National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Aruba Mobility Controller and Access Point Series

Report Number:	**CCEVS-VR-VID10569-2014**
Dated:	**22 October 2014**
Version:	**1.0**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Bradford O’Neill

Jean Petty

The MITRE Corporation

Common Criteria Testing Laboratory

Leidos (formerly SAIC, Inc.)
Columbia, MD

Table of Contents

List of Tables

1 Executive Summary

This report is intended to assist the end-user of this product and any Security Certification Agent for that end-user in determining the suitability of this Information Technology (IT) product in their environment. End-users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 4 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of Aruba Mobility Controller and Access Point Series devices running ArubaOS version 6.3.1.5-FIPS. It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation of the Aruba Mobility Controller and Access Point Series devices running ArubaOS version 6.3.1.5-FIPS was performed by Leidos (formerly Science Applications International Corporation (SAIC)) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America and was completed in October 2014. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1 and assurance activities specified in *Protection Profile for Wireless Local Area Network (WLAN) Access Systems*, Version 1.0, 1 December 2011. The evaluation was consistent with NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org).

The Leidos evaluation team determined that the product is conformant to *Protection Profile for Wireless Local Area Network (WLAN) Access Systems*, Version 1.0, 1 December 2011. The information in this VR is largely derived from the Assurance Activities Report (AAR) and associated test reports produced by the Leidos evaluation team.

The Aruba devices within the scope of the evaluation comprise the following Mobility Controllers and Access Points, all running ArubaOS version 6.3.1.5-FIPS:

- Aruba Mobility Controllers: Aruba 620, 650, 3200, 3400, 3600, 6000, 7210, 7220, and 7240
- Aruba Access Points: Aruba AP-92, AP-93, AP-104, AP-105, AP-114, AP-115, AP-134, AP-135, AP-175, AP-224, AP-225, RAP-3WN, RAP-5WN, RAP-108, RAP-109, and RAP-155.

The Aruba Mobility Controllers are wireless switch appliances that provide services and features including wireless and wired network mobility, centralized management, auditing, authentication, and remote access. The Aruba Access Point appliances service wireless clients. The ArubaOS is a suite of mobility applications that runs on all Aruba controllers and APs, and allows administrators to configure and manage the wireless and mobile user environment.

The TOE, when configured as specified in the guidance documentation, satisfies all of the security functional requirements stated in the Aruba Mobility Controller and Access Point Series Security Target.

1.1 Interpretations

Not applicable.

1.2 Threats

The ST identifies the following threats that the TOE and its operational environment are intended to counter:

- An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms
- A process or user may deny access to TOE services by exhausting critical resources on the TOE.
- Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
- 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.
- A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
- 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.
- User data may be inadvertently sent to a destination not intended by the original sender.

1.3 Organizational Security Policies

The ST identifies the following organizational security policies that the TOE and its operational environment are intended to fulfill:

- 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.
- The authorized users of the TOE shall be held accountable for their actions within the TOE.
- Administrators shall be able to administer the TOE both locally and remotely through protected communications channels.
- 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.
- The TOE must support standardized (RFCs) protocols for communication with a centralized audit server and a RADIUS authentication server.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs), using the Common Criteria for Information Technology Security Evaluation (CC) and its associated Common Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation, conduct security evaluations.

The NIAP Validation Body assigns validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of IT products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliant List (PCL).

Table 1 provides information needed to completely identify the product, including:

- the fully qualified identifier of the product as evaluated (the TOE)
- the ST, describing the security features, claims, and assurances of the product
- the conformance result of the evaluation
- the Protection Profile (if any) to which the product is conformant
- the organizations and individuals participating in the evaluation.

