to FIA_UID.1, dependencies of FAU_GEN.2, FMT_SMR.1, and FIA_UAU.1 on FIA_UID.1 are satisfied. In accordance with the requirements of the PP, FMT_MSA.2 is included only as a dependency of the Cryptographic Support family (FCS_CKM and FCS_COP). As there is no requirement for the TOE to implement an access control policy, the dependency of FMT_MSA.2 on ADV_SPM.1, the FDP class components and FMT_MSA.1 does not apply. All other included dependencies are relevant for this ST.

8.2.4 Explicitly Stated Requirements

FIA_UAU_EXP.5a and FIA_UAU_EXP.5b, Multiple authentication mechanisms, was explicitly stated because there is concern over whether or not existing CC requirements specifically require that the TSF provide authentication, and this TOE includes options for authentication to be provided by an authentication server in the IT Environment (see rationale in the PP for further discussion).

FCS_CKM_EXP.2, Cryptographic key establishment, was explicitly stated because the CC does not specifically provide components for key handling and storage.

FDP_PUD_EXP.1, Protection of User Data, was explicitly stated because the IFC/AFC requirements of the Common Criteria do not accommodate access control policies that are not object/attribute based.

FPT_STM_EXP.1, Reliable time stamps, was explicitly stated because the CC does not specifically provide a component which permits acquisition of reliable time stamps from the IT Environment, and for conformance with the PP the TOE is required to obtain time stamps from an external NTP time server.

FPT_TST_EXP.1, TSF testing, was explicitly stated because there are a number of issues concerning the CC version of the FPT_TST.1 component that would make its use inconsistent with the requirements of the PP (see rationale in the PP for further discussion).

FPT_TST_EXP.2, TSF testing of Cryptographic Modules, was explicitly stated because the CC basic self test requirement in FPT_TST.1 does not specify the required elements for testing of cryptographic functions, as required by the PP.

FTP_ITC_EXP.1a and FTP_ITC_EXP.1b, Inter-TSF trusted channel, was explicitly stated 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.

The assurance requirements at EAL2 are sufficient to support these explicitly stated requirements.

8.2.5 Strength of Function

Strength of function level of SOF-basic counters an attack level of low. The environment is one where the potential attacker is unsophisticated, with access to only standard equipment and public information about the product.

8.2.6 EAL Justification

CC part 3 states:

> *"EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practice. As such it should not require a substantially increased investment of cost or time.*
>
> *EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited."*

Evaluation Assurance Level EAL2, augmented with ACM_SCP.1 (CM Coverage), ALC_FLR.2 (Flaw Remediation) and AVA_MSU.1 (Misuse – Examination of guidance), in this ST was chosen for conformance with the PP requirement to invoke the Basic Robustness Assurance Package and due to the requirement for moderate independent security assurance within cost and time constraints of the sponsor i.e. Aruba Networks.

8.3 TOE Summary Specification Rationale

8.3.1 IT Security Functions

Table 8-5 shows that the IT Security Functions in the TOE Summary Specification (TSS) address all of the TOE Security Functional Requirements.

Table 8-5 Mapping of Functional Requirements to TOE Summary Specification

Security Functions	SFRs	Rationale
Wireless Intrusion Protection	FAU_ARP.1 FAU_SAA.3	The TOE detects defined wireless intrusion attempts (**FAU_SAA.3**), alerts the administrator and, if possible, prevents or contains the intrusion attempt (**FAU_ARP.1**).
Auditing	FAU_GEN.1a FAU_GEN.2 FAU_SEL.1	The TOE generates audit records of the auditable security-relevant events (**FAU_GEN.1a**) and associates with each user event the identity of the user that caused the event (**FAU_GEN.2**). The Mobility Controller provides the capability to include or exclude auditable events (**FAU_SEL.1**) based on user identity, event type, device interface and wireless client identity.

