Hewlett-Packard Company Wireless LAN Access Controllers and Access Points Security Target

Version 1.0
31 October 2014

Prepared for:
Hewlett-Packard Development Company, L.P.

11445 Compaq Center Drive West
Houston, Texas 77070

Prepared by:

Leidos Inc (formerly Science Applications International Corporation)

Common Criteria Testing Laboratory
6841 Benjamin Franklin Drive, Columbia, Maryland 21046

LIST OF TABLES

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is a series of products that are divided into 2 categories, Access Controllers (module or appliance) and Access Points.

The Access Controller portfolio consists of switch modules and unified appliances that integrate switches and access controller into a single box. Access Controllers are designed to meet different use cases such as campus, building or branch office.

HP offers IEEE 802.11n wireless access points, ranging from single-radio 802.11a/b/g/n to dual 802.11a/b/g/n APs. The MSM access points are wireless devices that provide expanded connectivity for existing networks. The MSM access points provide wireless coverage in managed mode as well as autonomous mode without a controller. All Access Point types work in control mode, also referred to as managed, Fit or FIT mode. In FIT mode, the access point can only be managed through the Access Controller.

Working in unison with HP controllers, the HP MSM-802.11n Access Point Series offers near gigabit client access and increased reliability compared to legacy models. The MSM-802.11n Access Point Series are ideal for voice and multi-media communications while providing full compatibility with legacy 802.11 clients and existing HP wireless controllers.

The Security Target contains the following additional sections:

- TOE Description (Section 2)
- Security (Section 3)
- Security Objectives (Section 4)
- IT Security Requirements (Section 5)
- TOE Summary Specification (Section 6)
- Protection Profile Claims (Section 7)
- Rationale (Section 8).

1.1 Security Target, TOE and CC Identification

ST Title – Hewlett-Packard Company WLAN Controllers and Access Points Security Target

ST Version – Version 1.0

ST Date – 10/31/2014

TOE Identification – Hewlett-Packard Company Wireless LAN Controllers and Access Points with Comware v5.2.109

The WLAN products in the evaluated configuration comprise the following:

- Access Controllers
  - HP 10500/7500 20G Unified Wired-WLAN Module (JG639A)
  - HP 830 8-Port PoE+ Unified Wired-WLAN Switch (JG641A)
  - HP 830 24-Port PoE+ Unified Wired-WLAN Switch (JG640A)
  - HP 850 Unified Wired-WLAN Appliance (JG722A)
  - HP 870 Unified Wired-WLAN Appliance (JG723A)
- Access Points
  - HP MSM430 Dual Radio 802.11n Access Point —Models AM (J9650A), WW (J9651A), JP (J9652A), IL (J9653A), TAA (J9654A)
  - HP MSM460 Dual Radio 802.11n Access Point—Models AM (J9590A), WW (J9591A), JP (J9589A), IL (J9618A), TAA (J9655A)
  - HP MSM466 Dual Radio 802.11n Access Points—Models AM (JJ9621A), WW (J9622A), JP (J9620A), IL (J9619A), TAA (J9656A)

- HP MSM466-R Dual Radio Outdoor 802.11n Access Point—Models AM (J9715A), WW (J9716A), JP (J9717A), IL (J9718A)
- HP 560 Wireless Dual Radio 802.11n Access Point—Models AM (J9845A), WW (J9846A), JP (J9847A), IL (J9848A).

Note: The model designations above represent the different regulatory domain variants that consist of a different bit being set in the manufacturing process that is not customer configurable. This bit identifies which regulatory domain these APs should operate in and restricts the available frequency of operation. The designations are defined as: (AM) = Americas; (WW) = World Wide; (JP) = Japan; (IL) = Israel; and (TAA) = US Trade Agreements Act.

TOE Developer – Hewlett-Packard Company

Evaluation Sponsor – Hewlett-Packard Company

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009

1.2 Conformance Claims

This TOE is conformant to the following CC specifications:

- *Protection Profile for Wireless Local Area Network (WLAN) Access Systems*, version 1.0, 01 December 2011 (WLASPP)
- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 3, July 2009.
    - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 3, July 2009.
    - Part 3 Conformant

1.3 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In the ST the iteration number is shown in parenthesis following the component identifier.
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …"). All refinement operations that are completed in the PP are not identified in the ST.
    - Extended Requirements are allowed to create requirements should the Common Criteria not offer suitable requirements to meet the ST needs. To ensure these requirements are explicitly identified, the ending "_EXT" is appended to the newly created short name and the component.
- The WLASPP uses an additional convention – the 'case' – which defines parts of an SFR that apply only when corresponding selections are made or some other identified conditions exist. Only the applicable cases are identified in this ST and they are identified using **bold** text.

- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.3.1 Abbreviations

AAA	Authentication, Authorization, and Accounting
AES	Advanced Encryption Standard
AP	Access Point
CC	Common Criteria
CLI	Command Line Interface
DoS	Denial of Service
EAP	Extensible Authentication Protocol
FPGA	Field Programmable Gate Array
FIPS	Federal Information Processing Standard
GUI	Graphical User Interface
IKE	Internet Key Exchange
IPsec	Internet Protocol Security
MAC	Media Access Control or Message Authentication Code
HMAC	Hashed Message Authentication Code
NAT	Network Address Translation
NTP	Network Time Protocol
PoE+	Power over Ethernet
PP	Protection Profile
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RF	Radio Frequency
RNG	Random Number Generator
SSH	Secure Shell
TACACS+	Terminal Access Controller Access-Control System +
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

2. TOE Description

The Target of Evaluation (TOE) includes Access Controllers and Access Points from the Hewlett-Packard family of Wireless LAN products. The WLAN products in the evaluated configuration include the HP 10500/7500 20G

Unified Wired-WLAN Module, HP 830 8-Port and 24-Port PoE+ Unified Wired-WLAN Switches, HP 850 and 870 Unified Wired-WLAN Appliances, HP MSM430, 460 and 466 Dual Radio 802.11n Access Points (Models AM, WW, JP, IL, TAA), the HP MSM466-R Dual Radio Outdoor 802.11n Access Point (Models AM, WW, JP, IL, TAA) and the HP 560 Wireless Dual Radio 802.11n Access Point (Models AM, WW, JP, IL, TAA).

2.1 TOE Overview

The HP Wireless LAN appliances consist of hardware and software components. While the physical form factor of each distinct series in the TOE differs, the underlying hardware shares a similar architecture. The software utilized is a common code base of a modular nature with only the modules applicable for the specific hardware installed. The TOE appliances include dedicated Access Controllers, Access Points, and switch appliances with Access Controller modules – all of which service wireless clients ensuring the wireless communication is secure and connecting those clients to wired networks.

HP 10500/7500 20G Unified Wired-WLAN Module

The HP 10500/7500 20G Unified Wired-WLAN Module is a wireless access controller product designed for the HP 10500 and 7500E series Ethernet switches. It provides user control and management, RF management and security mechanism, fast roaming, QoS and IPv4/IPv6 features, and WLAN access control capability. Designed for WLAN access of enterprise networks and metropolitan area networks (MANs), this module provides access control solutions for WLAN access of large enterprise campus networks, wireless MAN coverage and hot spot coverage.

The HP 10500/7500 20G Unified Wired-WLAN Access Controller module can support up to 1024 APs. The support chassis types, model numbers and maximum number of configurable modules supported by HP 10500 and 7500E Ethernet switch series is listed below.

- HP A7510 Switch Chassis (JD238B) : 9
- HP A7506 Switch Chassis (JD239B) : 5
- HP A7503 Switch Chassis (JD240B) : 2
- HP A7506-V Switch Chassis (JD241B) : 5
- HP A7502 Switch Chassis (JD242B) : 1
- HP A7503-S Switch Chassis (JD243B) : 2
- HP A10508-V Switch Chassis (JC611A) : 7
- HP A10508 Switch Chassis (JC612A) : 7
- HP A10504 Switch Chassis (JC613A) : 3
- HP 10512 Switch Chassis (JC748A) :11

HP 830 24/8-Port PoE+ Unified Wired-WLAN Switch

HP 830 series unified switch is the Integrated Gigabit Ethernet (GE) switching and wireless networking solution best suited for small to medium businesses and remote offices of large enterprises. This series provides 10/100/1000 Base-T interfaces, supports PoE+ and with 802.11a/b/g/n compliant. Both HP 830 series models: 24P and 8P; provide HP Fit Access Point (AP) access control providing wired and wireless solutions.

HP 850/870 Unified Wired-WLAN Appliance

The HP 850 and 870 Unified Wired-WLAN Appliances are next generation 40G products. By employing new multi-core Network Processors, switch ASICs and FPGAs, they have large capacity, high reliability and offer wired and wireless data processing capacity. Both appliances provide user control and management, RF management and security mechanisms, fast roaming, QoS and IPv4/IPv6 features, and WLAN access control functions. Designed for WLAN access of enterprise networks and metropolitan area networks (MANs), these appliances provide access control solutions for WLAN access of large enterprise campus networks, wireless MAN coverage and hot spot coverage.

HP MSM430/460/466/466-R and 560 Dual Radio Access Points

HP offers intelligent IEEE 802.11n wireless access points, ranging from single-radio 802.11a/b/g/n to dual 802.11a/b/g/n access points. The MSM access points are advanced wireless devices that provide consistent, easy-to-

manage connectivity that expands your existing network. The access points maintain your network without interruption and reduce bottlenecks and network complexity by determining where data needs to go throughout the network. The MSM access points provide complete wireless coverage for greater reliability and connectivity and can be used in managed mode as well as autonomous mode without a controller.

2.2 TOE Architecture

The HP Wireless LAN products all share a common software code base, called Comware. Comware is special purpose appliance system software that implements a wide array of networking technology, including: IPv4/IPv6 dual-stacks, a data link layer, Ethernet switching, Intelligent Resilient Framework (IRF), routing, Quality of Service (QoS), etc. The evaluated version of Comware is 5.2.109. It should be noted that Comware runs on a variety of underlying architectures including VxWorks, Linux, pSOS and Windows; however, the only underlying architecture found in the evaluated configuration is Linux.

The Comware v5.2.109 architecture can be depicted as follows:

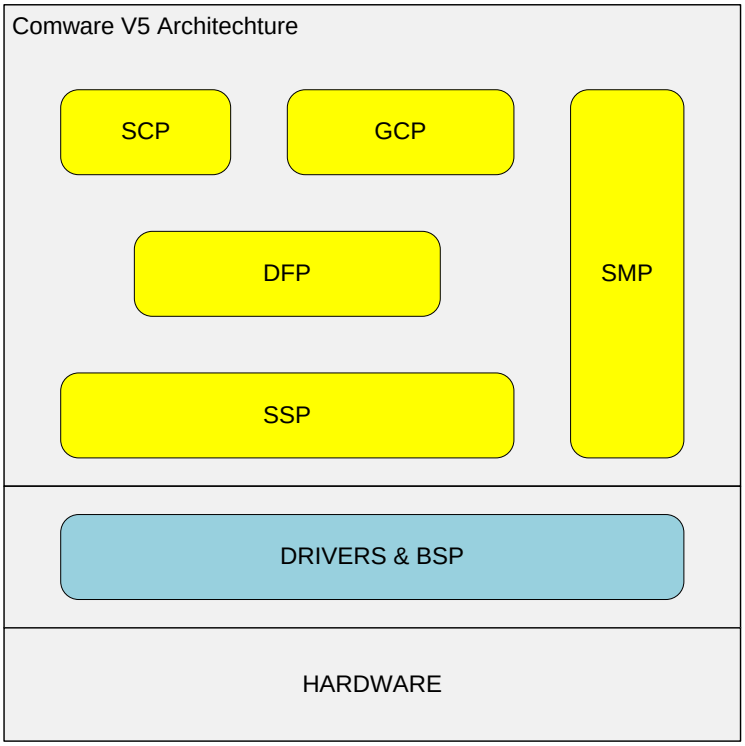

Figure 1 Comware v5.2.109 Architecture

- ***General Control Plane (GCP)*** **–** The GCP fully supports the IPv4 and IPv6 protocol stacks and provides support to a variety of IPv4/IPv6 applications including routing protocols, voice, WAN link features, and QoS features.
- ***Service Control Plane (SCP)*** **–** The SCP supports value-added services such as connection control, user policy management AAA, RADIUS, and TACACS/TACACS+.
- ***Data Forwarding Plane (DFP)*** **–** The DFP underpins all network data processing. The forwarding engine is the core of the DFP.
- ***System Management Plane (SMP)*** **–** The SMP provides user interfaces for device management. This includes implementations for Command line - CLI (SSHv2), and Web (HTTPS) management options.

- ***System Service Plane (SSP)* –** The SSP provides a foundation layer that implements primitives on which the other planes rely, for example, memory management, task management, timer management, message queue management, semaphore management, time management, IPC, RPC, module loading management and component management.

Underlying the main Comware components are the hardware-specific Board Support Package (BSP) and device drivers to provide necessary abstractions of the hardware components for the higher-level software components.

The Comware software components are composed of subsystems designed to implement applicable functions. For example there are subsystems dedicated to MIB, Web, and CLI management. There are also subsystems dedicated to the IPv4 and IPv6 network stacks as well as the applicable network protocols and forwarding, routing, etc.