Table 1 – Evaluation Details

Evaluated Product:	Aruba Mobility Controller and Access Point Series, running ArubaOS version 6.3.1.5-FIPS
Sponsor:	Aruba Networks, Inc. 1344 Crossman Avenue, Sunnyvale, CA 94089-1113
Developer:	Aruba Networks, Inc. 1344 Crossman Avenue, Sunnyvale, CA 94089-1206
CCTL:	Leidos (formerly Science Applications International Corporation) 6841 Benjamin Franklin Drive, Columbia, MD 21046
Kickoff Date:	18 April 2013
Completion Date:	22 October 2014
Interpretations:	None
CEM:	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, Version 3.1, Revision 3, July 2009.
Evaluation Class:	None
PP:	Protection Profile for Wireless Local Area Network (WLAN) Access Systems, Version 1.0, 1 December 2011
Evaluation Personnel:	Leidos (formerly Science Applications International Corporation): Anthony J. Apted, Dawn Campbell, Chris Keenan, Kevin Micciche, Pascal Patin

Validation Body:	National Information Assurance Partnership CCEVS Bradford O'Neill, Jean Petty

3 Security Policy

The TOE enforces the following security policies as described in the ST.

> ***Note:*** *Much of the description of the security policy has been derived from Aruba Mobility Controller and Access Point Series Security Target and the Final ETR.*

3.1 Security Audit

The TOE is capable of auditing security relevant events such as logins, administrator actions, use of trusted channel and path, cryptographic operations, resource limitation exceeded, etc. Each audit event includes the date and time of the event, the type of event, the subject identity (if applicable), and the outcome of the event. The administrator can include and exclude events to be audited based on specific criteria.

The TOE may utilize its internal real-time clock chip and/or an extenral NTP server to provide a reliable timestamp and syslog server to store and protect the audit trail. The administrator is provided an interface in the operating environment to read audit logs and that interface is restricted.

3.2 Cryptographic Support

The TOE includes NIST-validated cryptographic mechanisms that 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, TLS, HTTPS and IPsec. It additionally includes mechanisms that support 802.11i wireless security.

3.3 User Data Protection

The TOE ensures that any data packets passing through do not inadvertently contain any residual information that might be disclosed inappropriately.

3.4 Identification & Authentication

The TOE can maintain administrator and user attributes, including credentials such as username and password for administrators and session key and role for remote authenticated users (username and password are stored in the internal database or authentication server). The TOE requires identification and authentication (either locally or remotely through external authentication server, internally, or both) of administrators managing the TOE. Wireless clients are identified and authenticated by different authentication mechanisms such as 802.1X, etc. More detailed information is provided in section 6.1.4. After an administrator-specified number of failed attempts, the user account is locked out. In addition, the password mechanism can be configured to have a minimum length of eight characters.

3.5 Security Management

The TOE provides the capability to manage auditing, cryptographic operations, password minimum length enforcement, user accounts, advisory banner, and timeout (inactivity threshold) value. The management functions are restricted to an administrator role. The role must have the appropriate access privileges or access will be denied. The wireless user role has no access to the management interfaces.

3.6 Protection of the TOE's Security Functions

The TOE provides integrity and security protection for all communication between its components. This prevents unauthorized modification or disclosure of TSF data during transmission. The TOE also protects itself against replay attacks using cryptographic protocols.

The TOE provides self-tests to ensure the correct operation of the cryptographic functions and TSF hardware. There is an option for the administrator to verify the integrity of stored TSF executable code.

The TOE includes mechanisms so that the administrator can determine the TOE version and update the TOE securely using digital signatures and published hashes.

3.7 Resource Utilization

The TOE can enforce maximum usage quotas on the number of concurrent sessions available to a defined group of users (role).

3.8 TOE Access

The TOE allows administrators to configure a period of inactivity for administrator and wireless user sessions. Once that time period has been reached while the session has no activity, the session is terminated. Administrators as well as wireless users can also terminate their own sessions at any time. A warning banner is displayed at the management interfaces (Web GUI and CLI) to advise users on appropriate use and penalty for misuse of system.

The TOE can restrict the ability to connect to administrative interfaces based on time/date, location, and device MAC address and blacklist status.

3.9 Trusted Path/Channels

The TOE provides an encrypted channel between itself and third-party trusted IT entities in the operating environment. The TOE also provides a protected communication path between itself and wireless users.