Security Functions	SFRs	Rationale
I&A and TOE Access	FTA_SSL.3 FTA_TAB.1 FIA_UAU.1a FIA_UAU_EXP.5a FIA_UID.2a FIA_ATD.1a FIA_ATD.1b FIA_USB.1	The Mobility Controller displays a warning banner regarding authorized use of the TOE before establishing an administrator session (**FTA_TAB.1**). The Mobility Controller requires each user to be successful identified before allowing any TSF-mediated action (**FIA_UID.2a**). The Mobility Controller requires each user to be successfully authenticated, before allowing any TSF-mediated action except identification (**FIA_UAU.1a**). The TSF employs multiple authentication mechanisms,including an internal mechanism and an external RADIUS authentication server (**FIA_UAU_EXP.5a)**. A username and password is maintained for each administrator **(FIA_ATD.1a)**. A session key and role are maintained for each remotely authenticated wireless user **(FIA_ATD.1b)**. The username of an authenticated session is associated with processes acting on behalf of the user (**FIA_USB.1**). The Mobility Controller will terminate a wireless user or administrator session after a session idle timeout (**FTA_SSL.3**).
Cryptography	FCS_CKM.1a FCS_CKM.2a FCS_CKM_EXP.2 FCS_CKM.4a FCS_COP.1a	The Mobility Controller uses services of a FIPS 140-2 approved cryptographic module and specific FIPS approved cryptographic algorithms and cryptographic key sizes when it performs cryptographic operations **(FCS_COP.1a)** The Mobility Controller uses services of a FIPS 140-2 approved cryptographic module when it generates, distributes, establishes and destroys cryptographic keys (**FCS_CKM.1a, FCS_CKM.2a, FCS_CKM_EXP.2, FCS_CKM.4a)**.

Security Functions	SFRs	Rationale
User and TSF Data Protection	FDP_PUD_EXP.1 FDP_RIP.1a FPT_RVM.1a FPT_SEP.1a FPT_STM_EXP.1 FPT_TST_EXP.1 FPT_TST_EXP.2	If configured by the administrator, the Aruba Mobility Controller encrypts data transmitted to the wireless client and decrypts data received from the wireless client (**FDP_PUD_EXP.1**). The Mobility Controller clears resources used to process network packet objects prior to allocation of the resource (**FDP_RIP.1a**). Aruba Mobility Controllers provide well-defined interfaces, consistent implementation of security functions, clear representation of users, installation and configuration support for security (**FPT_RVM.1a**, **FPT_SEP.1a**). The Mobility Controller provides reliable time stamps, obtained from an external NTP time server, that are used in audit events (**FPT_STM_EXP.1**). The Mobility Controller runs a suite of hardware self tests during start-up or on request from the administrator and provides the capability for the administrator to use cryptographic functions to verify the integrity of TSF executable code and data (**FPT_TST_EXP.1**). The Mobility Controller runs the suite of FIPS 140-2 validated cryptographic module self tests during start-up or on request from the administrator, including immediately after generation of a key (**FPT_TST_EXP.2**).

Security Functions	SFRs	Rationale
Security Management	FMT_MSA.2 FMT_MOF.1a FMT_MOF.1b FMT_MOF.1c FMT_MOF.1d FMT_MTD.1a FMT_MTD.1b FMT_MTD.1c FMT_SMF.1a FMT_SMF.1b FMT_SMF.1c FMT_SMF.1d FMT_SMF.1e FMT_SMR.1a	Only the Mobility Controller's administrator (**FMT_SMR.1a**) has the ability to manage the behavior of the TOE security functions **(FMT_MOF.1a, FMT_MOF.1b, FMT_MOF.1c, FMT_MOF.1d)**. Only the administrator can manage manage TSF data (**FMT_MTD.1a, FMT_MTD.1b, FMT_MTD.1c).** Only secure values are accepted for cryptographic keys used by the TOE (**FMT_MSA.2**). The Mobility Controller maintains the administrator and user roles, and will associate users with roles **(FMT_SMR.1a)**. The Mobility Controller provides interfaces that can be used to manage the security functions (**FMT_SMF.1a, FMT_SMF.1b, FMT_SMF.1c, FMT_SMF.1d, FMT_SMF.1e**).
Trusted path/channels	FTP_TRP.1a FTP_TRP.1b FTP_ITC_EXP.1a	The Mobility Controller provides a trusted communication path between itself and the remote administrator when the remote administrator initially authenticates as a wired user (**FTP_TRP.1a**). The Mobility Controller provides a trusted communication path between itself and the wireless user when the wireless user authenticates using an open system connection (**FTP_TRP.1b**). The Mobility Controller provides trusted channels between itself and external audit/authentication/time servers using the IPSec/IKE security protocol **(FTP_ITC_EXP.1a)**.