While the Comware operating system is common to all devices in the evaluated configuration, the applications and hence security features of each device varies according to its role in the Wireless LAN system. In the case of a FAT access point, all of the security functions are implemented in the single device representing the TOE. However, in the case of FIT access points, most of the security functions are implemented in the access controller device while the access point is primarily responsible to send and receive applicable radio signals, to encrypt/decrypt those signals according to data (e.g., cryptographic keys) provided by the controller, and to otherwise broker the exchange of information between wireless clients and the controller (where, for example, wireless clients are authenticated). Logically, the entire set of security functions is implemented by the access controller –access point pair (i.e., the TOE), and this Security Target does not dwell on the specific details of where specifically each operation is performed or how a given operation might be divided between the applicable devices.

From a security perspective, the TOE includes cryptographic algorithms that have been NIST validated under the Cryptographic Algorithm Validation Program (CAVP). These cryptographic algorithms support SSHv2 and HTTPS (HTTP over TLSv1) and also digital signatures used to protect the available remote management and to enable secure update capabilities of the TOE. Otherwise, the TOE implements a wide range of network switching/routing protocols and functions.

The TOE provides 802.11n wireless protocol support which is backward compatible to 802.11a/b/g clients. The TOE provides 802.1X wireless client authentication and Wi-Fi Protected Access II (WPA2) security.

2.2.1 Physical Boundaries

The TOE consists of one or more of the following wireless controllers and one or more wireless access points:

- HP Wireless Controllers: HP 10500/7500 20G Unified Wired-WLAN Module, HP 830 8 port and 24 port PoE+ Unified Wired-WLAN Switches, HP 850 Unified Wired-WLAN Appliance, HP 870 Unified Wired-WLAN Appliance.
- HP Wireless Access Points: HP MSM430, 460 and 466 Dual Radio 802.11n Access Points, HP MSM466-R Dual Radio Outdoor 802.11n Access Point, HP 560 Wireless Dual Radio 802.11n Access Point.

All of the listed wireless controllers are rack-mountable appliances. All of the wireless access points are externally similar and have ports for wireless, Ethernet and for a local console. The access points differ primarily in their radio capabilities and the 466-R is also in an enclosure for outdoor use. They otherwise share common hardware characteristics such as processors, memory and network interfaces.

The TOE includes Comware v5.2.109 software which is used on all of HP's Wireless LAN products.

2.2.2 Logical Boundaries

This section summarizes the security functions provided by the TOE:

- Security audit
- Cryptographic support
- User data protection
- Identification and authentication
- Security management

- Protection of the TSF
- Resource utilization
- TOE access
- Trusted path/channels

All of the functionality supported by the TOE is included in the evaluated configuration. Note, however, that although the TOE supports both IPv4 and IPv6, support for IPv6 was not specifically covered by the evaluation. It should also be noted that although the TOE is comprised of two physical modules they must be treated as a single entity for the purpose of evaluation. The Access Points that are a part of the TOE only function in controlled mode which requires the use of an Access Controller.

2.2.2.1 Security audit

The TOE is able to generate logs of security relevant events. The TOE can be configured to be selective in the audit records logged and can store the logs locally so they can be accessed by an administrator. The TOE also has the option of storing audit records on an external server in the evaluated configuration.

Locally stored audit records can be reviewed by an administrator. The ability to view externally stored audit records is provided by the operational environment. All TOE audit records include a time stamp that comes from either the TOE's internal clock or from an optional NTP server.

2.2.2.2 Cryptographic support

The TOE includes cryptographic algorithms that have been NIST validated under the Cryptographic Algorithm Validation Program (CAVP). These cryptographic algorithms provide key management, random bit generation, encryption/decryption, digital signature and secure hashing and key-hashing features in support of higher level cryptographic protocols including SSH, and HTTPS.

Furthermore, the underlying cryptographic support is used to ensure that wireless communications can be secured (e.g., using WPA2).

The TOE must be configured and operated in FIPS mode.

2.2.2.3 User data protection

The TOE performs a wide variety of network switching and routing functions, passing network traffic among its various wireless, physical, and logical network connections. While implementing applicable network protocols associated with network traffic forwarding, the TOE is designed to ensure that it doesn't inadvertently reuse data found in network traffic.

The TOE implements WPA2 to encrypt and decrypt wireless network traffic as it is sent and received.

2.2.2.4 Identification and authentication

The TOE requires users (i.e., administrators) to be successfully identified and authenticated before they can access any security management functions available in the TOE. The TOE offers both a locally connected console as well as remote access to a CLI via SSHv2 and remote access to a GUI via HTTPS for interactive administrator sessions.

The TOE supports the local (i.e., on device) definition of administrators with usernames and passwords. Additionally, in the evaluated configuration the TOE can be configured to utilize the services of trusted RADIUS and TACACS/TACACS+ servers in the operational environment. These could be used to support, for example, centralized user administration.

The TOE implements 802.1X to support the authentication and authorization of wireless clients prior to establishing secure wireless sessions.

2.2.2.5 Security management

The TOE provides Command Line Interface (CLI) commands and a Web-based Graphical User Interface (Web GUI) to access the security management functions. The TOE's CLI can be accessed locally and remotely via SSH;

and the GUI is accessed through HTTPS. Security management commands are limited to administrators and are available only after they have provided acceptable user identification and authentication data to the TOE.

The TOE provides wireless clients access to manage their own credentials once connected, but otherwise security management functions are limited to administrators.

2.2.2.6 Protection of the TSF

The TOE implements a number of protection features designed to ensure the reliability and integrity of its security features.

It protects particularly sensitive data such as stored passwords and cryptographic keys so that they are not accessible even by an administrator. It also provides its own timing mechanism to ensure that reliable time information is available (e.g., for log accountability) and to ensure that information can be synchronized with a reliable time source.

From a communication perspective it employs both dedicated communication channels (based on physically separate networks) and also cryptographic means to protect communication between TOE components as well as between TOE and other components in the operational environment (e.g., administrator workstations).

The TOE includes functions to perform self-tests so that it might detect when it is failing. There is also self-test functionality that verifies the integrity of the TOE's stored executable files. This protects against corrupted executables that would cause unexpected or insecure behavior. There are also mechanisms so that the TOE itself can be updated while ensuring that the updates will not introduce malicious or other unexpected changes in the TOE.

2.2.2.7 Resource utilization

The TOE can limit network connections in order to ensure that administrators will be able to connect when they need to perform security management operations on the TOE.

2.2.2.8 TOE access

The TOE can be configured to display an informative banner when an administrator establishes an interactive session and subsequently will enforce an administrator-defined inactivity timeout value after which an inactive session will be terminated.

2.2.2.9 Trusted path/channels

The TOE protects interactive communication with administrators using SSHv2.0 for CLI access or HTTPS for Web GUI access. In each case, both integrity and disclosure protection is ensured. Similarly, remote wireless client communications are protected using WPA2 that involve the use of supporting cryptographic functions to ensure those wireless sessions are not subject to disclosure or modification.

The TOE protects communication with network peers, such as a log server or time server, using IPsec via IPv4 or IPv6 connections to prevent unintended disclosure or modification of logs or time updates.

2.3 TOE Documentation

There are numerous documents that provide information and guidance for the deployment of Hewlett-Packard Switches. The Hewlett-Packard Company WLAN Access Controllers and Access Points TOE includes the following guidance documentation:

- Command Reference for CC Supplement, Revision 1.4, 27 October 2014
- Configuration Guide for CC Supplement, Revision 1.3, 27 October 2014
- Comware V5 Web UI Configuration Guide, 1.11, 01 July 2014
- Comware V5 Platform System Log Messages, Revision 1.1, 29 Mar 2013
- Preparative Procedures for CC WLASPP Evaluated Wireless LAN Controllers and Access Points, Revision 1.06, 11 December 2014

- HP 830 8-Port PoE+ Unified Wired-WLAN Switch Installation Guide, Document version: 6W100-20130318
- HP 830 24-Port PoE+ Unified Wired-WLAN Switch Installation Guide, Document version: 6W100-20130318
- HP 850 Unified Wired-WLAN Appliance Installation Guide, Document version: 6W100-20140416
- HP 870 Unified Wired-WLAN Appliance Installation Guide, Document version: 6W100-20140416
- HP MSM3xx/MSM4xx APs Configuration Guide, October 2013
- HP 560 802.11ac Access Point Installation Guide, March 2014

The guidance above is supported by the following additional configuration guides and command references, all identified with the document version 6W102-20140818.

- HP Unified Wired-WLAN Products ACL and QoS Configuration Guide
- HP Unified Wired-WLAN Products ACL and QoS Command Reference
- HP Unified Wired-WLAN Products Network Management and Monitoring Configuration Guide
- HP Unified Wired-WLAN Products Network Management and Monitoring Command Reference
- HP Unified Wired-WLAN Products Security Configuration Guide
- HP Unified Wired-WLAN Products Security Command Reference
- HP Unified Wired-WLAN Products Fundamentals Configuration Guide
- HP Unified Wired-WLAN Products Fundamentals Command Reference
- HP Unified Wired-WLAN Products WLAN Configuration Guide
- HP Unified Wired-WLAN Products WLAN Command Reference
- HP Unified Wired-WLAN Products Layer 2 Configuration Guide
- HP Unified Wired-WLAN Products Layer 2 Command Reference
- HP Unified Wired-WLAN Products Layer 3 Configuration Guide
- HP Unified Wired-WLAN Products Layer 3 Command Reference
- HP Unified Wired-WLAN Products IP Multicast Configuration Guide
- HP Unified Wired-WLAN Products IP Multicast Command Reference
- HP Unified Wired-WLAN Products High Availability Configuration Guide
- HP Unified Wired-WLAN Products High Availability Command Reference
- HP Unified Wired-WLAN Products OAA Configuration Guide
- HP Unified Wired-WLAN Products OAA Command Reference
- HP Unified Wired-WLAN Products Basic Configuration Guide
- HP Unified Wired-WLAN Products Web-Based Configuration Guide

These documents are available via the ‘Manuals for HP Wireless Access Controller Modules – HP Support Center’ web page at:

http://h20566.www2.hp.com/portal/site/hpsc/template.PAGE/public/psi/manualsResults/?sp4ts.oid=4181241&spf_p.tpst=psiContentResults&spf_p.prp_psiContentResults=wsrp-navigationalState%3DmanLang%253Den&javax.portlet.begCacheTok=com.vignette.cachetoken&javax.portlet.endCacheTok=com.vignette.cachetoken

3. Security Problem Definition

The Security Problem Definition (composed of organizational policies, threat statements, and assumption) has been drawn from the *Protection Profile for Wireless Local Area Network (WLAN) Access Systems*, version 1.0, 01 December 2011 (WLASPP). The WLASPP offers additional information about the identified threats, but that has not been reproduced here and the WLASPP should be consulted if there is interest in that material.

In general, the WLASPP has presented a Security Problem Definition appropriate for network infrastructure devices and as such is applicable to the Mobility Controller and Access Point Series TOE.

3.1 Organizational Policies

P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.
P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE.
P.ADMIN_ACCESS	Administrators shall be able to administer the TOE both locally and remotely through protected communications channels.
P.COMPATIBILITY	The TOE must meet Request for Comments (RFC) requirements for implemented protocols to facilitate inter-operation with other network equipment (e.g., certificate authority, NTP server) using the same protocols.
P.EXTERNAL_SERVERS	The TOE must support standardized (RFCs) protocols for communication with a centralized audit server and a RADIUS authentication server.

3.2 Threats

T.ADMIN_ERROR	An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
T.RESOURCE_EXHAUSTION	A process or user may deny access to TOE services by exhausting critical resources on the TOE.
T.TSF_FAILURE	Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
T.UNAUTHORIZED_ACCESS	A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
T.UNAUTHORIZED_UPDATE	A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
T.UNDETECTED_ACTIONS	Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.
T.USER_DATA_REUSE	User data may be inadvertently sent to a destination not intended by the original sender.

3.3 Assumptions

A.NO_GENERAL_PURPOSE	It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available to the TOE, other than those services necessary for the operation, administration and support of the TOE.

A.NO_TOE_BYPASS	Information cannot flow between the wireless client and the internal wired network without passing through the TOE.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

4. Security Objectives

Like the Security Problem Definition, the Security Objectives have been drawn from the *Protection Profile for Wireless Local Area Network (WLAN) Access Systems*, version 1.0, 01 December 2011 (WLASPP). The WLASPP offers additional information about the identified security objectives, but that has not been reproduced here and the WLASPP should be consulted if there is interest in that material.

In general, the WLASPP has presented a Security Objectives appropriate for network infrastructure devices and as such are applicable to the Mobility Controller and Access Point Series TOE.

4.1 Security Objectives for the TOE

O.AUTH_COMM	The TOE will provide a means to ensure users are not communicating with some other entity pretending to be the TOE, and that the TOE is communicating with an authorized IT entity and not some other entity pretending to be an authorized IT entity.
O.CRYPTOGRAPHIC_FUNCTIONS	The TOE shall provide cryptographic functions (i.e., encryption/decryption and digital signature operations) to maintain the confidentiality and allow for detection of modification of TSF data that is transmitted between physically separated portions of the TOE, or stored outside the TOE.
O.DISPLAY_BANNER	The TOE will display an advisory warning regarding use of the TOE.
O.FAIL_SECURE	The TOE shall fail in a secure manner following failure of the power-on self-tests.
O.PROTECTED_COMMUNICATIONS	The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
O.PROTOCOLS	The TOE will ensure that standardized protocols are implemented in the TOE to RFC and/or Industry specifications to ensure interoperability, that also support communication with a centralized audit server and a RADIUS authentication server.
O.RESIDUAL_INFORMATION_CLEARING	The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated.
O.RESOURCE_AVAILABILITY	The TOE shall provide mechanisms that mitigate user attempts to exhaust TOE resources (e.g., persistent storage).
O.ROBUST_TOE_ACCESS	The TOE will provide mechanisms that control an administrator's logical access to the TOE and to control administrative access from a wireless client.
O.SESSION_LOCK	The TOE shall provide mechanisms that mitigate the risk of unattended sessions being hijacked.
O.SYSTEM_MONITORING	The TOE will provide the capability to generate audit data and send those data to an external IT entity.
O.TIME_STAMPS	The TOE shall provide reliable time stamps and the capability for the administrator to set the time used for these timestamps.