4 Assumptions

The ST identifies the following assumptions about the use of the product:

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

4.1 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (the assurance activities specified in *Protection Profile for Wireless Local Area Network (WLAN) Access Systems* and performed by the evaluation team).
2. This evaluation covers only the specific device models and software version identified in this document, and not any earlier or later versions released or in process.
3. The evaluation of security functionality of the product was limited to the functionality specified in the *Protection Profile for Wireless Local Area Network (WLAN) Access Systems*, Version 1.0, 1 December 2011. Any additional security related functional capabilities of the product were not covered by this evaluation.
4. This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.

5 Architectural Information

This section provides a high level description of the TOE and its components as described in the Security Target and guidance documentation.

The TOE consists of the following components:

- Aruba Mobility Controllers
- Aruba Access Points
- ArubaOS.

Aruba Mobility Controllers are hardware appliances consisting of a multicore network processor, Ethernet interfaces, and required supporting circuitry and power supplies enclosed in a metal chassis. ArubaOS, the software running on the Mobility Controller, consists of two main components, both implemented on multiple cores within a single network processor:

- Control Plane (CP)—implements functions which can be handled at lower speeds such as Mobility Controller system management (CLI and Web GUI), user authentication (e.g. 802.1X, RADIUS, LDAP), Internet Key Exchange (IKE), auditing/logging (syslog), and termination of protocols operating at the system level (e.g. SSH, TLS, NTP, etc.). The CP runs the Linux operating system along with various user-space applications (described below).
- Data Plane (DP)—implements functions that must be handled at high speeds such as high-speed switching functions (forwarding, VLAN tagging/enforcement, bridging), termination of 802.11 associations/sessions, tunnel termination (GRE, IPsec), and cryptographic acceleration. The DP runs a lightweight, proprietary real-time OS known as "SOS" (an acronym whose definition is no longer known).

The CP and DP are inseparable. Administrators install the software by loading a single file, identified as "ArubaOS". Internally, the Mobility Controller unpacks the ArubaOS software image into its various components. A given ArubaOS software image has a single version number, and includes all software components necessary to operate both Mobility Controllers and Access Points (APs). The Mobility Controller is responsible for storing the ArubaOS components needed to operate the APs, allowing APs to download their operating software from the Mobility Controller.

The CP runs the Linux OS along with various custom user-space applications that provide the following CP functions:

- Monitoring and managing critical system resources, including processes, memory, and flash
- Sending and receiving IPsec-encapsulated messages to and from managed APs as well as other Mobility Controllers
- Managing system configuration and licensing
- Managing an internal database used to store licenses, user authentication information, etc.
- Providing hardware monitoring, mobility management, wireless management, and radio frequency management services
- Providing a Command Line Interface (CLI)
- Providing a web-based (HTTPS/TLS) management UI for the Mobility Controller
- Providing various WLAN station and AP management functions

- Providing authentication services for the system management interfaces (CLI, web GUI) as well as for WLAN users
- Providing IPsec key management services for APs, VPN users, and connections with other Aruba Mobility Controllers
- Providing Network Time Protocol (NTP) service for APs, point to point tunneling protocol services for users, Layer 2 tunneling protocol services for users, SSH services for incoming management connections, SNMP client/agent services, and protocol independent multicast (routing) services for the controller
- Providing syslog services by sending logs to the operating environment.

The Linux OS running on the CP is a standard unmodified 2.6.32 kernel. Linux is a soft real-time, multi-threaded operating system that supports memory protection between processes. Only Aruba provided interfaces are used, and the CLI is a restricted command set. Administrators do not have access to the Linux command shell or operating system.

The DP is further subdivided into two subcomponents: Fast Path (FP) and Slow[1] Path (SP). The FP implements high-speed packet forwarding based on various proprietary tables and sends the packets to SP. The SP manages (create, delete, and age entries) all DP tables such as user, station, tunnel, route, ARP cache, session, bridge, VLAN, and port. The SP also performs deep packet inspection and cryptographic processing.

