National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for

Hewlett-Packard Company Wireless LAN Access Controllers and Access Points

Report Number: CCEVS-VR-VID10554-2014
Dated: 15 December 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

Jerome Myers
The Aerospace Corporation

Ken Stutterheim
The Aerospace Corporation

Common Criteria Testing Laboratory

Leidos Inc. (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 for 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 the Hewlett-Packard Company Wireless LAN Access Controllers and Access Points (the Target of Evaluation, or TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the 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 Hewlett-Packard Company Wireless LAN Access Controllers and Access Points 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*, v1.0, 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 TOE comprises Access Controllers and Access Points. The Access Controllers consist 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 deployment. The Access Points include single- and dual-radio IEEE 802.11a/b/g/n devices.

The Leidos evaluation team determined that the TOE is conformant to *Protection Profile for Wireless Local Area Network (WLAN) Access Systems*, v1.0, 1 December 2011. The TOE, when configured as specified in the evaluated guidance documentation, satisfies all of the security functional requirements stated in Hewlett-Packard Company Wireless LAN Access Controllers and Access Points Security Target, Version 1.0, 31 October 2014. 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 validation team reviewed the evaluation outputs produced by the evaluation team, in particular the AAR and associated test reports. The validation team found that the evaluation showed that the TOE satisfies all of the security functional and assurance requirements stated in the Security Target (ST). The evaluation also showed that the TOE is conformant to *Protection Profile for Wireless Local Area Network (WLAN) Access Systems*, v1.0, 1 December 2011, and that the assurance activities specified in the Protection Profile had been performed appropriately. Therefore, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the Evaluation Technical Report are consistent with the evidence produced.

1.1 Interpretations

The following NIAP Technical Decisions were applied during the course of this evaluation:

- TD0009: WLAN AS and NDPP Errata 2

  This Technical Decision allowed the ST to claim the versions of FCS_SSH_EXT.1 and FCS_TLS_EXT.1 specified in Security Requirements for Network Devices Errata #2 rather than the versions specified in Protection Profile for Wireless Local Area Network (WLAN) Access Systems.

- TD0010: WLAN AS PP Flawed Statement of FAU_SEL.1

  This Technical Decision allowed the ST to exclude the "administrator identity" attribute from the list of attributes required to support FAU_SEL.1.

- TD0016: Application of TD0005 and ERRATA2 to WLANASPP for FPT_ITT, FTP_ITC, and FTP_TRP

  This Technical Decision allowed the evaluation team to waive the testing for the TOE ability to detect modification of channel data, associated with FPT_ITT.1, FTP_ITC.1 and FTP_TRP.1.

- TD0027: Removal of FPT_RPL.1 in WLAN AS PP

  This Technical Decision allowed the vendor to remove claims for FPT_RPL.1 from the ST.

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.

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) use the Common Criteria and Common Methodology for IT Security Evaluation (CEM) to conduct security evaluations, in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

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 and its evaluation.

Table 1: Evaluation Details

Evaluated Product:	Hewlett-Packard Company Wireless LAN Controllers and Access Points with Comware version 5.2.109
Sponsor:	Hewlett-Packard Development Company, L.P. 11445 Compaq Center Drive West Houston, Texas 77070
Developer:	Hewlett-Packard Development Company, L.P. 11445 Compaq Center Drive West Houston, Texas 77070
CCTL:	Leidos (formerly Science Applications International Corporation) 6841 Benjamin Franklin Drive Columbia, MD 21046
Kickoff Date:	2 June 2014
Completion Date:	December 2014
CC:	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009.
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 Greg Beaver Pascal Patin Kevin Steiner
Validation Body:	National Information Assurance Partnership CCEVS

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 the Hewlett-Packard Company Wireless LAN Controllers and Access Points Security Target and Final Evaluation Technical Report (ETR).*

3.1 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 ability to transmit generated audit records to an audit server in its operational environment.

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.

3.2 Cryptographic Support

The TOE includes NIST-validated cryptographic mechanisms that provide key management, random bit generation, encryption/decryption, digital signature, cryptographic hashing and keyed hash authentication capabilities 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.

3.3 User Data Protection

The TOE performs 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.

3.4 Identification and Authentication

The TOE requires users (i.e., administrators) to be successfully identified and authenticated before they can access any security management functions provided by the TOE. 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 IEEE 802.1X to support the authentication and authorization of wireless clients prior to establishing secure wireless sessions.