O.TOE_ADMINISTRATION	The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE, and provide protections for logged-in administrators.
O.TSF_SELF_TEST	The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly.
O.VERIFIABLE_UPDATES	The TOE will provide the capability to help ensure that any updates to the TOE can be verified by the administrator to be unaltered and (optionally) from a trusted source.
O.WIRELESS_CLIENT_ACCESS	The TOE will provide the capability to restrict a wireless client in connecting to the TOE.

4.2 Security Objectives for the Environment

OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available to the TOE, other than those services necessary for the operation, administration and support of the TOE.
OE.NO_TOE_BYPASS	Information cannot flow between external and internal networks located in different enclaves without passing through the TOE.
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the IT environment.
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

5. IT Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) that serve to represent the security functional claims for the Target of Evaluation (TOE) and to scope the evaluation effort.

The SFRs have all been drawn from the Protection Profile (PP): *Protection Profile for Wireless Local Area Network (WLAN) Access Systems*, version 1.0, 01 December 2011 (WLASPP). The refinements and operations already performed in that PP are not identified (e.g., highlighted) here, rather the requirements have been copied from that PP and any residual operations have been completed herein. Of particular note, the WLASPP made a number of refinements and completed some of the SFR operations defined in the Common Criteria (CC) and that PP should be consulted to identify those changes if necessary.

The SARs are the set of SARs specified in WLASPP.

5.1 Extended Requirement Definitions

All of the extended requirements in this ST have been drawn from the WLASPP. The WLASPP defines the following extended SFRs and since they are not redefined in this ST, the WLASPP should be consulted for more information in regard to those CC extensions.

- FAU_STG_EXT.1: External Audit Trail Storage
- FAU_STG_EXT.3: Action in Case of Loss of Audit Server Connectivity
- FAU_STG_EXT.4: Prevention of Audit Data Loss
- FCS_CKM_EXT.4: Cryptographic Key Zeroization
- FCS_HTTPS_EXT.1: Explicit: HTTPS
- FCS_IPSEC_EXT Extended: Internet Protocol Security (IPsec) Communications
- FCS_RBG_EXT.1 Extended: Cryptographic operation (Random Bit Generation)
- FCS_SSH_EXT.1: Explicit: SSH
- FCS_TLS_EXT.1: Explicit: TLS
- FIA_PMG_EXT.1: Password Management
- FIA_UIA_EXT.1 User Identification and Authentication
- FIA_UAU_EXT.5 Extended: Password-based Authentication Mechanisms
- FIA_8021X_EXT.1 Extended: 802.1X Port Access Entity (Authenticator) Authentication
- FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition
- FIA_X509_EXT.1 Extended: X509 Certificates
- FPT_TST_EXT.1: TSF Testing
- FPT_TUD_EXT.1: Extended: Trusted Update
- FTA_SSL_EXT.1: TSF-initiated session locking

5.2 TOE Security Functional Requirements

The following table identifies the SFRs that are satisfied by Mobility Controller and Access Point Series TOE.

Requirement Class	Requirement Component
FAU: Security Audit	FAU_GEN.1: Audit Data Generation

Requirement Class	Requirement Component
	FAU_GEN.2: User Audit Association
	FAU_SAR.1: Audit Review
	FAU_SAR.2: Restricted Audit Review
	FAU_SEL.1: Selective Audit
	FAU_STG.1: Protected Audit Trail Storage (Local Storage)
	FAU_STG_EXT.1: External Audit Trail Storage
	FAU_STG_EXT.3: Action in Case of Loss of Audit Server Connectivity
	FAU_STG_EXT.4: Prevention of Audit Data Loss
FCS: Cryptographic Support	FCS_CKM.1(1): Cryptographic Key Generation (Symmetric Keys for WPA2 Connections)
	FCS_CKM.1(2): Cryptographic Key Generation (Asymmetric Keys)
	FCS_CKM.2(1): Cryptographic Key Distribution (PMK)
	FCS_CKM.2(2): Cryptographic Key Distribution (GTK)
	FCS_CKM_EXT.4: Cryptographic Key Zeroization
	FCS_COP.1(1): Cryptographic Operation (Data Encryption/Decryption)
	FCS_COP.1(2): Cryptographic Operation (Cryptographic Signature)
	FCS_COP.1(3): Cryptographic Operation (Cryptographic Hashing)
	FCS_COP.1(4): Cryptographic Operation (Keyed-Hash Message Authentication)
	FCS_COP.1(5): Cryptographic Operation (WPA2 Data Encryption/Decryption)
	FCS_HTTPS_EXT.1: Extended: HTTP Security (HTTPS)
	FCS_IPSEC_EXT.1: Extended: Internet Protocol Security (IPsec) Communications
	FCS_RBG_EXT.1: Extended: Cryptographic Operation: Random Bit Generation
	FCS_SSH_EXT.1: Extended: Secure Shell (SSH)
	FCS_TLS_EXT.1: Extended: Transport Layer Security (TLS)
FDP: User Data Protection	FDP_RIP.2: Full Resident Information Protection
FIA: Identification and Authentication	FIA_8021X_EXT.1: Extended: 802.1X Port Access Entity (Authenticator) Authentication
	FIA_AFL.1: Authentication Failure Handling
	FIA_PMG_EXT.1: Password Management
	FIA_PSK_EXT.1: Extended: Pre-Shared Key Composition
	FIA_UAU.6: Re-authenticating
	FIA_UAU.7: Protected Authentication Feedback
	FIA_UAU_EXT.5: Extended: Password-based Authentication Mechanisms
	FIA_UIA_EXT.1: User Identification and Authentication
	FIA_X509_EXT.1: Extended: X509 Certificates
FMT: Security Management	FMT_MOF.1: Management of Security Functions Behavior
	FMT_MTD.1(1): Management of TSF Data (General TSF Data)
	FMT_MTD.1(2): Management of TSF Data (Reading of Authentication Data)
	FMT_MTD.1(3): Management of TSF Data (for reading of all symmetric keys)
	FMT_SMF.1: Specification of management functions
	FMT_SMR.1: Security Management Roles
FPT: Protection of the TSF	FPT_FLS.1: Fail Secure
	FPT_ITT.1: Basic Internal TSF Data Transfer Protection
	FPT_STM.1: Reliable Time Stamp
	FPT_TST_EXT.1: Extended: TSF Testing
	FPT_TUD_EXT.1: Extended: Trusted Update Resource Utilization (FRU)

Requirement Class	Requirement Component
FRU: Resource Utilization	FRU_RSA.1: Maximum Quotas TOE Access (FTA)
FTA: TOE Access	FTA_SSL.3: TSF-initiated termination
	FTA_SSL.4: User-initiated termination
	FTA_SSL_EXT.1: TSF-initiated session locking
	FTA_TAB.1: Default TOE Access Banners
	FTA_TSE.1: TOE Session Establishment Trusted Path/Channels (FTP)
FTP: Trusted path/channels	FTP_ITC.1: Inter-TSF trusted channel
	FTP_TRP.1: Trusted Path

Table 1 TOE Security Functional Components

5.2.1 Security audit (FAU)

5.2.1.1 Audit Data Generation (FAU_GEN.1)

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events: a) Start-up and shutdown of the audit functions; b) All auditable events for the not specified level of audit; and c) *All* administrative actions; d) [Specifically defined auditable events listed in **Table 2 Audit Events**].

Requirement	Auditable Events	Additional Audit Record Content
FAU_GEN.1	None	
FAU_GEN.2	None	
FAU_SAR.1	None	
FAU_SAR.2	None	
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating.	None
FAU_STG.1	None	
FAU_STG_EXT.1	None	
FAU_STG_EXT.3	Loss of connectivity.	None
FAU_STG_EXT.4	None	
FCS_CKM.1(1)	Failure of the key generation activity.	None
FCS_CKM.1(2)	Failure of the key generation activity.	None
FCS_CKM.2(1)	Failure of the key distribution activity.	None
FCS_CKM.2(2)	Failure of the key distribution activity, including failures related to wrapping the GTK.	Identifier(s) for intended recipients of wrapped key.
FCS_CKM_EXT.4	Failure of the key zeroization process.	Identity of subject requesting or causing zeroization, identity of object or entity being cleared.
FCS_COP.1(1)	Failure of encryption or decryption.	Cryptographic mode of operation, name/identifier of object being encrypted/decrypted.
FCS_COP.1(2)	Failure of cryptographic signature.	Cryptographic mode of operation, name/identifier of object being signed/verified.
FCS_COP.1(3)	Failure of hashing function.	Cryptographic mode of operation, name/identifier of object being hashed.
FCS_COP.1(4)	Failure in Cryptographic Hashing for Non-Data Integrity.	Cryptographic mode of operation, name/identifier of object being hashed.
FCS_COP.1(5)	Failure of WPA2 encryption or decryption.	Cryptographic mode of operation, name/identifier of object being encrypted/decrypted, non-TOE endpoint of connection (IP address).

Requirement	Auditable Events	Additional Audit Record Content
FCS_HTTPS_EXT.1	Protocol failures. Establishment/Termination of a HTTPS session.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.
FCS_IPSEC_EXT.1	Protocol failures. Establishment/Termination of an IPsec SA. Negotiation "down" from an IKEv2 to IKEv1 exchange.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.
FCS_RBG_EXT.1	Failure of the randomization process.	None
FCS_SSH_EXT.1	Protocol failures. Establishment/Termination of an SSH session.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.
FCS_TLS_EXT.1	Protocol failures. Establishment/Termination of a TLS session.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.
FDP_RIP.2	None	
FIA_8021X_EXT.1	Attempts to access to the 802.1X controlled port.	Provided client identity (IP address).
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions taken (e.g., disabling of an account) and the subsequent, if appropriate, restoration to the normal state (e.g., re-enabling of a terminal).	None
FIA_PMG_EXT.1	None	
FIA_PSK_EXT.1	None	
FIA_UAU.6	Attempts to re-authenticate.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None	
FIA_UAU_EXT.5	All use of the authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Provided user identity, origin of the attempt (e.g., IP address).
FIA_X509_EXT.1	Attempts to load certificates. Attempts to revoke certificates.	None
FMT_MOF.1	None	
FMT_MTD.1(1)	None	
FMT_MTD.1(2)	None	
FMT_MTD.1(3)	None	
FMT_SMF.1	None	
FMT_SMR.1	None	
FPT_FLS.1	Failure of the TSF.	Indication that the TSF has failed with the type of failure that occurred.
FPT_ITT.1	None	
FPT_STM.1	None	
FPT_TST_EXT.1	Execution of this set of TSF self-tests. Detected integrity violations.	For integrity violations, the TSF code file that caused the integrity violation.
FPT_TUD_EXT.1	Initiation of the update. Any failure to verify the integrity of the update.	None
FRU_RSA.1	Maximum quota being exceeded.	Resource identifier.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None

Requirement	Auditable Events	Additional Audit Record Content
FTA_SSL.4	Terminating a session by quitting or logging off.	None
FTA_SSL_EXT.1	Locking of an interactive session by the session locking mechanism. Any attempts at unlocking of an interactive session.	None
FTA_TAB.1	None	
FTA_TSE.1	Denial of a session establishment due to the session establishment mechanism.	Reason for denial, origin of establishment attempt.
FTP_ITC.1	All attempts to establish a trusted channel. Detection of modification of channel data.	Identification of the initiator and target of channel.
FTP_TRP.1	All attempts to establish a remote administrative session. Detection of modification of session data.	Identification of the initiating IT entity (e.g., IP address).

Table 2 Audit Events

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [information specified in column three of **Table 2 Audit Events**].

5.2.1.2 User Audit Association (FAU_GEN.2)

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

5.2.1.3 Audit Review (FAU_SAR.1)

FAU_SAR.1.1 The TSF shall provide Authorized Administrators with the capability to read all audit data from the audit records.

FAU_SAR.1.2 Refinement: The TSF shall provide the audit records in a manner suitable for the ~~user~~ Authorized Administrators to interpret the information.

5.2.1.4 Restricted Audit Review (FAU_SAR.2)

FAU_SAR.2.1 Refinement: The TSF shall prohibit all users read access to the audit records in the audit trail, except Authorized Administrators.

5.2.1.5 Selective Audit (FAU_SEL.1)

FAU_SEL.1.1 The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes: a) event type; b) success of auditable security events; c) failure of auditable security events; and d) [**when applicable, device interface and wireless client identity**].

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

FAU_STG.1.1 Refinement: The TSF shall protect [**an administrator configurable maximum size from 1MB to 10MB**] locally stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to prevent unauthorized modifications to the stored audit records in the audit trail.

5.2.1.7 External Audit Trail Storage (FAU_STG_EXT.1)

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to an external IT entity using a trusted channel implementing the [***IPsec***] protocol.

5.2.1.8 Action in Case of Loss of Audit Server Connectivity (FAU_STG_EXT.3)

FAU_STG_EXT.3.1 The TSF shall [**generate an SNMP trap**] if the link to the external IT entity collecting the audit data generated by the TOE is not available.

5.2.1.9 Prevention of Audit Data Loss (FAU_STG_EXT.4)

FAU_STG_EXT.4.1 The TSF shall provide the Authorized Administrator the capability to select one or more of the following actions:

a) Prevent auditable events, except those taken by the Authorized Administrator, and;

b) Overwrite the oldest stored audit records;

to be taken if the audit trail is full.