The DP is implemented on a multi-core network processor. There is a lightweight, Aruba-proprietary OS running on the network processor called SOS. SOS contains an Ethernet driver, a serial driver, a logging facility, semaphore support, and a crypto driver. This OS is not a general purpose operating system. In the Aruba 6000 with M3 controller card, an FPGA is also used to control and monitor the switch fabric, Ethernet interface hardware, and to provide security functionality such as filtering.

The DP and CP run on different hardware platforms but the security functionality remains the same, regardless of the model. The differences in the platforms are in the processors, memory capacity, physical interfaces, FPGA implementation, etc., and are based on performance and scalability requirements.

The AP is a hardware device that is enclosed in a plastic or metal casing. All APs contain chips to provide IEEE 802.11 wireless LAN functionality. Some models contain a separate CPU, while other models combine the CPU with the wireless LAN chip (an integrated approach known as “system on a chip”). Some AP models contain integrated antennas, while other models provide connectors for attaching external antennas. Software functionality for the APs is provided by ArubaOS, which is downloaded from the Mobility Controller and stored in a local flash memory partition. In the case of the APs, ArubaOS consists of a Linux kernel and various custom user-space applications. Although the AP’s operating system is named ArubaOS, the Linux kernel and user-space applications are different from those running on the Mobility Controller. The version number of ArubaOS running on the AP and the version number of ArubaOS running on the controller is the same—the two software images are bundled into a single image file that is installed by the administrator on the Mobility Controller. Similar to the controllers, the security functionality of the different APs is the same, with differences in platforms based on performance and scalability requirements only. At a high level, APs consist of the following subsystems:

- Processor subsystem—performs the packet processing functions on the packet
- Memory subsystem—contains memory which supports the Processor subsystem

[1] The entire DP (including both FP and SP elements) is a high-speed packet processor, so the SP designation should be understood to be relative.

- Ethernet Controller (i.e., Network Interface Controller) subsystem—includes integrated Ethernet Media Access Control (MAC) for transfer of 10/100 Ethernet packets between the AP and the wired network
- Radio Controller subsystem—an AP has one or two radio controllers, depending on model, 802.11a/n (5 GHz range) and 802.11b/g/n (2.4 GHz range)
- Wireless Antenna subsystem—interface between the wireless world and the AP. The antenna handles both 5 GHz and 2.4 GHz ranges. Some AP models include connectors for external antennas, while other AP models contain integrated antennas
- PoE (Power over Ethernet) subsystem—receives 48V power over the Ethernet
- USB subsystem—the AP-70 and RAP-5wn support one USB V2.0 compliant port (up to 480 Mbps). A PCI to USB 2.0 controller is used to interface to the system host
- Serial subsystem—all 802.11n APs support a serial console port that utilizes a RJ45 jack and connects directly to serial port 0 via the RS232 transceiver.

Aruba APs may or may not perform cryptographic processing, depending on administrator configuration. The default mode of operation is known as “tunnel mode”, in which raw encrypted 802.11 frames are passed through the AP and processed by the Mobility Controller without decryption or further processing in between. This mode of operation places fewer security constraints on the AP, since cleartext network traffic is never present in the AP. Other modes of operation are available as well, including “decrypt-tunnel mode”, in which wireless traffic is decrypted by the AP and forwarded to the Mobility Controller, and “bridge mode”, in which wireless traffic is decrypted and forwarded directly from the AP to the local LAN segment. In the CC evaluated configuration, only tunnel mode is used.

6 Documentation

6.1 Product Guidance

The guidance documentation examined during the course of the evaluation and delivered with the TOE is as follows:

- *ArubaOS 6.3.x User Guide*, October 2013, Ref 0511497-00
- *ArubaOS 6.3.x Command-Line Interface Reference Guide*, October 2013, Ref 0511500-00
- *ArubaOS 6.3.x Syslog Messages Reference Guide*, July 2013, Ref 0511324-01
- *ArubaOS 6.3 Quick Start Guide*, May 2012, Ref 0511320-01
- *ArubaOS 6.x MIB Reference Guide*, June 2013, Ref 0511323-01, Ref 0511320-02
- ArubaOS 6.3.1.5 Release Notes, April 2014, Ref 0511467-05v1
- ArubaOS 6.3 FIPS Security Policy (available at CMVP website)

The above documents are considered to be part of the evaluated TOE. Any additional customer documentation delivered with the TOE or made available through electronic downloads should not be relied upon for using the TOE in its evaluated configuration.