8.3.2 Assurance Measures

Table 6-2 Assurance Measures in Section 6.2 shows how all assurance requirements are satisfied.

8.4 PP Claims Rationale

8.4.1 TOE Security Environment

The PP claims rationale justifies any differences between the ST and the PP TOE security environment; the statements of threats, assumptions and organizational security policies. This justification is provided in Table 8-6 Rationale for Difference between ST and PP TOE Security Environment below.

Table 8-6 Rationale for Difference between ST and PP TOE Security Environment

PP TOE Security Environment	ST TOE Security Environment	Difference Rationale
A.NO_EVIL	A.ADMIN	Name change only
A.NO_GENERAL_PURPOSE	A.NO_GENRL	Name change only
A.PHYSICAL	A.LOCATE	Name change only
A.TOE_NO_BYPASS	A.BYPASS	Name change only
T.ACCIDENTAL_ADMIN_ERROR	T.ERROR	Name change; semantically equivalent
T.ACCIDENTAL_CRYPTO_COMPROMISE	T.CRYPTO	Name change only
T.MASQUERADE	T.IMPERSON	Name change; semantically equivalent
T.POOR_DESIGN		This is a threat to the TOE development, not to the TOE
T.POOR_IMPLEMENTATION		This is a threat to the TOE development, not to the TOE
T.POOR_TEST		This is a threat to the TOE development, not to the TOE
T.RESIDUAL_DATA	T.RESIDUAL	Name change only
T.TSF_COMPROMISE	T.INTERNAL	Name change only
T.UNATTENDED_SESSION	T.SESSION	Name change only
T.UNAUTHORIZED_ACCESS	T.ATTACK	Name change; semantically equivalent
T.UNAUTH_ADMIN_ACCESS	T.ACCESS	Name change only

PP TOE Security Environment	ST TOE Security Environment	Difference Rationale
P.ACCESS_BANNER	P.BANNER	Name change only
P.ACCOUNTABILITY	P.ACCOUNT	Name change only
P.CRYPTOGRAPHIC	P.CRYPTO	Name change; semantically equivalent
P.CRYPTOGRAPHY_VALIDATED	P.CRYPTO	Name change; semantically equivalent
P.ENCRYPTED_CHANNEL	P.CHANNEL	Name change only
P.NO_AD_HOC_NETWORKS	P.NO_ADHOC	Name change only

8.4.2 Security Objectives

The PP claims rationale also justifies any differences between the ST and the PP security objectives. This justification is provided in Table 8-7 Rationale for Difference between ST and PP Security Objectives below.

Table 8-7 Rationale for Difference between ST and PP Security Objectives

PP Security Objectives	ST Security Objectives	Difference Rationale
Security Objectives for the TOE		
O.AUDIT_GENERATION	O.AUDIT_GEN	Name change; semantically equivalent
O.CORRECT_TSF_OPERATION	O.CORRECT	Name change only
O.CRYPTOGRAPHY	O.CRYPTO	Name change; semantically equivalent
O.CRYPTOGRAPHY_VALIDATED	O.CRYPTO	Name change; semantically equivalent
O.DISPLAY_BANNER	O.BANNER	Name change; semantically equivalent
O.MANAGE	O.MANAGE	Semantically equivalent
O.MEDIATE	O.TRAFFIC	Name change; semantically equivalent
O.RESIDUAL_ INFORMATION	O.RESIDUAL	Name change; semantically equivalent
O.SELF_PROTECTION	O.SELF_PROTECT	Name change only
O.TIME_STAMPS	O.TIME	Name change; semantically equivalent
O.TOE_ACCESS	O.TOE_ACCESS	Semantically equivalent
O.ADMIN_GUIDANCE		This is an objective for the TOE development, not for the TOE

