National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report

Aruba, a Hewlett Packard Enterprise Company 4100i, 6200, 6300, 6400, 8320, 8325, 8360, 8400, 9300, and 10000 Switch Series Version 10.11

Report Number:	**CCEVS-VR-VID11391-2023**
Dated:	**December 5, 2023**
Version:	**1.0**

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

Department of Defense
ATTN: NIAP, Suite 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Jenn Dotson
Randy Heimann
Lisa Mitchell
Linda Morrison
Lori Sarem
The MITRE Corporation

Common Criteria Testing Laboratory

Cody Cummins
Cornelius Haley
Will Micknick
Dip Pudasaini
Matai Spivey
Gossamer Security Solutions, Inc.
Columbia, MD

Table of Contents

1 Executive Summary

This report documents the assessment by the National Information Assurance Partnership (NIAP) validation team of the evaluation of Aruba, a Hewlett Packard Enterprise Company 4100i, 6200, 6300, 6400, 8320, 8325, 8360, 8400, 9300, and 10000 Switch Series Version 10.11 solution provided by Aruba. It presents the evaluation results, their justifications, and the conformance results. This Validation Report (VR) is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Columbia, MD, United States of America, and was completed in December 2023. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements of the collaborative Protection Profile for Network Devices, version 2.2e, 23 March 2020.

The TOE is the Aruba, a Hewlett Packard Enterprise Company 4100i, 6200, 6300, 6400, 8320, 8325, 8360, 8400, 9300, and 10000 Switch Series Version 10.11. The TOE identified in this VR has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5). This VR applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

The Validation team monitored the activities of the Evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The Validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). 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 ETR are consistent with the evidence produced.

The technical information included in this report was obtained from the *Aruba, a Hewlett Packard Enterprise Company 4100i, 6200, 6300, 6400, 8320, 8325, 8360, 8400, 9300, and 10000 Switch Series Version 10.11 Security Target*, Version 0.7, December 4, 2023 and analysis performed by the Validation Team.

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, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) 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 information technology 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 Validated Products List.

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

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

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Aruba, a Hewlett Packard Enterprise Company 4100i, 6200, 6300, 6400, 8320, 8325, 8360, 8400, 9300, and 10000 Switch Series Version 10.11
Protection Profile	collaborative Protection Profile for Network Devices, version 2.2e, 23 March 2020
ST	*Aruba, a Hewlett Packard Enterprise Company 4100i, 6200, 6300, 6400, 8320, 8325, 8360, 8400, 9300, and 10000 Switch Series Version 10.11 Security Target*, Version 0.7, December 4, 2023
Evaluation Technical Report	*Evaluation Technical Report for Aruba, a Hewlett Packard Enterprise Company 4100i, 6200, 6300, 6400, 8320, 8325, 8360, 8400, 9300, and 10000 Switch Series Version 10.11*, version 0.3, December 4, 2023
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 5
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Aruba, a Hewlett Packard Enterprise Company
Developer	Aruba, a Hewlett Packard Enterprise Company
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Columbia, MD
CCEVS Validators	Jenn Dotson, Randy Heimann, Lisa Mitchell, Linda Morrison, Lori Sarem

3 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

The Target of Evaluation (TOE) is Aruba, a Hewlett Packard Enterprise Company 4100i, 6200, 6300, 6400, 8320, 8325, 8360, 8400, 9300, and 10000 Switch Series running Aruba OS-CX version 10.11.

The TOE offers comprehensive Layer 2 and Layer 3 features. The Aruba, a Hewlett Packard Enterprise Company, 4100i, 6200, 6300, 6400, 8320, 8325, 8360, 8400, 9300, and 10000 Switch Series provides security, scalability, and ease of use for enterprise edge deployments.

3.1 TOE Description

The TOE is a family of switches designed to support scalability, security and high performance for campus networks.

