National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

TM

Validation Report
for the
Aruba Mobility Conductor with ArubaOS 8.10

Report Number: CCEVS-VR-VID11345-2023
Dated: June 23, 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

Chris Thorpe

The MITRE Corporation

Common Criteria Testing Laboratory

Sean Bennett

Eric Isaac

Greg McLearn

Wasif Sikder

Kevin Steiner

Lightship Security USA, Inc.

Table of Contents

List of Tables

1. Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) Validation team of the evaluation of Aruba Mobility Conductor with ArubaOS 8.10 provided by Aruba, A Hewlett Packard Enterprise Company. 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 Lightship Security USA Common Criteria Laboratory (CCTL) in Baltimore, MD, United States of America, and was completed in June 2023. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Lightship Security (LS). 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 Mobility Conductor with ArubaOS 8.10. The TOE identified in this VR has been evaluated at a NIAP approved CCTL 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 Mobility Conductor with ArubaOS 8.10 Security Target,* Version 1.2, June 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 Mobility Conductor with ArubaOS 8.10
Sponsor and Developer	Aruba, A Hewlett Packard Enterprise Company 6280 America Center Dr. San Jose, CA 95002
CCTL	Lightship Security USA, Inc. 3600 O'Donnell St., Suite 2 Baltimore, MD 21224
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.
CEM	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, Version 3.1, Revision 5, April 2017.

Item	Identifier
Protection Profile	collaborative Protection Profile for Network Devices, v2.2e, 23 March 2020
ST	*Aruba Mobility Conductor with ArubaOS 8.10 Security Target*, Version 1.2, June 2023
Evaluation Technical Report	*Aruba Mobility Conductor with ArubaOS 8.10 Evaluation Technical Report*, Version 0.7, June 2023
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Evaluation Personnel	Sean Bennett, Eric Isaac, Greg McLearn, Wasif Sikder, Kevin Steiner
CCEVS Validators	Jenn Dotson, Randy Heimann, Lisa Mitchell, Linda Morrison, Lori Sarem, Chris Thorpe

3. Architectural Information

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

The Target of Evaluation (TOE) is the Aruba Mobility Conductor with ArubaOS 8.10. The Aruba Mobility Conductor simplifies the management of multiple Aruba controllers running ArubaOS 8 or later. Key features include a centralized dashboard to easily see and manage controllers deployed in multiple sites, a hierarchical configuration tool to pre-stage network deployments, and the ability to perform live firmware and feature upgrades during active user sessions. The addition of licensing pools simplifies the transfer of licenses between different controllers to quickly address expanded deployment needs.

3.1. TOE Evaluated Configuration

The TOE is a network device that provides centralized management of multiple Aruba Mobility Controllers.

The TOE interfaces are as follows:

a) **CLI.** Administrative CLI via direct serial connection or SSH.

b) **GUI.** Administrative web GUI via HTTPS/TLS.

c) **RADIUS/TACACS+.** Authentication with a remote server via IPsec.

d) **Logs.** Logs are sent to an external syslog server via IPsec.

e) **NTP.** Time synchronization with an NTP server via IPsec.

f) **Mobility Controller.** Management of Aruba Mobility Controllers via IPsec.

3.2. Physical Boundary

The physical boundary of the TOE includes the appliance models shown in Table 2 executing ArubaOS 8.10 software.

Table 2: TOE models

Model	CPU	Software	Notes on Differences
MCR-HW-1K-F1	Intel Xeon E5-2609v4 (Broadwell)	ArubaOS 8.10	Difference in the number of managed nodes/ supported devices, clients, and controllers due to the licenses applied.
MCR-HW-5K-F1	Intel Xeon E5-2620v4 (Broadwell)		
MCR-HW-10K-F1	Intel Xeon E5-2650v4 (Broadwell)		

3.3. Required Non-TOE Hardware, Software, and Firmware

The TOE operates with the following components in the environment:

a) **Audit Server.** The TOE is capable of sending audit events to a Syslog server.

b) **NTP Server.** The TOE synchronizes time with an NTP server.

c) **Authentication Server.** The TOE can utilize RADIUS and TACACs+ servers to authenticate users.
d) **Mobility Controllers.** The TOE manages Aruba controllers running ArubaOS 8 or later. Note: The TOE security functions are not reliant on the presence of Mobility Controllers.