5.2.2 Cryptographic support (FCS)

5.2.2.1 Cryptographic Key Generation (Symmetric Keys for WPA2 Connections) (FCS_CKM.1(1))

FCS_CKM.1.1(1) Refinement: The TSF shall derive symmetric cryptographic keys in accordance with a specified cryptographic key derivation algorithm [PRF-384] with specified cryptographic key size [128 bits] using a Random Bit Generator as specified in FCS_RBG_EXT.1 and that meet the following: [802.11-2007].

5.2.2.2 Cryptographic Key Generation (Asymmetric Keys) (FCS_CKM.1(2))

FCS_CKM.1.1(2) Refinement: The TSF shall generate asymmetric cryptographic keys used for key establishment in accordance with [

- ***NIST Special Publication 800-56B, 'Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography' for RSA-based key establishment schemes***]

and specified cryptographic key sizes equivalent to, or greater than, a symmetric key strength of 112 bits.

5.2.2.3 Cryptographic Key Distribution (PMK) (FCS_CKM.2(1))

FCS_CKM.2.1(1) Refinement: The TSF shall distribute the 802.11 Pairwise Master Key in accordance with a specified cryptographic key distribution method: [receive from 802.1X Authorization Server] that meets the following: [802.11-2007] and does not expose the cryptographic keys.

5.2.2.4 Cryptographic Key Distribution (GTK) (FCS_CKM.2(2))

FCS_CKM.2.1(2) Refinement: The TSF shall distribute Group Temporal Key in accordance with a specified cryptographic key distribution method: [AES Key Wrap in an EAPOL-Key frame] that meets the following: [RFC 3394 for AES Key Wrap, 802.11-2007 for the packet format and timing considerations] and does not expose the cryptographic keys.

5.2.2.5 Cryptographic Key Zeroization (FCS_CKM_EXT.4)

FCS_CKM_EXT.4.1 The TSF shall zeroize all plaintext secret and private cryptographic keys and cryptographic security parameters when no longer required.

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

FCS_COP.1.1(1) Refinement: The TSF shall perform [encryption and decryption] in accordance with a specified cryptographic algorithm [AES operating in [**CBC, CCM, and CTR mode**]] and cryptographic key sizes 128-bits, 256-bits, and [***192 bits***] that meet the following: FIPS PUB 197, 'Advanced Encryption Standard (AES)' **and** [***NIST SP 800-38A, NIST SP 800-38C***].

5.2.2.7 Cryptographic Operation (Cryptographic Signature) (FCS_COP.1(2))

FCS_COP.1.1(2) Refinement: The TSF shall perform cryptographic signature services in accordance with a [

(2) RSA Digital Signature Algorithm (rDSA) with a key size (modulus) of 2048 bits or greater, or

]

that meets the following:

Case: RSA Digital Signature Algorithm

[***FIPS PUB 186-3, 'Digital Signature Standard'***].

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

FCS_COP.1.1(3) Refinement: The TSF shall perform [cryptographic hashing services] in accordance with a specified cryptographic algorithm [***SHA-1, SHA-256***] and message digest sizes [***160, 256***] bits that meet the following: FIPS Pub 180-3, 'Secure Hash Standard.'

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

FCS_COP.1.1(4) Refinement: The TSF shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm HMAC- [***SHA-1, SHA-256***], key size [**160bits, 256bits**], and message digest size of [***160, 256***] bits that meet the following: FIPS PUB 198-1, 'The Keyed-Hash Message Authentication Code', and FIPS PUB 180-3, 'Secure Hash Standard'.

5.2.2.10 Cryptographic Operation (WPA2 Data Encryption/Decryption) (FCS_COP.1(5))

FCS_COP.1.1(5) Refinement: The TSF shall perform encryption and decryption in accordance with the specified cryptographic algorithm AES CCMP and cryptographic key size of 128 bits that meet the following: FIPS PUB 197, NIST SP 800-38C and IEEE 802.11-2007.

5.2.2.11 Extended: HTTP Security (HTTPS) (FCS_HTTPS_EXT.1)

FCS_HTTPS_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2 The TSF shall implement HTTPS using TLS as specified in FCS_TLS_EXT.1.

5.2.2.12 Extended: Internet Protocol Security (IPsec) Communications (FCS_IPSEC_EXT.1)

FCS_IPSEC_EXT.1.1 The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using the cryptographic algorithms AES-CBC-128, AES-CBC-256 (both specified by RFC 3602), [***no other algorithms***], and using [***IKEv1 as defined in RFCs 2407, 2408, 2409, RFC 4109, and [RFC 4868 for hash functions]***] for connections to the Authentication Server and [***[audit and NTP servers]***].

FCS_IPSEC_EXT.1.2 The TSF shall ensure that only ESP confidentiality and integrity security service is used.

FCS_IPSEC_EXT.1.3 The TSF shall ensure that IKEv1 Phase 1 exchanges use only main mode.

FCS_IPSEC_EXT.1.4 The TSF shall ensure that [***IKEv1 SA lifetimes are able to be limited by number of packets and time: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs***].

FCS_IPSEC_EXT.1.5 The TSF shall generate the secret value x used in the IKE Diffie-Hellman key exchange ('x' in gx mod p) using the random bit generator specified in FCS_RBG_EXT.1, and having a length of at least [**512**] bits.

FCS_IPSEC_EXT.1.6 The TSF shall generate nonces used in IKE exchanges in a manner such that the probability that a specific nonce value will be repeated during the life a specific IPsec SA is less than 1 in 2^[**256**].

FCS_IPSEC_EXT.1.7 The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP) and***, [no other DH groups]***.

FCS_IPSEC_EXT.1.8 The TSF shall ensure that all IKE protocols implement peer authentication using Pre-shared Keys and [**rDSA**] that use X.509v3 certificates that conform to RFC 4945.

FCS_IPSEC_EXT.1.9 The TSF shall be able to ensure by default that the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [***IKEv1 Phase 1***] connection is greater than or equal to the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [***IKEv1 Phase 2***] connection.

5.2.2.13 Extended: Cryptographic Operation: Random Bit Generation (FCS_RBG_EXT.1)

FCS_RBG_EXT.1.1 The TSF shall perform all random bit generation (RBG) services in accordance with [***NIST Special Publication 800-90*** using [***CTR_DRBG (AES)***] seeded by an entropy source that accumulates entropy from at least one independent TSF-hardware-based noise sources.

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded with a minimum of [128 ***bits***] of entropy at least equal to the greatest bit length of the keys and authorization factors that it will generate.

5.2.2.14 Extended: Secure Shell (SSH) (FCS_SSH_EXT.1)

FCS_SSH_EXT.1.1 The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, 4254, and 5656.

FCS_SSH_EXT.1.2 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, password-based.

FCS_SSH_EXT.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than [**32,768**] bytes in an SSH transport connection are dropped.

FCS_SSH_EXT.1.4 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms: AES-CBC-128, AES-CBC-256, [***no other encryption algorithms***].

FCS_SSH_EXT.1.5 The TSF shall ensure that the SSH transport implementation uses [***SSH_RSA***] and [***no other public key algorithms***] as its public key algorithm(s).

FCS_SSH_EXT.1.6 The TSF shall ensure that the data integrity algorithm used in the SSH transport connection is [***hmac-sha1, hmac-sha1-96***].

FCS_SSH_EXT.1.7 The TSF shall ensure that diffie-hellman-group14-sha1 and [***no other methods***] are the only allowed key exchange methods used for the SSH protocol.

5.2.2.15 Extended: Transport Layer Security (TLS) (FCS_TLS_EXT.1)

FCS_TLS_EXT.1.1 The TSF shall implement one or more of the following protocols [***TLS 1.0 (RFC 2246)***] supporting the following ciphersuites:

Mandatory Ciphersuites:

TLS_RSA_WITH_AES_128_CBC_SHA

Optional Ciphersuites:

[***TLS_RSA_WITH_AES_256_CBC_SHA***].

5.2.3 User data protection (FDP)

5.2.3.1 Full Resident Information Protection (FDP_RIP.2)

FDP_RIP.2.1 The TSF shall enforce that any previous information content of a resource is made unavailable upon the [***allocation of the resource to***] all objects.

5.2.4 Identification and authentication (FIA)

5.2.4.1 Extended: 802.1X Port Access Entity (Authenticator) Authentication (FIA_8021X_EXT.1)

FIA_8021X_EXT.1.1 The TSF shall conform to IEEE Standard 802.1X for a Port Access Entity (PAE) in the 'Authenticator' role.

FIA_8021X_EXT.1.2 The TSF shall support communications to a RADIUS authentication server conforming to RFCs 2865 and 3579.

FIA_8021X_EXT.1.3 The TSF shall ensure that no access to its 802.1X controlled port is given to the wireless client prior to successful completion of this authentication exchange.

5.2.4.2 Authentication Failure Handling (FIA_AFL.1)

FIA_AFL.1.1 Refinement: The TSF shall detect when an Authorized Administrator configurable positive integer of successive unsuccessful authentication attempts occur related to administrators attempting to authenticate remotely.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met, the TSF shall [***[prevent the offending remote administrator from successfully authenticating until an Authorized Administrator defined time period has elapsed]***].

5.2.4.3 Password Management (FIA_PMG_EXT.1)

FIA_PMG_EXT.1.1 The TSF shall provide the following password management capabilities for administrative passwords:

1. Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and special characters (that include: '!', '@', '#', '$', '%', '^', '&', '*', '(', and ')');

2. Minimum password length shall be settable by the Authorized Administrator, and support passwords of 8 characters or greater;

3. Passwords composition rules specifying the types and number of required characters that comprise the password shall be settable by the Administrator.

4. Passwords shall have a maximum lifetime, configurable by the Authorized Administrator.

5. New passwords must contain a minimum of 4 character changes from the previous password.

5.2.4.4 Extended: Pre-Shared Key Composition (FIA_PSK_EXT.1)

FIA_PSK_EXT.1.1 The TSF shall be able to use pre-shared keys for IPsec and [***WPA2***].

FIA_PSK_EXT.1.2 The TSF shall be able to accept text-based pre-shared keys that: are 22 characters and [***[a maximum of 128 characters for IPsec and a maximum of 64 characters for WPA2]***] composed of any combination of upper and lower case letters, numbers, and special characters (that include: '!', '@', '#', '$', '%', '^', '&', '*', '(', and ')').

FIA_PSK_EXT.1.3 The TSF shall condition the text-based pre-shared keys by using [***SHA-1***].

FIA_PSK_EXT.1.4 The TSF shall be able to [***accept***] bit-based pre-shared keys.

5.2.4.5 Re-authenticating (FIA_UAU.6)

FIA_UAU.6.1 The TSF shall re-authenticate the administrative user under the conditions: when the user changes their password, [***unlocks a locked session***].

Application Note: Only administrators with "root" privilege level can change passwords. Users without "root" privilege cannot change any password, even their own.

5.2.4.6 Protected Authentication Feedback (FIA_UAU.7)

FIA_UAU.7.1 The TSF shall provide only obscured feedback to the administrative user while the authentication is in progress at the local console.

5.2.4.7 Extended: Password-based Authentication Mechanisms (FIA_UAU_EXT.5)

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

FIA_UAU_EXT.5.2 The TSF shall ensure that administrative users with expired passwords are [***locked out until their password is reset by an administrator***].

5.2.4.8 User Identification and Authentication (FIA_UIA_EXT.1)

FIA_UIA_EXT.1.1 The TSF shall allow responses to the following actions prior to requiring the non-TOE entity to initiate the identification and authentication process: Display the warning banner in accordance with FTA_TAB.1; [**no other services.**]

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

5.2.4.9 Extended: X509 Certificates (FIA_X509_EXT.1)

FIA_X509_EXT.1.1 The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for IPsec and [***TLS, SSH***] connections.

FIA_X509_EXT.1.2 The TSF shall store and protect certificate(s) from unauthorized deletion and modification.

FIA_X509_EXT.1.3 The TSF shall provide the capability for Authorized Administrators to load X.509v3 certificates into the TOE for use by the security functions specified in this PP.

5.2.5 Security management (FMT)

5.2.5.1 Management of Security Functions Behavior (FMT_MOF.1)

FMT_MOF.1.1 Refinement: The TSF shall restrict the ability to enable, disable, determine and modify the behavior of all of the security functions of the TOE identified in this PP to the Authorized Administrator.

5.2.5.2 Management of TSF Data (General TSF Data) (FMT_MTD.1(1))

FMT_MTD.1.1(1) The TSF shall restrict the ability to manage the TSF data to the Authorized Administrators.

5.2.5.3 Management of TSF Data (Reading of Authentication Data) (FMT_MTD.1(2))

FMT_MTD.1.1(2) Refinement: The TSF shall prevent reading of the password-based authentication data.

5.2.5.4 Management of TSF Data (for reading of all symmetric keys) (FMT_MTD.1(3))

FMT_MTD.1.1(3) Refinement: The TSF shall prevent reading of all pre-shared keys, symmetric key, and private keys.

5.2.5.5 Specification of management functions (FMT_SMF.1)

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions:

- Ability to configure the list of TOE services available before an entity is identified and authenticated, as specified in FIA_UIA.1, respectively.
- Ability to configure the cryptographic functionality.
- Ability to update the TOE, and to verify the updates using the digital signature capability (FCS_COP.1(2)) and ***[no other functions].***
- Ability to configure the TOE advisory notice and consent warning message regarding unauthorized use of the TOE.
- Ability to configure all security management functions identified in other sections of this PP.