PP Security Objectives	ST Security Objectives	Difference Rationale
O.CONFIGURATION_ IDENTIFICATION		This is an objective for the TOE development, not for the TOE
O.DOCUMENTED_ DESIGN		This is an objective for the TOE development, not for the TOE
O.PARTIAL_ FUNCTIONAL_TESTING		This is an objective for the TOE development, not for the TOE
O.VULNERABILITY_ ANALYSIS		This is an objective for the TOE development, not for the TOE
	O.INTRUSION	Additional to the PP
Security Objectives for the IT and Non IT Environment		
OE.AUDIT_PROTECTION	OE.AUDIT_PROTECT	Name change only
OE.AUDIT_REVIEW	OE.AUDIT_REVIEW	Identical
OE.MANAGE	OE.MANAGE	Identical
OE.NO_EVIL	OE.ADMIN	Name change; semantically equivalent
OE.NO_GENERAL_PURPOSE	OE.NO_GENRL	Name change only
OE.PHYSICAL	OE.PROTECT	Name change only
OE.PROTECT_MGMT_COMMS	OE.PROTECT_COMMS	Name change; semantically equivalent
OE.RESIDUAL_INFORMATION	OE.RESIDUAL	Name change only
OE.SELF_PROTECTION	OE.SELF_PROTECT	Name change; semantically equivalent
OE.TIME_STAMPS	OE.TIME	Name change; semantically equivalent
OE.TOE_ACCESS	OE.TOE_ACCESS	Semantically equivalent
OE.TOE_NO_BYPASS	OE.BYPASS	Name change only

8.4.3 TOE and IT Environment SFRs

Finally, the PP claims rationale justifies any differences between the TOE and IT Environments SFRs specified in this ST and the PP SFRs specified in [3], other than valid assignment, iteration and selection operations. This justification is provided in Table 8-8 Rationale for Difference between ST SFRs and PP SFRs below.

Table 8-8 Rationale for Difference between ST SFRs and PP SFRs

PP SFR	ST SFR	Difference Rationale
TOE Security Functional Requirements		
FAU_GEN.1(1)	FAU_GEN.1a	The ST SFR requires auditable events for the [not specified] level of audit, rather than the [minimum] level of audit – in fact, all of the PP required auditable events are included explicitly in Table 5-3 TOE Auditable Events, and the [not specified] level of audit is selected to apply to additional ST SFRs. The PP auditable event for the FCS_CKM.1 SFR should apply to FCS_CKM_EXP.2 and the auditable event for FCS_CKM.1 should be on success or failure of key generation. The ST auditable events for these SFRs have been modified accordingly. The PP auditable event for the FTP_TRP.1 SFR is incorrectly worded, referring to a trusted channel, rather than a trusted path – the ST auditable events for the FTP_TRP.1a and FTP_TRP.1b SFRs have been corrected to refer to trusted path.
FIA_AFL.1(1)		The PP SFR is not applicable to the TOE in the evaluated configuration. Remote administrator authentication failure handling is performed by the RADIUS server for the wired user account, which is used for initial logon. Local administrators are not subject to lockout.
FTA_SSL.3	FTA_SSL.3	The ST SFR is a refinement of the PP SFR, the refinement being made to apply sessions termination to all user sessions, wireless user and administrator, whether locally or remotely authenticated. Additionally, the fixed idle timeout of 30 minutes for the termination of a Web UI session is taken to narrow the requirement and to be a refinement.
FAT_TAB.1	FAT_TAB.1	The PP SFR has been modified in the ST SFR to make it clear that the access banner is only required by the PP to be displayed for administrators.