3.5 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 via a directly-connected console device and remotely via SSH. The GUI can be accessed remotely via 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.

3.6 Protection of the TSF

The TOE 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.

The TOE implements cryptographic protocols 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.

3.7 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.

3.8 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.

3.9 Trusted Path/Channels

The TOE protects interactive communication with administrators using SSHv2 for CLI access or HTTPS for Web GUI access. In each case, the cryptographic protocols protect confidentiality and integrity of communicated data. 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.

4 Assumptions and Clarification of Scope

4.1 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.

4.2 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:

- 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).
- This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process.
- The evaluation of security functionality of the product was limited to the functionality specified in *Hewlett-Packard Company Wireless LAN Access Controllers and Access Points Security Target*, Version 1.0, 31 October 2014. Any additional security related functional capabilities of the product were not covered by this evaluation.
- 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.
- The TOE appliances consist of software and hardware and do not rely on the operational environment for any supporting security functionality.
- The evaluated version of Comware is 5.2.109. Although Comware runs on a variety of underlying architectures, including VxWorks, Linux, pSOS and Windows, the only underlying architecture covered by this evaluation is Linux.
- Although the TOE supports both IPv4 and IPv6, support for IPv6 was not specifically covered by the evaluation.
- Although the TOE implements DSA and ECDSA asymmetric cryptographic algorithms, the use of these algorithms is not specified in any of the security functional requirements and they are not covered within the scope of the evaluation.

- The TOE must be installed, configured and managed as described in the following guidance documents included in the evaluated configuration:
    - *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

5 Architectural Information

The TOE is the Hewlett-Packard Company Wireless LAN Controllers and Access Points with Comware version 5.2.109.

The TOE includes Access Controllers and Access Points from the Hewlett-Packard family of Wireless Local Area Network (WLAN) products, all running Comware V5.2.109. The WLAN products in the evaluated configuration comprise the following:

- Access Controllers
    - HP 10500/7500 20G Unified Wired-WLAN Module
    - HP 830 8-Port PoE+ Unified Wired-WLAN Switch
    - HP 830 24-Port PoE+ Unified Wired-WLAN Switch
    - HP 850 Unified Wired-WLAN Appliance
    - HP 870 Unified Wired-WLAN Appliance
- Access Points
    - HP MSM430 Dual Radio 802.11n Access Point (Models AM, WW, JP, IL, TAA)
    - HP MSM460 Dual Radio 802.11n Access Point (Models AM, WW, JP, IL, TAA)
    - HP MSM466 Dual Radio 802.11n Access Point (Models AM, WW, JP, IL, TAA)
    - HP MSM466-R Dual Radio Outdoor 802.11n Access Point (Models AM, WW, JP, IL)
    - HP 560 Wireless Dual Radio 802.11n Access Point (Models AM, WW, JP, IL).

Note: The Access Point (AP) model designations in the preceding list identify different regulatory domain variants. The model designation is determined by the setting of a bit during the manufacturing process—it is not customer configurable. This bit identifies which regulatory domain the AP should operate in and restricts the available frequency of operation for the AP radios. The designations are defined as follows:

- AM—Americas
- WW—World Wide
- JP—Japan
- IL—Israel
- TAA—US Trade Agreements Act.

There are two types of Access Controller in the TOE: switch module, which operates within a switch chassis; and unified appliances, which integrate switch and access controller into a single appliance.

The APs in the TOE are IEEE 802.11a/b/g/n wireless devices that provide wireless coverage in both managed mode (i.e., managed through an Access Controller) and autonomous mode (i.e., without a controller). Only managed mode is supported in the evaluated configuration.