5.2.5.6 Security Management Roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles: Authorized Administrator; [No other roles].

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

FMT_SMR.1.3 The TSF shall ensure that the conditions Authorized Administrator role shall be able to administer the TOE locally; Authorized Administrator role shall be able to administer the TOE remotely; he ability to remotely administer the TOE remotely from a wireless client shall be disabled by default; are satisfied.

5.2.6 Protection of the TSF (FPT)

5.2.6.1 Fail Secure (FPT_FLS.1)

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: failure of the power-on self-tests.

5.2.6.2 Basic Internal TSF Data Transfer Protection (FPT_ITT.1)

FPT_ITT.1.1 Refinement: The TSF shall protect TSF data from disclosure and protect it from modification when it is transmitted between separate parts of the TOE through the use [***IPsec***].

5.2.6.3 Reliable Time Stamp (FPT_STM.1)

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

5.2.6.4 Extended: TSF Testing (FPT_TST_EXT.1)

FPT_TST_EXT.1.1 The TSF shall run a suite of self-tests during the initial start-up (on power on) to demonstrate the correct operation of the TSF.

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

5.2.6.5 Extended: Trusted Update Resource Utilization (FRU) (FPT_TUD_EXT.1)

FPT_TUD_EXT.1.1 The TSF shall provide authorized administrators the ability to query the current version of the TOE firmware/software.

FPT_TUD_EXT.1.2 The TSF shall provide authorized administrators the ability to initiate updates to TOE firmware/software.

FPT_TUD_EXT.1.3 The TSF shall provide a means to verify firmware/software updates to the TOE using a digital signature mechanism and [***no other functions***] prior to installing those updates.

5.2.7 Resource utilization (FRU)

5.2.7.1 Maximum Quotas TOE Access (FTA) (FRU_RSA.1)

FRU_RSA.1.1 The TSF shall enforce maximum quotas of the following resources: [**administrative sessions**], [***no other resources***] that [***defined group of users***] can use [***simultaneously***].

5.2.8 TOE access (FTA)

5.2.8.1 TSF-initiated termination (FTA_SSL.3)

FTA_SSL.3.1 The TSF shall terminate a remote interactive session after an Authorized Administrator-configurable time interval of session inactivity.

5.2.8.2 User-initiated termination (FTA_SSL.4)

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

5.2.8.3 TSF-initiated session locking (FTA_SSL_EXT.1)

FTA_SSL_EXT.1.1 Refinement: The TSF shall, for local interactive sessions, [***terminate the session***] after an Authorized Administrator specified time period of inactivity.

5.2.8.4 Default TOE Access Banners (FTA_TAB.1)

FTA_TAB.1.1 Refinement: Before establishing an administrative user session the TSF shall be capable of displaying an Authorized Administrator-specified advisory notice and consent warning message regarding unauthorized use of the TOE.

5.2.8.5 TOE Session Establishment Trusted Path/Channels (FTP) (FTA_TSE.1)

FTA_TSE.1.1 Refinement: The TSF shall be able to deny establishment of a wireless client session based on location, time, day, [**no other attributes**].

5.2.9 Trusted path/channels (FTP)

5.2.9.1 Inter-TSF trusted channel (FTP_ITC.1)

FTP_ITC.1.1 Refinement: The TSF shall use 802.11-2007, IPsec, and [***no other protocols***] to provide a trusted communication channel between itself and all authorized IT entities that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

FTP_ITC.1.2 The TSF shall permit the TSF, or the authorized IT entities to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [**remote logging, NTP, and authentication functions**].

5.2.9.2 Trusted Path (FTP_TRP.1)

FTP_TRP.1.1 Refinement: The TSF shall use [***SSH, TLS/HTTPS***] provide a trusted communication path between itself and remote administrators that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from disclosure and detection of modification of the communicated data.

FTP_TRP.1.2 Refinement: The TSF shall permit remote administrators to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for initial administrator authentication and all remote administration actions.

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are included by reference from the WLASPP.

Requirement Class	Requirement Component
ADV: Development	ADV_FSP.1: Basic functional specification
AGD: Guidance documents	AGD_OPE.1: Operational user guidance
	AGD_PRE.1: Preparative procedures
ALC: Life-cycle support	ALC_CMC.1: Labeling of the TOE
	ALC_CMS.1: TOE CM coverage
ATE: Tests	ATE_IND.1: Independent testing - conformance
AVA: Vulnerability assessment	AVA_VAN.1: Vulnerability survey

Table 3 Assurance Components

Consequently, the assurance activities specified in WLASPP apply to the TOE evaluation.

6. TOE Summary Specification

This chapter describes the security functions:

- Security audit
- Cryptographic support
- User data protection
- Identification and authentication
- Security management
- Protection of the TSF
- Resource utilization
- TOE access
- Trusted path/channels

6.1 Security audit

The TOE is able to generate log records for security relevant and other events as they occur. The events that can cause an audit record to be logged include starting and stopping the audit function, any use of an administrator command via the CLI and Web interfaces, as well as all of the events identified in Table 2.

In general, the logged audit records identify the date and time, the nature or type of the triggering event, an indication of whether the event succeeded, failed or had some other outcome, and the identity of the agent (e.g., user) responsible for the event (e.g., user or network host). The logged audit records also include event-specific content that includes at least all of the content required in Table 2.

When audit records are being generated, the TOE can filter them based on severity level (i.e., syslog event type). Furthermore, the records can be filtered to include records based on device interface and wireless client identity (MAC address).

The TOE includes an internal log implementation that can be used to store and review audit records locally. The default maximum size of the log file depends on the device model. However, the administrative guidance recommends setting the maximum size to a value between 1 MB and 10 MB to ensure normal operation of the device. Audit records are viewable through the Monitor, System and Manage roles. Alternately, the TOE can be configured to send generated audit records to an external syslog server using IPsec.

Note that audit records are not buffered for transmission to the syslog server. If the connection to the syslog server goes down, generated audit records are not queued and will not be transmitted to the syslog server when the connection is re-established. However, audit records will still be delivered to any other configured audit destinations, such as the log buffer and local log file. Additionally, the TOE generates audit records when connection to the syslog server is lost and when it is restored, and these audit records are sent to any other configured audit destinations. Therefore, the administrator is advised to ensure additional audit destinations are configured so that generated audit records will still be available for review in the event of loss of connectivity to the syslog server. In addition, multiple log servers can be configured to provide redundancy.

The TOE also generates an SNMP trap to notify the loss of connectivity to a syslog server. By default, this trap is recorded to each of the following audit destinations (where configured): console; monitor terminal; trap buffer; SNMP module; web interface; and log file.

The Security audit function is designed to satisfy the following security functional requirements:

- FAU_GEN.1: The TOE can generate audit records for events include starting and stopping the audit function, administrator commands, and all other events identified in Table 2. Furthermore, each audit record identifies the date/time, event type, outcome of the event, responsible subject/user, as well as the additional event-specific content indicated in Table 2.

- FAU_GEN.2: The TOE identifies the responsible user for each event based on the specific administrator or network entity (identified by IP address) that caused the event.
- FAU_SAR.1: TOE administrators can view audit data through the TOE's internal log implementation.
- FAU_SAR.2: Only users logged in with the Monitor, System or Manage roles can view audit data.
- FAU_SEL.1: The TOE has the ability to select audit records to include or exclude in its log based on success or failure, device interface, wireless client identity or general (i.e., syslog) event type.
- FAU_STG.1: The TOE protects locally stored audit records from unauthorized modification or deletion by limiting access to those records to authorized administrators only.
- FAU_STG_EXT.1: The TOE can be configured to export audit records to an external syslog server and can be configured to use IPsec for communication with the syslog server.
- FAU_STG_EXT.3: The TOE will issue an SNMP trap when it discovers the configured external syslog server is not responding.
- FAU_STG_EXT.4: If the TOE's audit logs are full its default action is to overwrite the oldest stored audit records (FAU_STG_EXT.4.1.b). Comware v5 also has an overwrite-protection function that prevents the audit records from being overwritten if audit logs are full. The authorized administrator can configure the log file overwrite-protection or use the default behavior. If overwrite protection is enabled, then when the log file is full or the storage device runs out of space, the TOE stops saving logs into the log file. The command to enable the 'info-center logfile overwrite-protection' has an optional parameter 'all-port-powerdown' that shuts down all the service ports on the device when the log file is full or the storage device runs out of space. (FAU_STG_EXT.4.1.a).

6.2 Cryptographic support

The TOE includes cryptographic algorithms that have been NIST validated under the Cryptographic Algorithm Validation Program (CAVP). The following functions have been CAVP certified in accordance with the identified standards.

Functions	Standards	Certificates
Asymmetric key generation		
• Domain parameter generation (key size 2048 bits)	NIST Special Publication 800-56B	RSA #1542
• Random prime generation	NIST SP 800-90A	DRBG: #543
Symmetric key generation		
• WPA2 PRF-384 (128-bits)	IEEE 802.11-2007	N/A
Encryption/Decryption		
• AES CBC, CCM and CTR (128-256 bits)	FIPS PUB 197 NIST SP 800-38A NIST SP 800-38C IEEE 802.11-2007	#1840 #2930 #2940
Cryptographic signature services		
• RSA Digital Signature Algorithm (rDSA) (modulus 2048)	FIPS PUB 186-2 FIPS PUB 186-3	#1542
Cryptographic hashing		
• SHA-1 and SHA-256 (digest sizes 160 and 256 bits)	FIPS Pub 180-3	#2466 #2476
Keyed-hash message authentication		
• HMAC-SHA-1 (key size 160 bits and digest size 160)	FIPS Pub 198-1 FIPS Pub 180-3	#1864
• HMAC-SHA-256 (key size 256 bits and digest size 256 bits)	FIPS Pub 198-1 FIPS Pub 180-3	#1864
Random bit generation		

Random number generation		
• CTR_DRBG (AES) with software based noise source of 512 bytes of non-determinism	NIST Special Publication 800-90A	#543

Table 4 Cryptographic Functions

The following table demonstrates that the TSF complies with 800-56B. The table identifies the sections in 800-56B that are implemented by the TSF; and the "should", "should not", and "shall not" conditions from the publication along with an indication of whether the TOE conforms to those conditions with deviations rationalized. Key establishment is among the identified sections.

NIST SP800-56B Section Reference	"should", "should not", or "shall not"	Implemented accordingly?	Rationale for deviation
5.6	should	yes	
5.8	shall not	no	RSA-OAEP is not supported. The device supports RSA-PKCS1 Padding
5.9	shall not (first occurrence)	yes	
5.9	shall not (second occurrence)	yes	
6.1	should not	yes	
6.1	should (first occurrence)	yes	
6.1	should (second occurrence)	yes	
6.1	should (third occurrence)	yes	
6.1	should (fourth occurrence)	yes	
6.1	shall not (first occurrence)	yes	
6.1	shall not (second occurrence)	yes	
6.2.3	should	yes	
6.5.1	should	yes	
6.5.2	should	yes	
6.5.2.1	should	yes	
6.6	shall not	yes	
7.1.2	should	yes	
7.2.1.3	should	yes	
7.2.1.3	should not	yes	
7.2.2.3	should (first occurrence)	no	RSA-OAEP is not supported. The device supports RSA-PKCS1 Padding
7.2.2.3	should (second occurrence)	no	RSA-OAEP is not supported. The device supports RSA-PKCS1 Padding
7.2.2.3	should (third occurrence)	no	RSA-OAEP is not supported. The device supports RSA-PKCS1 Padding
7.2.2.3	should (fourth occurrence)	no	RSA-OAEP is not supported. The device supports RSA-PKCS1 Padding
7.2.2.3	should not	no	RSA-OAEP is not supported. The device supports RSA-PKCS1 Padding
7.2.2.3	shall not	no	RSA-OAEP is not supported. The device supports RSA-PKCS1

NIST SP800-56B Section Reference	"should", "should not", or "shall not"	Implemented accordingly?	Rationale for deviation
			Padding
7.2.3.3	should (first occurrence)	no	RSA-KEM-KWS is not supported
7.2.3.3	should (second occurrence)	no	RSA-KEM-KWS is not supported
7.2.3.3	should (third occurrence)	no	RSA-KEM-KWS is not supported
7.2.3.3	should (fourth occurrence)	no	RSA-KEM-KWS is not supported
7.2.3.3	should (fifth occurrence)	no	RSA-KEM-KWS is not supported
7.2.3.3	should not	no	RSA-KEM-KWS is not supported
8	Should	yes	
8.3.2	should not	yes	

Table 5 NIST SP800-56B Conformance

The TOE uses a software-based deterministic random bit generator (DRBG) that complies with NIST SP 800-90, using CTR_DRBG (AES). The DRBG is seeded with 128 bits of entropy drawn from the Comware entropy pool of 512 bytes. The design architecture of the Comware entropy source is the same as the architecture of the Linux kernel entropy pool. The noise sources for the Comware entropy pool include interrupt, process scheduling and memory allocation. Since the mechanism for seeding the DRBG has access to a live entropy source, it is permissible to instantiate the DRBG with 128 bits, in accordance with NIST SP 800-90. The secret value x used in the IKE Diffie-Hellman key exchange ('x' in gx mod p)and each nonce is generated using the random bit generator CTR_DRBG (AES).

The TOE is designed to zeroize secret and private keys when they are no longer required by the TOE. Table 6 identifies the applicable secret and private keys and summarizes, how and when they are deleted. Note that only some of the keys and CSPs are applicable to the evaluation. Also note that where identified zeroization occurs as follows: 1) when deleted from FLASH, the previous value is overwritten once with zeroes; 2) when added or changed in FLASH, any old value is overwritten completely with the new value; and, 3) the zeroization of values in RAM is achieved by overwriting once with zeroes.