7 Product Testing

This section describes the testing efforts of the Evaluation Team. It is derived from information contained in the following:

- Aruba Mobility Controller and Access Point Series Common Criteria Test Report and Procedures

7.1 Developer Testing

The assurance activities in the Protection Profile for Wireless Local Area Network (WLAN) Access Systems do not specify any requirement for developer testing of the TOE.

7.2 Evaluation Team Independent Testing

The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in the Protection Profile for Wireless Local Area Network (WLAN) Access Systems. The Test Plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the Test Plan and documented the results in the test report identified above. All tests were executed on the following sample of platforms claimed in the ST:

- Aruba 7220 Mobility Controller
- Aruba 6000 Mobility Controller
- Aruba 3200 Mobility Controller
- Aruba 620 Branch Office Controller
- AP-92, AP-104, AP-175, AP-224, RAP-155

Testing was conducted from March 3 through March 15, 2012, with subsequent testing through August 2014, at the CCTL's facility in Columbia, MD. The testing demonstrated the TOE satisfies the security functional requirements specified in the Protection Profile for Wireless Local Area Network (WLAN) Access Systems.

The testing performed by the evaluation team is summarized as follows:

- The evaluation team confirmed the TOE's ability to generate the audit events specified in the ST, and to be able to specify that auditable events generate audit records based on various criteria
- The evaluation team confirmed the TOE's ability to establish a trusted channel with an external audit server, an external authentication server, and an NTP server, and to be able to communicate securely with each external server via the trusted channel
- The evaluation team confirmed the TOE appropriately protects Group Temporal Keys it transmits to wireless clients
- The evaluation team confirmed the TOE implements IPsec as specified in the PP
- The evaluation team confirmed the TOE supports RSA for public key authentication and password-based authentication over SSH
- The evaluation confirmed the TOE drops an SSH connection if it receives a packet over 256K bytes in length
- The evaluation team confirmed the TOE supports SSH connections using AES-CBC-128 and AES-CBC-256
- The evaluation team confirmed the TOE does not support DH Group 1 and that it does support DH Group 14

- The evaluation team confirmed the TOE implements the TLS ciphersuites specified in the ST
- The evaluation team confirmed the administrator can configure the TOE to lock out a user after a configured number of consecutive failed authentication attempts
- The evaluation team confirmed the TOE supports the specified password composition requirements, including the specified minimum length
- The evaluation team confirmed administrators are required to re-authenticate to the TOE prior to changing their passwords
- The evaluation team confirmed the TOE provides only obscured feedback when authentication information is entered at the local console
- The evaluation team confirmed, for all supported methods of administrator access, the TOE allows access to the administrative interfaces when the correct authentication credentials are provided, and denies access when incorrect credentials are provided, and that the services available without authentication are as specified in the ST
- The evaluation team confirmed the TOE implements pre-shared keys for use with IPsec as specified in the PP
- The evaluation team confirmed the TOE correctly validates X.509 certificates
- The evaluation team confirmed that, by default, the TOE cannot be administered from a wireless client
- The evaluation team confirmed the TOE provides self-tests to verify the integrity of TOE executables
- The evaluation team confirmed a legitimate update could be installed successfully on the TOE and that an illegitimate update was rejected
- The evaluation team confirmed the TOE enforces quotas on the amount of control-plane bandwidth that can be used by individual users simultaneously
- The evaluation team confirmed the TOE terminated a remote interactive session after the configured period of inactivity had elapsed
- The evaluation team confirmed the administrator was able to terminate an interactive session with the TOE
- The evaluation team confirmed the TOE displayed a configured notice and consent warning message for each method of access supported by the TOE
- The evaluation team confirmed the TOE can deny establishment of a wireless client session based on various criteria.