PP SFR	ST SFR	Difference Rationale
FCS_BCM_EXP.1 FCS_CKM_.1 FCS_CKM_EXP.2 FCS_CKM.4 FCS_COP_EXP.1 FCS_COP_EXP.2	FCS_CKM.1a FCS_CKM_EXP.2 FCS_CKM.4a FCS_COP.1a	The ST SFRs fully meet the requirements of the PP SFRs. The ST SFRs have been re-drafted to conform more completely with the CC Part 2 FCS components. FCS_BCM_EXP.1 is met by explicitly including in the ST SFRs the requirement to provide the cryptographic services using a FIPS 140-2 validated cryptographic module. FCS_COP_EXP.1 and FCS_COP_EXP.2 are met by the cryptographic operations specified in FCS_COP.1a. Note that FCS_CKM.2a is an additional requirement for the TOE to provide automatic cryptographic key distribution, in addition to the manual key establishment provided by the PP SFR FCS_CKM_EXP.2.
FDP_PUD_EXP.1	FDP_PUD_EXP.1	The PP SFR has been refined in the ST SFR to extend the encrypted path to include the path between the radio interface of the AP and the Mobility Controller TOE.
FPT_TST_EXP.2	FPT_TST_EXP.2	The ST SFR is a refinement of the PP SFR, the refinement being made to restrict the PP required FIPS 140-1/2 cryptomodule to the FIPS 140-2 validated cryptographic module.
FMT_SMF.1(1)	FMT_SMF.1a	The PP SFR has been modified in the ST SFR to refer to FCS_COP.1 instead of FCS_COP_EXP.2.
FMT_SMR.1(1)	FMT_SMR.1a	The ST SFR is a refinement of the PP SFR. The TOE implements an administrator defined set of wireless user roles. The refinement brings the full set of wireless user roles under TSF control.

PP SFR	ST SFR	Difference Rationale
FTP_TRP.1	FPT_TRP.1a FPT_TRP.1b	The PP SFR is considered to be in error, because the trusted path protecting authentication of wireless users using 802.11i is set up between the IT Environment and the wireless user and not the TOE and the wireless user. ST SFR FTP_TRP.1c has therefore been included in the IT environment SFRs. TOE SFR FTP_TRP.1b reflects the provision of the trusted path between the wireless user and the TOE in the case where the authentication uses an open system connection (not using 802.11i) and is protected using a VPN. The PP also fails to provide for trusted path between the TOE and the remote administrator. PP SFR FTP_TRP.1a has been included to address protection for the remote administrator authentication dialogue.
IT Environment Security Functional Requirements		
FAU_GEN.1(2)	FAU_GEN.1b	The ST SFR requires auditable events for the [not specified] level of audit, rather than the [minimum] level of audit – in fact, all of the PP required auditable events are included explicitly in Table 5-6 TOE IT Environment Auditable Events, and the [not specified] level of audit is selected to apply to additional ST SFRs. The PP Auditable event for FIA_AFL.1(2) is met by the ST TOE auditable events for FIA_AFL.1a and FIA_AFL.1b.
FIA_AFL.1(2)	FIA_AFL.1	The PP SFR has been modified in the ST SFR to make it clear that the handling of authentication failures applies to failed user authentication attempts, not to users logging on.
FIA_UID.1	FIA_UID.2b	The ST SFR is hierarchical to the PP SFR.
FMT_MTD.1(4)	FMT_MTD.1d	The ST SFR is a refinement of the PP SFR, the refinement being made to restrict management to “the ability to modify”, as well as “set initial value of”, to restrict management to the administrator only, and to bring other TSF data under TSF control.

PP SFR	ST SFR	Difference Rationale
FMT_MOF.1c	FMT_MOF.1(3)	The PP SFR has been modified in the ST to remove the setting of the number of authentication failures before lockout, as this is handled in the IT Environment.

8.5 Rationale for Satisfaction of Strength of Function Claims

The claimed minimum strength of function is SOF-basic. The following security mechanisms have specific SOF claims.