The HP Wireless LAN appliances consist of hardware and software components. While the physical form factor of each distinct series in the TOE is substantially different, 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 IEEE 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 Switch Module

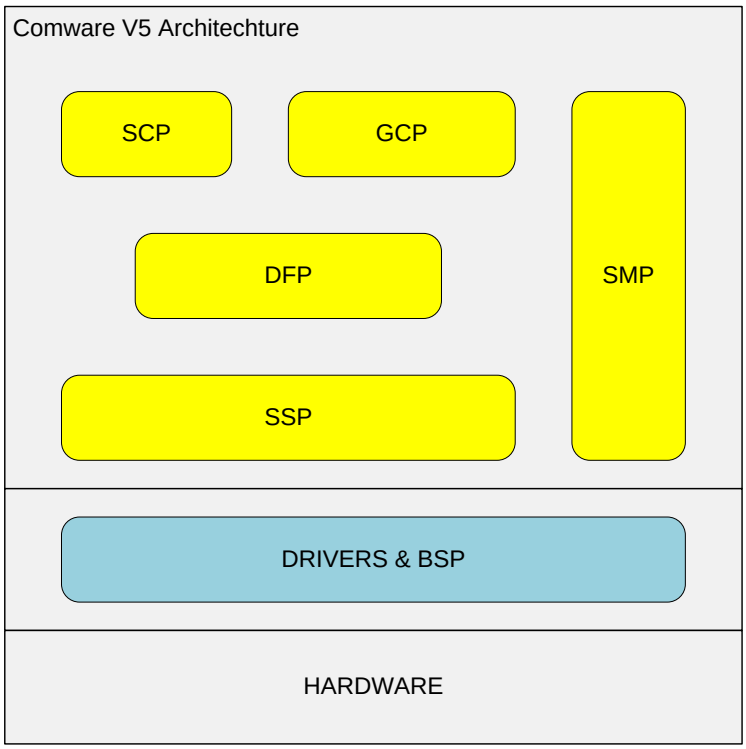
The HP 850 and 870 Unified Wired-WLAN Appliances are next generation 40G products. By employing new multi-core Network Processors, switch ASICs and FPGAs, they have large capacity, high reliability and offer wired and wireless data processing capacity. Both appliances provide user control and management, 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.

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. The following figure provides a visual depiction of the Comware 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 Interface (CLI) and Graphical User Interface (GUI) management options.
- ***System Service Plane (SSP)***—the SSP provides a foundation layer that implements primitives on which the other planes rely, e.g., 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).

The TOE includes NIST-validated cryptographic mechanisms that support SSHv2 and HTTPS (HTTP over TLSv1.0) and digital signatures used to protect the available remote management and to enable secure update capabilities of the TOE.

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

6 Documentation

HP offers a number of guidance documents that provide information and guidance for the deployment of Hewlett-Packard Switches. The following documents were specifically examined in the context of the evaluation:

- *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
- *HP Unified Wired-WLAN Products ACL and QoS Configuration Guide*, Document version: 6W102-20140818
- *HP Unified Wired-WLAN Products ACL and QoS Command Reference*, Document version: 6W102-20140818
- *HP Unified Wired-WLAN Products Network Management and Monitoring Configuration Guide*, Document version: 6W102-20140818
- *HP Unified Wired-WLAN Products Network Management and Monitoring Command Reference*, Document version: 6W102-20140818
- *HP Unified Wired-WLAN Products Security Configuration Guide*, Document version: 6W102-20140818
- *HP Unified Wired-WLAN Products Security Command Reference*, Document version: 6W102-20140818
- *HP Unified Wired-WLAN Products Fundamentals Configuration Guide*, Document version: 6W102-20140818
- *HP Unified Wired-WLAN Products Fundamentals Command Reference*, Document version: 6W102-20140818
- *HP Unified Wired-WLAN Products WLAN Configuration Guide*, Document version: 6W102-20140818

- *HP Unified Wired-WLAN Products Web-Based Configuration Guide*, Document version: 6W102-20140818

The complete set of configuration guides and command references for all aspects of the TOE are available on-line via this URL:

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

7 IT Product Testing

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

- Hewlett-Packard Company Wireless LAN Access Controllers and Access Points Test Report (10500/7500 Series), Version 1.0, 3 December 2014
- Hewlett-Packard Company Wireless LAN Access Controllers and Access Points Test Report (800 Series), Version 1.0, 3 December 2014.