For the purpose of evaluation, the TOE will be treated as a network device offering CAVP tested cryptographic functions, security auditing, secure administration, trusted updates, self-tests, and secure connections to other servers (e.g., to transmit audit records). The scope of the evaluation is limited to the NDcPP22e requirements. Functions outside the scope of the NDcPP22e were not evaluated such as MACsec.

3.2 TOE Evaluated Configuration

The evaluated configuration includes the following devices:

Model	Processor ID	Microarchitecture
Aruba 4100i	ARM Cortex-A9	ARM Cortex-A9
Aruba 6200F	NXP 1046A	ARM Cortex A72
Aruba 6300M	NXP 1046A	ARM Cortex A72
Aruba 6300F		
Aruba 6405		
Aruba 6410		
Aruba 8360	NXP 1046A	ARM Cortex A72
Aruba 8320	Intel Atom C2538	Rangeley
Aruba 8325	Intel Xeon D-1518	Broadwell
Aruba 8400	Intel Xeon D-1527	Broadwell
Aruba 9300	Intel Xeon D-1537	Broadwell
Aruba 10000	Intel Xeon D-1637	Hewitt Lake

3.3 TOE Architecture

The underlying architecture of each TOE appliance consists of hardware that supports physical network connections, memory, processor, and software that implements switching functions, configuration information and drivers. While hardware varies between different appliance models, the software code is shared across all platforms. The software code enforces the security functions claimed in the Security Target.

3.4 Physical Boundaries

Each TOE appliance runs the 10.11 version of the ArubaOS-CX software and has physical network connections to its environment to facilitate the switching of network traffic. The TOE appliance can also be the destination of network traffic, where it provides interfaces for its own management.

The TOE may be accessed and managed through a PC or terminal in the environment which can be remote from or directly connected to the TOE.

4 Security Policy

This section summaries the security functionality of the TOE:

1. Security audit
2. Cryptographic support
3. Identification and authentication
4. Security management
5. Protection of the TSF
6. TOE access
7. Trusted path/channels

4.1 Security audit

The TOE is able to generate logs for a wide range of security relevant events. The TOE can be configured to store the logs locally so they can be accessed by an administrator and also to send the logs to a designated log server using TLS to protect the logs while in transit on the network.

4.2 Cryptographic support

The TOE provides CAVP certified cryptography in support of its SSHv2 and TLS v1.2 protocol implementations. Cryptographic services include key management, random bit generation, encryption/decryption, digital signature and secure hashing.

4.3 Identification and authentication

The TOE requires users to be identified and authenticated before they can use functions mediated by the TOE, with the exception of passing network traffic in accordance with its configured switching rules and reading the login banner. It provides the ability to both assign attributes (user names, passwords and roles) and to authenticate users against these attributes.

4.4 Security management

The TOE provides Command Line Interface (CLI) commands over SSH and an HTTP over TLS (HTTPS) Graphical User Interface (GUI) to access the wide range of security management functions to manage its security policies. The TOE also offers HTTP over TLS protection for RESTAPI interfaces that can be used for administration. All administrative activity and functions including security management commands are limited to authorized users (i.e., administrators) only after they have provided acceptable user identification and authentication data to the TOE. The security management functions are controlled through the use of roles that can be assigned to TOE users. The TOE supports the following roles: Administrators, Operators. The Administrator role can make changes to the TOE configuration while the Operator role is a read-only role.

4.5 Protection of the TSF

The TOE implements a number of measures to protect the integrity of its security features. The TOE protects stored passwords and cryptographic keys, so they are not directly accessible in plaintext. The TOE also ensures that reliable time information is available for both log accountability and synchronization with the operating environment by providing a hardware clock. The TOE employs both dedicated communication channels as well as cryptographic means to protect communication between itself and other components in the operating environment. The TOE performs self-tests to detect failure and protect itself from malicious updates.

4.6 TOE access

The TOE can be configured to display a logon banner before and after (a post-login banner) a user session is established. The TOE also enforces inactivity timeouts for local and remote sessions.