#	Key/ CSP Name	Generation/ Algorithm	Description	Storage	Zeroization
CSP1	RSA private keys	CTR_DRBG(AES)/RSA(2048 bits)	Identity certificates for the security appliance itself and also used in IPsec, TLS, and SSHV2 negotiations.	FLASH (cipher text/AES-CTR-256) and RAM (plain text)	FLASH: Using CLI command to zeroize. RAM: Resetting or rebooting the security appliance.

#	Key/ CSP Name	Generation/ Algorithm	Description	Storage	Zeroization
CSP2	DSA private keys *(note that DSA is not included in the evaluated configuration)*	CTR_DRBG(AES)/DSA(2048 bits)	Identity certificates for the security appliance itself and also used in TLS and SSHV2 negotiations.	FLASH (cipher text/ AES-CTR-256) and RAM (plain text)	FLASH: Using CLI command to zeroize. RAM: Resetting or rebooting the security appliance.
CSP2-1	ECDSA Private keys *(note that ECDSA is not included in the evaluated configuration)*	CTR_DRBG(AES)/ECDSA(P-256)	Identity certificates for the security appliance itself and also used in SSHV2 negotiations.	FLASH (cipher text/ AES-CTR-256) and RAM (plain text)	FLASH: Using CLI command to zeroize. RAM: Resetting or rebooting the security appliance.
CSP3	Diffie-Hellman Key Pairs	CTR_DRBG(AES)/ DH(2048 bits modulus)	Key agreement for IKE, TLS, and SSHV2 sessions.	RAM (plain text)	Resetting or rebooting the security appliance.
CSP4	Public keys	DSA(2048 bits) / RSA(2048 bits) / ECDSA (P-256) *(note that DSA and ECDSA are not included in the evaluated configuration)*	Public keys of peers.	FLASH(plain text)/RAM (plain text)	Delete public keys of peers from configuration, write to startup config, then reboot
CSP5	HTTPS TLS Pre-Master Secret	Shared secret(48 bytes)	Shared secret created using asymmetric Cryptography	RAM (plain text)	Resetting or rebooting the security appliance.
CSP6	HTTPS TLS Encryption Key	AES-CBC (128-bits,256-bits)	used to encrypt HTTPS data.	RAM (plain text)	Resetting or rebooting the security appliance.
CSP7	HTTPS TLS Integrity Key	HMAC- SHA-1(160-bits)	used for HTTPS integrity protection.	RAM (plain text)	Resetting or rebooting the security appliance.
CSP8	SSHV2 Session Keys	CTR_DRBG(AES) Algorithms: AES(128-bits, 256-bits), HMAC-SHA1(160bits), HMAC-SHA1-96(160bits)	SSHV2 keys.	RAM (plain text)	Resetting or rebooting the security appliance

#	Key/ CSP Name	Generation/ Algorithm	Description	Storage	Zeroization
CSP9	IPsec authentication keys	CTR_DRBG(AES) + DH(2048bits modulus) Algorithms: HMAC-SHA1-96	Exchanged using the IKE protocol and the public/ private key pairs. These are authentication keys.	RAM (plain text)	Resetting or rebooting the security appliance
CSP10	IPsec traffic keys	CTR_DRBG(AES)+ DH(2048 bits modulus) Algorithms: AES(128-bits,192-bits, 256-bits)	Exchanged using the IKE protocol and the public/ private key pairs. These are encryption keys.	RAM (plain text)	Resetting or rebooting the security appliance
CSP11	IPsec authentication keys	HMAC-SHA1-96	Manually configured key for IPv6 routing protocol such as OSPFv3, RIPng, IPv6 BGP.	FLASH(cipher text/ AES-CTR-256)/RAM (plaintext)	Delete IPsec keys from configuration, write to startup config, then reboot
CSP12	IPsec traffic keys	AES(128-bits,192-bits,256-bits)	Manually configured keys for IPv6 routing protocol such as OSPFv3, RIPng, IPv6 BGP.	FLASH(cipher text/ AES-CTR-256)/RAM (plaintext)	Delete IPsec keys from configuration, write to startup config, then reboot
CSP13	IKE pre-shared keys	Shared Secret(8 ~ 128 bytes)	Entered by the Crypto-Officer in plain text form and used for authentication during IKE	FLASH(cipher text/ AES-CTR-256) and RAM (plaintext)	Deleting keys from the configuration via erase flash: command (or replacing), write to startup config, then reboot.
CSP14	IKE Authentication key	Generated using IKE (CTR_DRBG(AES)+HMAC-SHA1(160-bits)/HMAC-SHA256(256-bits)+DH(2048 bits modulus)). Algorithms: HMAC-SHA-1(160-bits), HMAC-SHA-256(256-bits)	Used to authenticate IKE negotiations	RAM (plain text)	Resetting or rebooting the security appliance

#	Key/ CSP Name	Generation/ Algorithm	Description	Storage	Zeroization
CSP15	IKE Encryption Key	Generated using IKE (CTR_DRBG(AES)+HMAC-SHA1(160-bits)/HMAC-SHA256(256-bits)+DH(2048 bits modulus)). Algorithms: AES(128-bits,192-bits,256-bits)	Used to encrypt IKE negotiations	RAM (plain text)	Resetting or rebooting the security appliance
CSP16	RADIUS shared secret keys	Shared Secret(8 ~ 64 bytes)	Used for authenticating the RADIUS server to the security appliance and vice versa. Entered by the Crypto-Officer in plain text form and stored in plain text form.	FLASH(cipher text/ AES-CTR-256) and RAM (plaintext)	Deleting keys from the configuration via erase flash: command (or replacing), write to startup config, then reboot.
CSP17	Usernames/ Passwords/ super password	Secret(8 ~ 63bytes)	Critical security parameters used to authenticate the administrator login or privilege promoting.	FLASH(cipher text/ AES-CTR-256) and RAM (plaintext)	Overwriting the passwords with new ones, write to startup config, then reboot.
CSP18	Certificates of Certificate Authorities (CAs)	RSA/DSA *(note that DSA is not included in the evaluated configuration)*	Necessary to verify certificates issued by the CA. Install the CA's certificate prior to installing subordinate certificates.	FLASH (plain text) and RAM (plain text)	1. Delete PKI domain from configuration via erase flash: command, write to startup config, then reboot. 2. Use “pki delete-certificate”CLI command to delete certificates, then reboot
CSP19	PRNG Seed Key	CTR_DRBG(AES)/AES(128bits)	Seed key for CTR_DRBG	RAM (plain text)	Zeroized by deleting firmware image
CSP20	802.11i Pairwise Master Key (PMK)	Shared secret(256bits)	The PMK is a secret shared between an 802.11 supplicant and authenticator, and is used to establish the other 802.11i keys.	RAM (plain text)	Resetting or rebooting the security appliance
CSP21	802.11i Key Confirmation Key (KCK)	HMAC- SHA-1(160-bits)	The KCK is used by IEEE 802.11i to provide data origin authenticity in the 4-Way Handshake and Group Key Handshake	RAM (plain text)	Resetting or rebooting the security appliance

#	Key/ CSP Name	Generation/ Algorithm	Description	Storage	Zeroization
			messages.		
CSP22	802.11i Key Encryption Key (KEK)	AES-Key Wrap(128-bits)	The KEK is used by the EAPOL-Key frames to provide confidentiality in the 4-Way Handshake and Group Key Handshake messages.	RAM (plain text)	Resetting or rebooting the security appliance
CSP23	802.11i Pairwise Transient Key (PTK)	AES-CCM(128-bits)	The PTK, also known as the CCMP Key, is the 802.11i session key for unicast communications.	RAM (plain text)	Resetting or rebooting the security appliance
CSP24	802.11i Temporal Key (TK)	AES-CCM(128-bits)	AES-CCM key used in 802.11i unicast communications.	RAM (plain text)	Resetting or rebooting the security appliance
CSP25	802.11i Group Temporal Key (GTK)	AES-CCM(128-bits)	The GTK is the 802.11i session key for broadcast communications.	RAM (plain text)	Resetting or rebooting the security appliance
CSP26	EAP-TLS Pre-Master Secret	Shared secret(48 bytes)	Shared secret created using asymmetric cryptography from which new EAP-TLS session keys can be created.	RAM (plain text)	Resetting or rebooting the security appliance
CSP27	EAP-TLS Encryption Key	AES-CBC(128bits)	AES key used to encrypt EAP-TLS session data.	RAM (plain text)	Resetting or rebooting the security appliance
CSP28	EAP-TLS Integrity Key	HMAC- SHA-1(160bits)	HMAC-SHA-1 key used for EAP-TLS integrity protection.	RAM (plain text)	Resetting or rebooting the security appliance
CSP29	EAP-TLS Peer Encryption Key	Shared Secret (32-byte)	This 32-byte key is master session key of the EAP-TLS authentication algorithm. It is the PMK for 802.11i.	RAM (plain text)	Resetting or rebooting the security appliance
CSP30	SNMPv3 Authentication/Encryption Key	AES(128bits)-SHA1(160bits)	Used to encrypt and verify SNMPv3 packet.	RAM (plain text)	Resetting or rebooting the security appliance

Table 6 Key/CSP Zeroization Summary

These supporting cryptographic functions are included to support the SSHv2 (RFCs 4251, 4252, 4253,4254, and 5656), and TLSv1 (RFC 2246)/HTTPS (RFC 2818) secure communication protocols.

The TOE supports TLSv1 with AES (CBC) 128 or 256 bit ciphers, in conjunction with SHA-1, and RSA. The following cipher suites are implemented by the TOE: TLS_RSA_WITH_AES_128_CBC_SHA, and TLS_RSA_WITH_AES_256_CBC_SHA. The TOE supports certificate-based identity authentication of the server and client by using the digital signatures. The TLS server and client obtain certificates from a CA through the PKI

The TOE supports SSHv2 with AES (CBC) 128 or 256 bit ciphers, in conjunction with HMAC-SHA-1 or HMAC-SHA-1-96, and RSA (with diffie-hellman-group14-sha1 for the key exchange method). SSHv2 packets are limited to 32,768 bytes. Diffie-hellman-group14-sha1 is the only allowed key exchange method used for the SSH protocol. This is pre-configured or hard-coded when the TOE in configured into FIPS mode. The TOE maintain a count of the bytes being collected in an internal buffer and when a packet is determined to be greater than 32,768 bytes in length, the TOE discards the packet and also terminates the SSH connection.

The TOE supports IPv6 that utilizes an implementation of IPsec in accordance with RFC 4303 for security. Confidentiality only ESP security service is disabled by default. If enabled it can be disabled using the transform command: transform{ ah | ah-esp | esp }. The symmetric cryptographic algorithms used by the TOE are AES-CBC-128 and AES-CBC-256 (both specified by RFC 3602) along with IKEv1 as defined in RFCs 2407, 2408, 2409, and RFC 4109. Note that the TOE only supports main mode, since aggressive mode is disabled in the evaluated configuration (FIPS mode). IKEv1 SA lifetimes can be limited to 24 hours for phase 1 and 8 hours for phase 2 and also to as little as 2.5 MB (and up to well over 200 MB) of traffic for phase 2. Phase 2 lifetimes can be configured in terms of both duration (in seconds) and traffic (in kilobytes). The relevant command line interface commands are ‘sa duration’ in the IKE proposal view for Phase 1, and ‘sa duration’ in the IPsec policy view for Phase 2. The IKEv1 protocols implemented by the TOE include DH Group 14 and support Pre-shared Keys, and RSA (aka rDSA) peer authentication with X.509v3 certificates conforming to RFC 4945. Pre-shared keys can be constructed of essentially any alphabetic character (upper and lower case), numerals, and special characters (e.g., “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”) and can be anywhere from 1(8 in FIPS mode) to 128 characters in length (e.g., 22 characters).

The TOE’s implementation conforms to IEEE 802.11-2007. This is assured by testing and certification by the Wi-Fi Alliance. The Group Temporal Key is distributed in accordance with cryptographic key distribution method: AES Key Wrap in an EAPOL-Key frame. Prior to distribution, the GTK is wrapped as described in RFC 3394 for AES Key Wrap using 128 bits of Key Data with a 128-bit KEK. The AAA key is generated on both supplicant and AS server during a successful 802.1X authentication. The PMK is the first 256 bits of a AAA key, which is defined in 802.11i protocol. AS server will send the AAA key copy to the authenticator which could be either a controller or an autonomous AP. Hence a PMKSA could be established between supplicant and its authenticator. For example, for EAP-PEAP-MSCHAPv2, the AAA key is contained in a MPPE RADIUS attribute within a secure tunnel. When multiple clients connect to the TOE, the GTK is sent from the authenticator to a supplicant encrypted by PTK during the 4-way handshake between the supplicant and authenticator.

The method also conforms to 802.11-2007 for the packet format and timing considerations. The cryptographic keys are not exposed during any part of the process. Section 6.9 describes how the TOE uses 802.1X for wireless client authentication and how it protects wireless communication using WPA2. The TOE implementation was also systematically tested internally as the product was developed and regression tested as internal policy dictates to ensure the implementation conforms to 802.11-2007.

The Cryptographic support function is designed to satisfy the following security functional requirements:

- FCS_CKM.1(1): See table above.
- FCS_CKM.1(2): See table above.
- FCS_CKM.2(1): See table above.
- FCS_CKM.2(2): See table above.
- FCS_CKM_EXT.4: Keys are zeroized when they are no longer needed by the TOE.
- FCS_COP.1(1): See table above.
- FCS_COP.1(2): See table above.
- FCS_COP.1(3): See table above.
- FCS_COP.1(4): See table above.
- FCS_COP.1(5): See table above.
- FCS_COP_EXT.1: See table above.