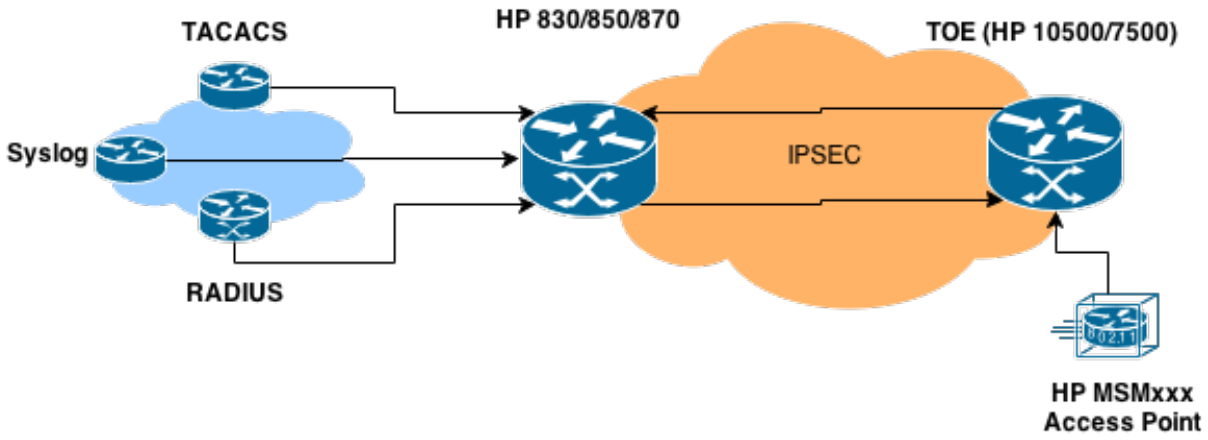
7.1 Developer Testing

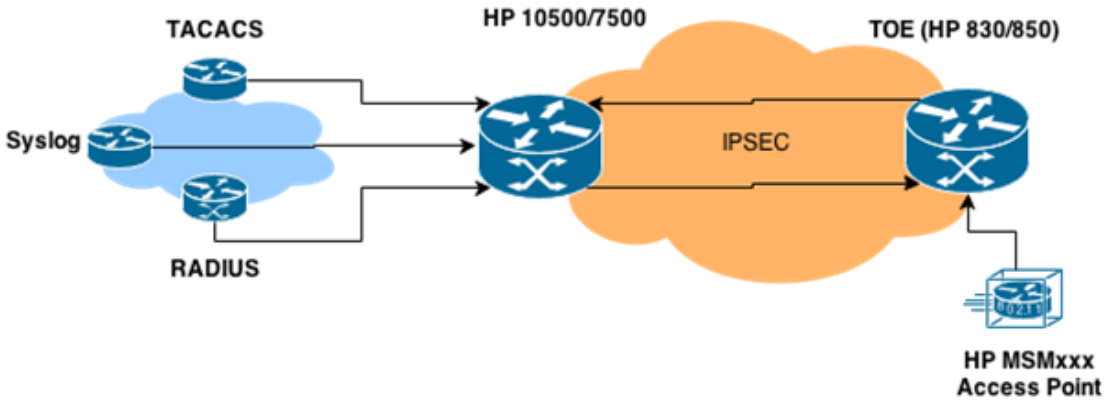
The assurance activities in *Protection Profile for Wireless Local Area Network (WLAN) Access Systems* do not specify any requirement for developer testing of the TOE.

7.2 Evaluation Team Independent Testing

The evaluation team devised a test plan based on the Test Assurance Activities specified in *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 team test report identified above.

The evaluation team created two test configurations in order to provide appropriate coverage of all devices included in the scope of evaluation. One configuration covered the 10500/7500 20G Unified Wired-WLAN Module, while the other configuration covered the 830/850/870 Unified Wired-WLAN Appliances. The following figures depict the two test configurations created by the evaluation team.





The test environments included:

- TOE components, running Comware v5.2.109:
  - HP 10500/7500 20G Unified Wired-WLAN Module
  - HP 830/850/870 Unified Wired-WLAN Appliances (sampled across all tests)
  - HP MSM430 Access Point
- Operational environment components:
  - Wireless client running Windows 8
  - HP 10500 IPsec peer
  - TACACS authentication server (TACACS.NET v 1.2.2.0)
  - RADIUS authentication server (FreeRadius v 2.2.0)
  - Syslog server (3CDaemon v 2.0 Revision 10)
- Test tools:
  - Putty (remote access client)
  - Wireshark (network packet capture tool)
  - Openssh (command line SSH tool).

The configurations used during testing of the TOE match the configurations specified in the ST.