4.7 Trusted path/channels

The TOE protects communication channels between itself and remote administrators using HTTPS/TLS and SSH. The SSH protocol is used to protect administrative connections utilizing the TOE’s command line interface (CLI). Additionally, web-based GUI and RESTAPI programmatic interfaces are available for remote administration which are protected using HTTP over TLS (HTTPS/TLS).

The TOE protects communication with network peers, such as a log server, using TLS connections to prevent unintended disclosure or modification of logs.

5 Assumptions & Clarification of Scope

5.1 Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- collaborative Protection Profile for Network Devices, version 2.2e, 23 March 2020

That information has not been reproduced here and the NDcPP22e should be consulted if there is interest in that material.

5.2 Clarification of scope

The scope of this evaluation was limited to the functionality and assurances covered in the NDcPP22e as described for this TOE in the ST. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. 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 in accordance with the evaluation activities specified in the NDcPP22e and performed by the Evaluation team.
- This evaluation covers only the specific device models and software as identified in this document and referenced in the ST, and not any earlier or later versions released or in process.
- Apart from the Admin Guide, additional customer documentation for the specific network device models was not included in the scope of the evaluation and therefore should not to be relied upon when configuring or operating the device as evaluated.
- 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 functionality evaluated is scoped exclusively to the security functional requirements specified in the NDcPP22e and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

6 Documentation

The following documents were available with the TOE for evaluation:

- *Common Criteria Administrator Guidance Target of Evaluation: Aruba 4100, 6000, 8000, 9000, and 10000 Switch Series*, Version 2.4, November 28, 2023

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated.

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation team. It is derived from information contained in the proprietary *Detailed Test Report for Aruba, a Hewlett Packard Enterprise Company 4100i, 6200, 6300, 6400, 8320, 8325, 8360, 8400, 9300, and 10000 Switch Series Version 10.11*, Version 0.3, December 4, 2023 (DTR), as summarized in the evaluation Assurance Activity Report (AAR).

7.1 Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

7.2 Evaluation Team Independent Testing

The Evaluation team verified the product according to a Common Criteria Certification document and ran the tests specified in the NDcPP22e including the tests associated with optional requirements. The *Assurance Activity Report for Aruba, a Hewlett Packard Enterprise Company 4100i, 6200, 6300, 6400, 8320, 8325, 8360, 8400, 9300, and 10000 Switch Series Version 10.11*, Version 0.3, December 4, 2023 (AAR) in section 1.1, combined with the DTR provides the tested devices, provides a list of test tools, and has diagrams of the test environment.

8 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all assurance activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 5 and CEM version 3.1 rev 5. The evaluation determined the Aruba, a Hewlett Packard Enterprise Company 4100i, 6200, 6300, 6400, 8320, 8325, 8360, 8400, 9300, and 10000 Switch Series Version 10.11 TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP22e (Part 3 conformant. The Validation team reviewed all the work of the Evaluation team and agreed with their practices and findings.

8.1 Evaluation of the Security Target (ASE)

The Evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Aruba, a Hewlett Packard Enterprise Company 4100i, 6200, 6300, 6400, 8320, 8325, 8360, 8400, 9300, and 10000 Switch Series Version 10.11 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

8.2 Evaluation of the Development (ADV)

The Evaluation team applied each ADV CEM work unit. The Evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the ST and Guidance documents. Additionally the evaluator performed the assurance activities specified in the NDcPP22e related to the examination of the information contained in the TSS.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

8.3 Evaluation of the Guidance Documents (AGD)

The Evaluation team applied each AGD CEM work unit. The Evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the Evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

8.4 Evaluation of the Life Cycle Support Activities (ALC)

The Evaluation team applied each ALC CEM work unit. The Evaluation team found that the TOE was appropriately labeled with a unique identifier consistent with the TOE identification in the evaluation evidence and that the TOE references used are consistent.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

8.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The Evaluation team applied each ATE CEM work unit. The Evaluation team ran the set of tests specified by the assurance activities in the NDcPP22e and recorded the results in a Test Report, summarized in the AAR.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

8.6 Vulnerability Assessment Activity (VAN)

The Evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the evaluator. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities conducted on November 29, 2023, did not uncover any residual vulnerability.