- FCS_HTTPS_EXT.1: The TOE supports HTTPS web-based secure administrator sessions.
- FCS_IPSEC_EXT.1: The TOE supports IPsec cryptographic network communication protection via an implementation of IPv6.
- FCS_RBG_EXT.1: See table above.
- FCS_SSH_EXT.1: The TOE supports SSHv2 interactive command-line secure administrator sessions as indicated above.
- FCS_TLS_EXT.1: The TOE supports HTTPS web-based secure administrator sessions.

6.3 User data protection

The TOE is designed to ensure its own internal integrity as well as to protect user data from potential, unintended reuse by clearing resources (e.g., memory) as they are allocated to create objects used in the implementation of the TOE operations. Note that volatile memory is the primary resource involved in normal TOE execution while its persistent storage is based on non-volatile flash memory.

When a network packet is sent, the buffer used by the packet is recalled and managed by the buffer pool. After that, if a new packet acquires a buffer from the buffer pool, the new packet data will be used to overwrite any previous data in the buffer. If an allocated buffer exceeds the size of the packet, the additional space will be overwritten (padded) with zeroes.

The User data protection function is designed to satisfy the following security functional requirements:

- FDP_RIP.2: The TOE always clears resources when allocated for use in objects.

6.4 Identification and authentication

The TOE requires users to be identified and authenticated before they can access any of the TOE functions. Note that the normal switching of network traffic is not considered accessing TOE functions in this regard.

In the evaluated configuration, authorized configured users can connect to the TOE's command line interface via a local console or remotely using SSHv2, or to the GUI via HTTP over TLS (HTTPS). In each case, the user is required to successfully log in using a valid userid (username) and password prior to successfully establishing a session through which TOE functions can be exercised.

The TOE also supports the use of certificate credentials using 2048 bit modulus RSA keys and SHA-1 for remote administration through SSHv2 and HTTPS. The authorized remote administrator must enter both a password and the correct public key for successful authentication. For a client that sends the user's public key information to the server through a digital certificate, the PKI domain must be identified on the server. This PKI domain verifies the client certificate. To make sure the authorized SSH users can pass the authentication, the specified PKI domain must have the correct CA certificate.

The certificates used are X509 v3 certificates as defined by RFC 5280 to support authentication for IPsec, TLS, and SSH connections. The X.509v3 certificates are stored as files under a default directory called 'pki' in the flash file system, the location of the directory is configurable. The store is protected from unauthorized access by user privilege. Only authorized administrators with the privilege required (assigned by role) are permitted to import, export, or operate on local certificates.

Users can be defined locally within the TOE with a user identity, password, and privilege level. Alternately, users can be defined within an external RADIUS or TACACS/TACACS+ server configured to be used by the TOE, each of which also defines the user's privilege level in the TOE. Locally defined users are authenticated directly by the TOE, while remotely defined users are authenticated by the external server and the result is enforced by the TOE. In either case, any resulting session is dependent upon successful authentication and established sessions are associated with the privilege level (see section 6.5) assigned to the user. A successfully established session will be assigned the authenticated user's identity and privilege level and those attributes cannot change during the life of the session.

Note that wireless users can be defined locally or within an associated external RADIUS or TACACS/TACACS+ server configured by an administrator. In the case of locally defined wireless users, they are defined with a user name and password.

When logging in, if a user's password has been expired by the TOE, the user will be required to both provide their current expired password and also provide a new password that is acceptable to the TOE. This results in a password change for the user. Also, when logging in the TOE will not echo passwords so that passwords are not inadvertently displayed to the user and any other users that might be able to view the login display.

If a user fails to log in an administrator configured number of times in a row, the user is prohibited from logging in for the administrator configured period of time. The user is permitted to log in again after that time has lapsed. This method of locking out remote users must be configured in the evaluated configuration; and applies to all methods of remote administration (i.e., CLI over SSHv2, GUI over HTTPS).

Should a user have their session locked (e.g., due to inactivity), they are required to successfully re-authenticate, by reentering their identity and authentication data, in order to regain access to their locked session.

In order to ensure that passwords are changed periodically, an administrator can configure a maximum password lifetime for locally defined users. Additionally, an administrator can define a value which identifies the number of times a user can log in with an expired password before the password has to be changed. The password lifetime is checked each time a user logs in and if the configured lifetime is expired, the user is notified that the password has expired. The configured value allowing the use of expired passwords is also checked and if that value has been exceeded the user is required to change their password immediately. Note that the TOE can also be configured with a minimum password update interval to similarly ensure that passwords are not changed too frequently.

When changing passwords, they must be composed of upper and lower case letters, numbers and special characters and ~`!@#$%^&*()_+-={}|[]\:";'<>,./. Also, new passwords have to satisfy configured minimum password length. The default in FIPS mode is 15. The administrator can specify a minimum password length of 15 to 32 characters. New passwords must have at least four characters different than the previous one retained within the scope of the configured history.

Administrators have even more control over password composition using configurable complexity checking. First, the number (1 through 4) of categories (upper case letters, lower case letters, numbers, and special characters) can be configured. Next, the minimum number of characters in each of the required categories can also be configured. Finally, a password complexity feature can be enabled which ensures a password cannot contain the username or the reverse of the username and also that no character of the password is repeated three or more times consecutively.

The Identification and authentication function is designed to satisfy the following security functional requirements:

- FIA_8021X_EXT.1: Wireless users can be defined locally or within an associated external RADIUS server conforming to RFCs 2865 and 3579. Testing and certification by the Wi-Fi Alliance ensures that the implementation conforms to the 802.1X-2010 standard and is operating correctly. The developer test methodology includes functional tests that systematically test that the product was developed and conform to the standard. Additionally, internal developer policy includes code reviews and approval milestones to help ensure the implementation conforms.
- FIA_AFL.1: The administrator can configure a non-zero threshold for authentication failures (the default is three attempts) that can occur before the TOE takes action to prevent subsequent authentication attempts. The TOE can be configured to lock the user account until an administrator specified time-limit. The default is 1 minute. The TOE prevents the user from logging in for the specified time –interval. A user failing to log in after the specified number of attempts must wait for 1 minute (or the configured time interval) before trying again.
- FIA_PMG_EXT.1: The TOE implements a rich set of password composition and aging constraints as described above.
- FIA_PSK_EXT.1: The TOE supports pre-shared keys that can be used with WPA2, and can be constructed of essentially any alphabetic character (upper and lower case), numerals, and special characters (e.g., "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")") and can be anywhere from 1 to 64 characters in length (e.g., 22 characters). In FIPS mode the minimum length of a pre-shared key is 8 characters. The TSF conditions the text-based pre-shared keys using SHA-1 to transform the text to the bit string used by the

IPsec and WPA2 protocols. The PSK input is hashed twice using SHA1. This generates 40 bytes, of which the first 32 bytes are used.

- FIA_UAU.6: The TOE requires re-authentication when changing passwords and unlocking locked sessions.
- FIA_UAU.7: The TOE does not echo passwords as they are entered.
- FIA_UAU_EXT.5: The TOE implements a local password-based authentication mechanism and supports remote authentication using RADIUS or TACACS+. Administrative users with expired passwords are locked out until their password is reset by an administrator
- FIA_UIA_EXT.1: The TOE doesn't offer any services or access to its functions without requiring a user to be identified and authenticated.
- FIA_X509_EXT.1: The TOE protects, stores and allows authorized administrators to load X.509v3 certificates for use to support authentication.

6.5 Security management

The TOE supports four privilege levels (i.e., roles): Visit, Monitor, System, and Manage. Manage is the highest privilege level followed closely by the System privilege level and, given limited differences, for the purpose of this Security Target both are considered instances of the 'Authorized Administrator' as defined in the WLASPP. The other two privilege levels represent logical subsets of those security management roles, but do not offer any security relevant configuration management capabilities.

Visit: Involves commands for network diagnosis and accessing an external device. Configuration of commands at this level cannot survive a device restart. Upon device restart, the commands at this level will be restored to the default settings. Commands at this level include ping, tracert, telnet and ssh2.

Monitor: Involves commands for system maintenance and service fault diagnosis. Commands at this level are not allowed to be saved after being configured. After the switch is restarted, the commands at this level will be restored to the default settings. Commands at this level include debugging, terminal, refresh, reset, and send.

System: Involves service configuration commands, such as routing configuration commands and commands for configuring services at different network levels. By default, commands at this level include all configuration commands except for those at the manage level.

Manage: Involves commands that influence the basic operation of the system and commands for configuring system support modules. By default, commands at this level involve the configuration commands of file system, SFTP, STELNET, user management, level setting, and parameter settings within a system (which are not defined by any protocols or RFCs).

The System and Manage roles, and hence the Authorized Administrator, are the only roles capable of managing the security functions of the TOE. The other roles are limited to non-security relevant functions and review of information.

The TOE offers command-line, and web-based graphical user interfaces each providing a range of security management functions for use by an authorized administrator. Among these functions are those necessary to manage all aspects of the cryptographic functions of the TOE, those necessary to manage the security audit functions of the TOE, those necessary to manage the authentication functions of the TOE, those necessary to enable or disable the network services offered by the TOE (including those that might not require users to be authenticated), and the functions necessary to review the TOE versions, update the TOE components, and also to verify the validity of those updates.

The TOE also offers the following functions, limited to the Authorized Administrator (i.e., System and Manage roles):

- Query and set the encryption/decryption of network packets (via FCS_COP.1(1)) in conformance with the administrators configuration of the TOE,
- Query, enable or disable Security Audit,

- Query, set, modify, and delete the cryptographic keys and key data, and
- Enable/disable verification of cryptographic key testing.

Note that the exception to limiting management of security relevant data to the Authorized Administrator is that all users (including wireless users) can change their own passwords (when locally defined by the TOE).

Wireless users are considered a 'role' in the context of the WLANPP though the TOE doesn't really offer any special recognition for them as 'wireless' users per se.

The TOE ensures that values entered by users are valid in accordance with the validity requirements of the data in question. In particular passwords are subject to acceptability criteria as claimed in this ST and certificates are subject to checksum checking to ensure they are not only valid, but are presumably secure.

The TOE is designed specifically to provide access only to hashed (and not plain text) passwords and also, while cryptographic keys can be entered, the TOE does not disclose any keys stored in the TOE.

The Security management function is designed to satisfy the following security functional requirements:

- FMT_MOF.1: The TOE limits management of all security functions to Authorized Administrators (i.e., System and Manage roles).
- FMT_MTD.1(1): The TOE restricts the access to manage TSF data that can affect the security functions of the TOE to Authorized Administrators (i.e., System and Manage roles).
- FMT_MTD.1(2): The TOE only allows access to hashed passwords and does not allow them to be read in plaintext.
- FMT_MTD.1(3): The TOE does not disclose any keys stored in the TOE.
- FMT_SMF.1: The TOE includes the functions necessary to enable/disable available network services, to manage the cryptomodule and associated functions, and to manage and verify updates of the TOE software and firmware.
- FMT_SMR.1: The TOE includes four defined administrator roles, two of which correspond to the required 'Authorized Administrator'. The TOE can define and recognize wireless users, though they are not explicitly identified as such.

6.6 Protection of the TSF

The TOE is an appliance and as such is designed to work independent of other components to a large extent. Secure communication with third-party peers is addressed in section 6.9 and secure communication among multiple instances of the TOE is limited to a direct link between redundant switch appliances deployed in a high-availability configuration and communication between Access Point and Access Controller TOE devices. Normally redundant components are co-located and connected via a link that would not be exposed outside of the same physical environment. As such, no additional protection (e.g., encryption) should be necessary in most operational environments. Similarly, Access Points and associated Access Controllers would often be co-located. When not co-located, IPsec must be configured to protect the network traffic between the devices.

The TOE utilizes SSHv2, and HTTPS for secure communications.

The TOE is a hardware appliance that, with one exception, includes a hardware-based real-time clock. The TOE's embedded OS manages the clock and exposes administrator clock-related functions. The TOE can also be configured to use a network time server in order to automatically synchronize the time of its internal clock. The exception is that the 'FIT' model Access Point TOE devices do not actually include an internal clock, but rather rely on an associated Access Controller to provide time information when needed.

The TOE includes a number of built in diagnostic tests that are run during start-up to determine whether the TOE is operating properly. An administrator can configure the TOE to reboot or to stop, with errors displayed, when an error is encountered. The built-in self-tests include basic read-write memory, flash read, software checksum tests, and device detection tests. Furthermore, the TOE is designed to query each pluggable module which in turn includes its own diagnostics that will serve to help identify any failing modules. Similarly, the TOE includes cryptographic self-tests designed to ensure the key generation, key error detection, cryptographic algorithms, and (pseudo) random

number generators are all working correctly and to verify the integrity of applicable security relevant data. The tests use the applicable cryptographic algorithm to calculate a result using the key and plain text and compare the calculated result with the known result. If they are not identical, the known-answer test fails. Additionally, conditional self-tests are run when an asymmetrical cryptographic module or a random number generator module is invoked. Conditional self-tests include the following:

- Pair-wise consistency test—This test is run when a DSA/RSA/ECDSA asymmetrical key-pair is generated. It uses the public key to encrypt a plain text, and uses the private key to decrypt the encrypted text. If the decryption is successful, the test succeeds. Otherwise, the test fails.
- Continuous random number generator test—This test is run when a random number is generated. If two consecutive random numbers are different, the test succeeds. Otherwise, the test fails. This test is also run when a DSA/RSA/ECDSA asymmetrical key pair is generated

These latter tests are all subject to CAVP certification and are designed to run at appropriate times – during start-up, when keys are generated, at the request of an administrator, or during other required circumstances. If any self-tests fail during power-on then none of the TOE's roles can perform services. The power-on self-tests are performed prior to the initialization of the forwarding function, which prevents the security appliance from passing any data during a power-on self-test failure. An error detection code (EDC) is used for the Firmware Integrity Test (RSA 2048 with SHA-256 which acts as a 256 bit EDC).