A portion of evaluation team testing occurred at the vendor facility in Boston, MA. The remainder of the testing took place at the Leidos CCTL facility in Columbia, MD. Testing took place during September and October 2014.

The vendor provided the TOE platforms as described above. The evaluation team followed the installation and configuration procedures documented in the product guidance to install the TOE in the test environment.

Subsequently, the evaluators exercised all the test cases. The tests were selected in order to ensure that each of the test assertions specified in *Protection Profile for Wireless Local Area Network (WLAN) Access Systems* were covered. All tests passed. A summary of the testing performed by the evaluation

team is provided in *Assurance Activities Report for Hewlett-Packard Company Wireless LAN Access Controllers and Access Points*.

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 obvious vulnerabilities applicable to the TOE in its evaluated configuration.

8 Evaluated Configuration

The TOE is Hewlett-Packard Company Wireless LAN Controllers and Access Points with Comware version 5.2.109, which is installed and configured according to the product installation guidance identified in Section 6. The TOE appliances are configured to operate in FIPS mode.

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*, v1.0, 1 December 2011, in conjunction with Version 3.1, Revision 3 of the CC and 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 PP, and correctly verified that the product meets the claims in the ST.

The details of the evaluation are recorded in the Final ETR, which is controlled by the Leidos CCTL. The security assurance requirements are listed in the following table.

Table 2: Evaluated 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

Administrators are cautioned to pay particular attention to the Common Criteria preparative procedures when configuring the devices. Administrators should plan for the fact that log records are not buffered for transmission to the syslog server. Therefore, if the connection to the syslog server goes down, generated log records are not queued and will not be transmitted to the syslog server when the connection is re-established. The document, *Preparative Procedures for CC WLASPP Evaluated Wireless LAN Controllers and Access Points*, Revision 1.06, 11 December 2014, provides several configuration options that help reduce the risk that audit records will be lost.

Note that although the product supports DSA and ECDSA algorithms, those are not part of the evaluated configuration. As well, the devices provide additional security functionality, such functionality has not been evaluated and no claims can be made as to their effectiveness; only the security functional requirement claims made in the security target were evaluated.

11 Annexes

Not applicable.

12 Security Target

The ST for this product's evaluation is Hewlett-Packard Company WLAN Access Controllers and Access Points Security Target, Version 1.0, 31 October 2014.

13 Abbreviations and Acronyms

AAA	Authentication, Authorization, and Accounting
AAR	Assurance Activities Report
AP	Access Point
CC	Common Criteria for Information Technology Security Evaluation
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology for Information Technology Security
CLI	Command Line Interface
CM	Configuration Management
DSA	Digital Signature Algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standard
GUI	Graphical User Interface
IP	Internet Protocol—communications protocol for relaying datagrams across network boundaries
IPsec	Internet Protocol Security—a protocol suite for securing IP communications
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NTP	Network Time Protocol—a means of synchronizing clocks over a computer network
NVLAP	National Voluntary Laboratory Assessment Program
PCL	Product Compliant List
PoE+	Power over Ethernet
PP	Protection Profile
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RF	Radio Frequency
SSH	Secure Shell—a network protocol for secure data communication and remote command execution
ST	Security Target
TACACS+	Terminal Access Controller Access-Control System +
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
URL	Uniform Resource Locator—typically a web address
VR	Validation Report
WLAN	Wireless Local Area Network
WPA2	Wi-Fi Protected Access II

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009. Part 1: Introduction and general model. CCMB-2009-07-001.

[2] Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009. Part 2: Security functional components. CCMB-2009-07-002.

[3] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009. Part 3: Security assurance components. CCMB-2009-07-003.

[4] Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009. Evaluation methodology. CCMB-2009-07-004.

[5] Protection Profile for Wireless Local Area Network (WLAN) Access Systems, v1.0, 1 December 2011.

[6] Hewlett-Packard Company WLAN Access Controllers and Access Points Security Target, Version 1.0, 31 October 2014.

[7] Common Criteria Evaluation and Validation Scheme - Guidance to CCEVS Approved Common Criteria Testing Laboratories, Version 2.0, 8 Sep 2008.

[8] Evaluation Technical Report for Hewlett-Packard Company WLAN Controllers and Access Points, Parts 1 and 2 (and associated AAR and Test Report), Version 1.0, 3 December 2014.