The evaluator searched the following:

- National Vulnerability Database (https://web.nvd.nist.gov/vuln/search)
- Vulnerability Notes Database (http://www.kb.cert.org/vuls/)
- Rapid7 Vulnerability Database (https://www.rapid7.com/db/vulnerabilities)
- Tipping Point Zero Day Initiative (http://www.zerodayinitiative.com/advisories)
- cve.org CVE Database (https://www.cve.org/),
- Tenable Network Security (http://nessus.org/plugins/index.php?view=search)

- Offensive Security Exploit Database (https://www.exploit-db.com/)

with the following search terms: “ArubaOS”, “AOS 10.11”, “TLS”, “SSH”, “Cortex A9”, “NPX 1046A”, “Xeon D-1518”, “Xeon D-1527“,“Xeon D-1537“, “Xeon D-1637”, “Atom Atom C2538”, “AOS-CX”, “AOS-CX RSA Engine”, “AOS-CX Crypto”, “AES ECB”

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

8.7 Summary of Evaluation Results

The Evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's test activities also demonstrated the accuracy of the claims in the ST.

The Validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the Evaluation team followed the procedures defined in the CEM and performed the Evaluation Activities in CPP_ND_V2.2-SD, and correctly verified that the product meets the claims in the ST.

9 Validator Comments/Recommendations

The Validation team suggests that the consumer pay particular attention to the evaluated configuration of the TOE. As stated in the Clarification of Scope, the evaluated functionality is scoped exclusively to the security functional requirements specified in the ST, and the only evaluated functionality was that which was described by the SFRs claimed in the ST. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about its effectiveness.

The Validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the Guidance provided in Section 6. As noted in Section 6, consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated. No versions of the TOE and software, either earlier or later, were evaluated.

Any additional customer documentation, not listed in Section 6, provided with the product, or that which may be available online, was not included in the scope of the evaluation and therefore, should not be relied upon to configure or operate the TOE as evaluated.

10 Annexes

Not applicable

11 Security Target

The Security Target is identified as: *Aruba, a Hewlett Packard Enterprise Company 4100i, 6200, 6300, 6400, 8320, 8325, 8360, 8400, 9300, and 10000 Switch Series Version 10.11 Security Target, Version 0.7, December 4, 2023*.

12 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

13 **Bibliography**

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

[1] Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.

[4] collaborative Protection Profile for Network Devices, version 2.2e, 23 March 2020.

[5] *Aruba, a Hewlett Packard Enterprise Company 4100i, 6200, 6300, 6400, 8320, 8325, 8360, 8400, 9300, and 10000 Switch Series Version 10.11 Security Target*, Version 0.7, December 4, 2023 (ST).

[6] *Assurance Activity Report for Aruba, a Hewlett Packard Enterprise Company 4100i, 6200, 6300, 6400, 8320, 8325, 8360, 8400, 9300, and 10000 Switch Series Version 10.11*, Version 0.3, December 4, 2023 (AAR).

[7] *Detailed Test Report for Aruba, a Hewlett Packard Enterprise Company 4100i, 6200, 6300, 6400, 8320, 8325, 8360, 8400, 9300, and 10000 Switch Series Version 10.11*, Version 0.3, December 4, 2023 (DTR).

[8] *Evaluation Technical Report for Aruba, a Hewlett Packard Enterprise Company 4100i, 6200, 6300, 6400, 8320, 8325, 8360, 8400, 9300, and 10000 Switch Series Version 10.11*, Version 0.3, December 4, 2023 (ETR)