Implementation	Tests Performed
Security Appliance Software	Software/firmware Test (RSA 2048 with SHA-256 which acts as a 256 bit EDC)
	DSA KAT (signature/verification)
	RSA KAT (signature/verification)
	RSA KAT (encrypt/decrypt)
	ECDSA KAT (signature/verification)
	AES KAT (encrypt/decrypt)
	Triple-DES KAT (encrypt/decrypt)
	SHA-1 KAT
	SHA-256 KAT
	HMAC SHA-1 KAT
	HMAC SHA-256 KAT
	DRBG KAT

Table 7 HP unified wired-WLAN module, appliance and switches Power-On Self-Tests

The conditional self-tests are identified in the table below. Conditional self-tests run when a unified wired-WLAN module, appliance or switches generate an RSA key pair and when it generates a random number.

1. For RSA pairwise consistency test, sign/verify and encrypt/decrypt are both performed.
2. Only use CAVP-approved CTR DRBG to generate random number.
3. Firmware load using an Approved RSA 2048 with SHA-256

Implementation	Tests Performed
Security Appliance Software	Pairwise consistency test for RSA
	Pairwise consistency test for DSA
	Pairwise consistency test for ECDSA
	Continuous Random Number Generator Test for the CAVP-approved CTR DRBG
	Continuous Random Number Test for entropy source
	Manual key entry test

Table 8 HP unified wired-WLAN module, appliance and switches Conditional Self-Tests

If any of the self-tests fail the administrator may choose to run the self-tests again. If the self-tests still fail, the software will fail to load and the administrator should contact HP for support. Likewise, if the firmware integrity

test fails, the administrator should contact HP for support. To verify whether the test has passed or failed, the administrator should run the SHA Hash command on the appliance. If the hash value is different from release notes of this software, contact HP for support. At the conclusion of a successful self-test run and after the TOE has been configured according to the guidance documentation the TOE is in a secure state. This includes configuring the product to run in FIPS mode.

The TOE is designed to support upgrades to the boot ROM program and system boot file as well as to support software hotfixes. The TOE provides interfaces so that an administrator can query the current boot ROM program or system boot file versions as well as to identify any installed patches. Both the boot ROM program and system boot file can be upgraded via the Boot ROM menu or the command line interface, but a reboot is required in each case. Hotfixes, which can affect only the system boot file, can be installed via the command line interface and do not require a reboot to become effective.

The TOE includes a validity checking function that can be enabled when upgrading the boot ROM program, while system boot files and software patches are always validated prior to installation. In each case, the upgrade version will be checked to ensure it is appropriate and the upgrade file will be verified using an embedded digital signature verified against a configured trusted public certificate. If the version is incorrect or the signature cannot be verified, the upgrade will not proceed in order to protect the integrity of the TOE. More specifically, each update includes a header and data. The header includes a SHA-256 secure hash of the data that is signed (using rDSA/RSA 2048) by HP. In order to verify the data, the TOE generates a SHA-256 hash of the update data, compares it with the signed hash in the update header to ensure they match, and verifies the hash signature using its configured public key.

The Protection of the TSF function is designed to satisfy the following security functional requirements:

- FPT_FLS.1: If any self-tests fail during power-on then none of the TOE's roles can perform services.
- FPT_ITT.1: The TOE implements IPsec to protect communications between Access Points and the Access Controller,
- FPT_STM.1: The TOE includes its own hardware clock and is capable of being configured to use a network time server for synchronization.
- FPT_TST_EXT.1: The TOE includes a number of power-on diagnostics that ensure the TOE is functioning correctly. The power on self-tests ensure the availability of FIPS-allowed cryptographic algorithms; ensure the successful generation of asymmetric key pairs; and ensure that the random number generator is operating correctly.
- FPT_TUD_EXT.1: The TOE provides functions to query and upgrade the versions of the boot ROM program and system boot file (including installing hotfixes). Digital signatures are used to ensure the integrity of each upgrade prior to performing the upgrade; this checking is optional for the boot ROM program since special circumstances might require those checks to be disabled.

6.7 Resource utilization

The TOE is designed so that all administrative sessions including local sessions and those available via the SSH and HTTPS interfaces can be limited. Locally defined users can be limited to a maximum number of concurrent administrative sessions. Remotely defined administrator sessions can be restricted to a maximum number of concurrent sessions based on their domain membership. Each established session has a predefined amount of memory and CPU resources available to those sessions.

The TOE can limit the maximum number of concurrent interactive sessions that a particular local user can have at any given time. The 'local-user abc access-limit' command is used to limit the number of concurrent sessions that can be logged on to the locally (i.e., TOE) defined user 'abc'. This includes local users and users logging on remotely via the SSH and HTTPS interfaces. All concurrent sessions initiated via any of these interfaces using the same locally defined user account combine together to restrict this particular user's total number of permitted sessions.

If the user is defined at the remote server, then session control is domain based. Concurrent session restrictions are implemented at the remote server using the "access-limit" command under the domain. This command defines the threshold of the number of concurrent sessions permitted within a domain.

If the concurrent session threshold is reached, new sessions using the same username (for locally defined users) will be blocked. Or in the case of users defined at the remote server, new sessions for users defined within the domain will be blocked.

When memory usage reaches the defined threshold, the Comware memory manager will notify the offending task to free memory to ensure administrators will always have access to necessary memory resources. Similarly, Comware is a non-preemptive system and each task has its own limited and scheduled CPU time slice. This ensures the administrator tasks can always get CPU resources.

The Resource utilization function is designed to satisfy the following security functional requirements:

- FRU_RSA.1: The TOE limits the number of interactive user sessions an administrator can have at any given time and also the memory and CPU resources available to each of those sessions.

6.8 TOE access

The TOE can be configured to display administrator-configured advisory banners that will appear under a variety of circumstances. A session banner can be configured to be displayed when a session is established. A login banner can be configured to display welcome information displayed in conjunction with login prompts. A message of the day can also be configured to be displayed before authentication is completed. A legal banner can be configured to present legal advisories prior to a user logging in and this banner waits, requiring the user to confirm whether they want to continue with the authentication process.

The TOE can be configured by an administrator to set an interactive session timeout value (any integer value in minutes and also optionally in seconds, with 0 disabling the timeout) – the default timeout is 10 minutes. A remote session that is inactive (i.e., no commands issuing from the remote client) for the defined timeout value will be terminated. A local session that is similarly inactive for the defined timeout period will be locked. Once locked, the TOE will not interact with the console display or accept console inputs except to re-authenticate the user that was locked. The user will be required to re-enter their user id and their password so they can be reauthenticated. If the user id and password match those of the user that was locked, the session is reconnected with the console and normal input/output can again occur for that user.

The TOE can deny establishment of a wireless client session based on MAC address, time, and day of the week. The nature of wireless client access to an Access Point (and thence to the wired network) means it is not possible to deny session establishment based on location (e.g., IP address) as this can't be determined until the wireless client is authenticated and the session established. The TOE denies access by adding the client's MAC address to a blacklist. The TOE can use a scheduled job to place the MAC address on the blacklist for specified day and time.

The TOE access function is designed to satisfy the following security functional requirements:

- FTA_SSL.3: The TOE terminates remote sessions that have been inactive for an administrator-configured period of time.
- FTA_SSL.4: Administrators can lock or terminate their sessions which will prevent access without reauthentication.
- FTA_SSL_EXT.1: The TOE locks local sessions that have been inactive for an administrator-configured period of time. Locked sessions are disconnected from the local console input/output functions and can be reconnected only if the locked user correctly reenters their user id and password in order to be reauthenticated.
- FTA_TAB.1: The TOE can be configured to display administrator-defined advisory banners when administrators successfully establish interactive sessions with the TOE.
- FTA_TSE.1 The TOE can deny establishment of a wireless client session based on MAC address, time, and day of the week.

6.9 Trusted path/channels

The TOE can be configured to export audit records to an external syslog server using IPsec. This ensures exported audit records are protected from disclosure or modification. The TOE can be configured to utilize IPsec via IPv4 or IPv6 connections. Of course, the syslog server would need to be configured to also use IPv4 or IPv6.

Note that other remote peers, such as NTP, RADIUS, and TACACS/TACACS+ servers, could also be configured to utilize IPv4 or IPv6.

To support secure remote administration, the TOE includes implementations of SSHv2, and HTTPS (HTTP over TLSv1). In each case, a remote host (presumably acting on behalf of an administrator) can initiate a secure remote connection for the purpose of security management. Note that only the local console is available by default and each of these remote administration services can be independently enabled by an administrator.

In the cases of SSHv2 and HTTPS, the TOE offers both a secure command line interface (CLI) and a graphical user interface (GUI) interactive administrator sessions. An administrator with appropriate SSHv2 or HTTPS capable clients can establish secure remote connections with the TOE. However, to successfully establish such an interactive session, the administrator must be able to provide acceptable user credentials (e.g., user id and password), after which they will be able to issue commands within their assigned authorizations.

The TOE provides 802.11n wireless protocol support which is backward compatible to 802.11a/b/g clients. When a wireless network client wants to connect to the TOE (Access Point of Access Controller), 802.1X is used to gather the wireless client and user credentials in order to authenticate the wireless client. Once a wireless client is successfully authenticated, an encrypted channel using WPA2 is used to protect that wireless connection from network traffic disclosure or modification.

All of the secure protocols are supported by the CAVP validated cryptographic algorithms included in the TOE implementation.

The Trusted path/channels function is designed to satisfy the following security functional requirements:

- FTP_ITC.1: The TOE can be configured to use IPsec via IPv4 or IPv6 to ensure sensitive data (audit records, NTP data, and authentication data) is not subject to inappropriate disclosure or modification.
- FTP_TRP.1: The TOE provides SSH and HTTPS, based on its embedded cryptomodule, to support secure remote administration. In each case, the administrator can initiate the remote session, the remote session is secured (disclosure and modification) using CAVP certified cryptographic operations, and all remote security management functions require the use of one of these secure channels.

7. Protection Profile Claims

The ST conforms to the *Protection Profile for Wireless Local Area Network (WLAN) Access Systems*, version 1.0, 01 December 2011 (WLASPP). As explained previously, the security problem definition, security objectives, and security requirements have been drawn verbatim from the WLASPP.

8. Rationale

This security target includes by reference the WLASPP Security Problem Definition, Security Objectives, and Security Assurance Requirements. The security target makes no additions to the WLASPP assumptions. WLASPP security functional requirements have been reproduced with the protection profile operations completed. Operations on the security requirements follow WLASPP application notes and assurance activities. Consequently, WLASPP rationale applies but is incomplete. The TOE Summary Specification rationale below serves to complete the rationale required for the security target.

8.1 TOE Summary Specification Rationale

Each subsection in Section 6, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. **Table 9 Security Functions vs. Requirements Mapping** demonstrates the relationship between security requirements and security functions.

	Security audit	Cryptographic support	User data protection	Identification and authentication	Security management	Protection of the TSF	Resource utilization	TOE access	Trusted path/channels
FAU_GEN.1	X								
FAU_GEN.2	X								
FAU_SAR.1	X								
FAU_SAR.2	X								
FAU_SEL.1	X								
FAU_STG.1	X								
FAU_STG_EXT.1	X								
FAU_STG_EXT.3	X								
FAU_STG_EXT.4	X								
FCS_CKM.1(1)		X							
FCS_CKM.1(2)		X							
FCS_CKM.2(1)		X							
FCS_CKM.2(2)		X							
FCS_CKM_EXT.4		X							
FCS_COP.1(1)		X							
FCS_COP.1(2)		X							
FCS_COP.1(3)		X							
FCS_COP.1(4)		X							
FCS_COP.1(5)		X							
FCS_HTTPS_EXT.1		X							
FCS_IPSEC_EXT.1		X							
FCS_RBG_EXT.1		X							
FCS_SSH_EXT.1		X							
FCS_TLS_EXT.1		X							
FDP_RIP.2			X						
FIA_8021X_EXT.1				X					

	Security audit	Cryptographic support	User data protection	Identification and authentication	Security management	Protection of the TSF	Resource utilization	TOE access	Trusted path/channels
FIA_AFL.1				X					
FIA_PMG_EXT.1				X					
FIA_PSK_EXT.1				X					
FIA_UAU.6				X					
FIA_UAU.7				X					
FIA_UAU_EXT.5				X					
FIA_UIA_EXT.1				X					
FIA_X509_EXT.1				X					
FMT_MOF.1					X				
FMT_MTD.1(1)					X				
FMT_MTD.1(2)					X				
FMT_MTD.1(3)					X				
FMT_SMF.1					X				
FMT_SMR.1					X				
FPT_FLS.1						X			
FPT_ITT.1						X			
FPT_STM.1						X			
FPT_TST_EXT.1						X			
FPT_TUD_EXT.1						X			
FRU_RSA.1							X		
FTA_SSL.3								X	
FTA_SSL.4								X	
FTA_SSL_EXT.1								X	
FTA_TAB.1								X	
FTA_TSE.1								X	
FTP_ITC.1									X
FTP_TRP.1									X

Table 9 Security Functions vs. Requirements Mapping