The strength of the password-based authentication mechanism (including serial console, SSH and Web Interfaces for administrators and for wireless users) is:

> Passwords are required to be at least six characters long. Numeric, alphabetic (upper and lowercase), and extended characters can be used, which gives a total of 95 characters to choose from. Therefore, the number of potential six-character passwords is 95^6 (735,091,890,625).
>
> Aruba 6000 and Aruba 800 series Mobility Controllers have been FIPS 140-2 validated to enforce the metric that the probability of authentication success within one minute is less than 1 in 100,000 both for password-based authentication and pre-shared key-based authentication. The enforcement of the FIPS metric is based on performance restrictions of the authentication protocols. This leads an approximate exploit time of 100,000/(24*60) = 69 days, which is more than one month and satisfies the requirements of SOF-basic, as detailed in CEM Part 2 Annex B.
>
> To satisfy the claimed SOF-basic minimum strength of function, it is necessary to consider the worst case in which a dictionary word is selected using single case letters. Based on estimates of the number of commonly used English words having one, through to six, letters and the possible combinations to form a six letter word, it has been calculated that the exploit time would reduce to approximately 6000/(24*60) = 4 days. This still just satisfies the requirements of SOF-basic, as detailed in CEM Part 2 Annex B.

The strength of the pre-shared key-based IKE handshake is:

> Pre-shared keys must be at least 32 characters long and up to 64 bytes long with a random construction comprising mixed case alphabetic, numeric and special characters.
>
> With this construction, the following analysis shows that the key is uncrackable:
>
> a) No rainbow tables can be found for the length and construction of the secret and a brute force attack must therefore be assumed
>
> b) The number of possible secrets is approximately $100^{32} = 10^{64}$.

c) Assuming 10^6 hashes may be processed per second, 3×10^{13} hashes may be processed in one year.

d) Therefore the secret is uncrackable in any practical terms.

9 Appendix

Table 9-1 Acronyms

AAA	Authentication, authorization and accounting
AES	Advanced Encryption Standard
AP	Access Point
CC	Common Criteria [for IT Security Evaluation]
CLI	Command Line Interface
CPU	Central Processing Unit
DES	Data Encryption Standard
DOS	Denial of Service
EAL	Evaluation Assurance Level
EAP	Extensible Authentication Protocol
EAP-TLS	Extensible Authentication Protocol Transport Layer Security
EAP-TTLS	EAP Tunneled TLS
FIPS 140-2	Federal Information Processing Standard Publication 140-2
HMAC	Keyed-Hash Message Authentication Code
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
IKE	Internet Key Exchange
IP	Internet Protocol
IPSec	Internet Protocol Security
IT	Information Technology
LAN	Local Area Network
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OS	Operating System
PCI	Peripheral Component Interconnect
PEAP	Protected Extensible Authentication Protocol
PKCS	Public-Key Cryptography Standards
PRNG	Pseudorandom number generator
RADIUS	Remote Authentication Dial-In User Service
RF	Radio Frequency
RFC	Request For Comments
SF	Security Function
SFP	Security Function Policy
SHS	Secure Hash Standard
SOS	SiByte OS
SSH	Secure Shell
SSID	Service Set Identifier
ST	Security Target
TDES	Triple DES
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
UDP	User Datagram Protocol

UI	User Interface
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy or Wireless Encryption Protocol
WIP	Wireless Intrusion Protection
WLAN	Wireless Local Area Network
WPA	WiFi Protected Access

Table 9-2 References

Ref. #	Reference title
[1]	Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005: Part 1 Introduction and general model, CCMB-2005-08-001 Part 2 Security functional requirements, CCMB-2005-08-002 Part 3 Security assurance requirements, CCMB-2005-08-003
[2]	Cryptographic Module Security Policy for the Aruba Mobility Controller (Certificate #649), http://csrc.nist.gov/cryptval/140-1/1401val2006.htm#649.
[3]	Wireless Local Area Network (WLAN) Access System Protection Profile for Basic Robustness Environments, Version 1.0, April 2006