7.3 Penetration Testing

The evaluation team conducted an open source search for vulnerabilities in the product. The open source search did not identify any vulnerabilities applicable to the TOE in its evaluated configuration.

8 Evaluated Configuration

The evaluated version of the TOE is Aruba Mobility Controller and Access Point Series running ArubaOS version 6.3.1.5-FIPS, including the following series and models:

- Aruba Mobility Controllers: Aruba 620, 650, 3200, 3400, 3600, 6000, 7210, 7220, and 7240.
- Aruba Access Points: Aruba AP-92, AP-93, AP-104, AP-105, AP-114, AP-115, AP-134, AP-135, AP-175, AP-224, AP-225, RAP-3WN, RAP-5WN, RAP-108, RAP-109, and RAP-155.

9 Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in Protection Profile for Wireless Local Area Network (WLAN) Access Systems, Version 1.0, 1 December 2011 (WLANAS PP), in conjunction with version 3.1, revision 3 of the CC and the CEM. A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each assurance component. For Fail or Inconclusive work unit verdicts, the evaluation team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the evaluation team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the assurance activities in the WLANASPP, and correctly verified that the product meets the claims in the ST.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by the Leidos CCTL. The security assurance requirements are listed in the following table.

TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ADV_FSP.1	Basic functional specification
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.1	Labeling of the TOE
ALC_CMS.1	TOE CM coverage
ATE_IND.1	Independent testing - conformance
AVA_VAN.1	Vulnerability survey

10 Validator Comments/Recommendations

The validation team suggests that the consumer pay particular attention to the installation guidance to ensure the devices are placed into the evaluated configuration. In order to remain CC compliant, the device(s) must first be configured for FIPS mode.

As was noted in in the Clarification of Scope section of this report, the devices provide more functionality than was covered by the evaluation. Only the functionality claimed in the SFR's in the Security Target was evaluated. All other functionality provided by the devices needs to be assessed separately and no further conclusions should be drawn as to their effectiveness, nor can any claims be made relative to their security based upon this evaluation. The functionality associated with denying wireless clients access base on their location (FTA_TSE.1) merits special consideration. In this case, access restrictions using firewall policies to restrict connections from the wireless client's source IP address was verified, but access restrictions to virtual access points/SSIDs based on the user's role was not claimed or verified.

Note that the TOE provides capabilities to select the set of audited events from the set of all auditable events, but the selectable attributes do not align precisely with the attributes specified in the WLANAS PP. Specifically, the TOE does not provide the capability to exclude events based on administrator identity. In the TD0010 Technical Decision, the CCEVS found that the TOE capabilities were sufficient to meet the intent of the requirement for selectable audit events and plan to update the Protection Profile to more clearly define the requirements.

The validators note that the TD0002 and TD0016 Technical Decisions were also applied to this evaluation. These decisions allowed for better alignment between the WLANAS PP and the Network Device PP. The Technical Decisions are available on the NIAP web site.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the assurance activities prescribed in the WLANAS PP and that the evaluation team correctly verified that the product meets the claims of the associated Security Target.

11 Annexes

Not applicable.

12 Security Target

The ST for this product's evaluation is Aruba Mobility Controller and Access Point Series Security Target, Version 1.0, 9 September 2014.

13 Bibliography

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1, Revision 3, July 2009, CCMB-2009-07-001.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 3.1, Revision 3, July 2009, CCMB-2009-07-002.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 3.1, Revision 3, July 2009, CCMB-2009-07-003.
4. Common Methodology for Information Technology Security: Evaluation Methodology, Version 3.1, Revision 3, July 2009, CCMB-2009-07-004.
5. Protection Profile for Wireless Local Area Network (WLAN) Access Systems, Version 1.0, 1 December 2011.
6. Aruba Mobility Controller and Access Point Series Security Target, Version 1.0, 9 September 2014.