4. Security Policy

This section summarizes the security functionality of the TOE:

4.1. Security Audit

The TOE generates logs of security relevant events. The TOE stores logs locally and is capable of sending log events to a remote syslog server. Log events are sent in real-time via IPsec.

4.2. Cryptographic Support

The TOE implements a cryptographic module. In the evaluated configuration, the TOE is in FIPS mode to support the cryptographic functionality. The TOE implements cryptographic protocols such as SSH, TLS, HTTPS, and IPsec.

4.3. Identification and Authentication

The TOE requires users who connect to the TOEs administrator interfaces (direct serial connection, remote CLI, and GUI) to authenticate prior to being granted access to any TOE functionality. The TOE supports the use of authentication servers via IPsec.

4.4. Secure Management

The TOE enables secure management of its security functions, including:

Local and remote administration
Access banners
Session inactivity and termination
TOE updates
Management of critical security functions and data
Protection of cryptographic keys and passwords

4.5. Protection of TSF

The TOE prevents reading of private keys and plaintext passwords by any user. The TOE synchronizes with an external time source. This date and time are used as a timestamp that is part of each audit record generated by the TOE. The TOE ensures the authenticity and integrity of software updates through digital signatures. The TOE performs a suite of self-tests to ensure the correct operation and enforcement of its security functions.

4.6. TOE Access

The TOE can terminate inactive sessions after configurable period. The TOE can also display specified banner on the local and remote CLI interfaces prior to allowing any administrative access to the TOE. The TOE allows users to manually terminate an established management session with the TOE.

4.7. Trusted Path/Channels

The TOE protects the integrity and confidentiality of communications via the following TOE interfaces: CLI via SSH; Administrative web GUI via HTTPS/TLS; authentication with a remote server via IPsec; external syslog server via IPsec; NTP server via IPsec; and management of Aruba Mobility Controllers via IPsec.

5. Assumptions and 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*, v2.2e, 23 March 2020 (CPP_ND_V2.2E)

That information has not been reproduced here and the CPP_ND_V2.2E 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 CPP_ND_V2.2E 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 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 in accordance with the evaluation activities specified in CPP_ND_V2.2-SD and performed by the Evaluation team
- This evaluation only covers the software version and platform versions identified in this document and referenced in the *Aruba Mobility Conductor with ArubaOS 8.10 Security Target*, Version 1.2, June 2023, and not any earlier or later versions released or in process.
- Apart from the Admin Guides identified in Section 6, additional customer documentation for the specific software version and platform versions was not included in the scope of the evaluation and therefore should not 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 CPP_ND_V2.2E and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

6. Documentation

The following guidance documents are provided with the TOE upon delivery in accordance with the PP:

- *ArubaOS 8.10.0.0 User Guide,* Revision 02, 2022
- *ArubaOS 8.10 Getting Started Guide,* Revision 01, 2022
- *ArubaOS 8.x Command-Line Interface Reference Guide*, 2023
- *ArubaOS 8.10.0.0 Syslog Reference Guide,* Revision 01
- *Aruba OS 8.10 Supplemental Guidance (Common Criteria Configuration Guidance for Aruba Mobility Conductor with ArubaOS 8.10-FIPS),* Version 2.6, June 2023

To use the product in the evaluated configuration, the product must be installed and configured as specified in *ArubaOS 8.10 Supplemental Guidance (Common Criteria Configuration Guidance for Aruba Mobility Conductor with ArubaOS 8.10-FIPS).* This document provides references to other documentation for specific steps in to place the TOE into its the evaluated configuration and these documents are provided on the NIAP website.

7. IT Product Testing

This section describes the testing efforts of the Evaluation team. It is derived from information contained in *Aruba Mobility Conductor with ArubaOS 8.10 Assurance Activity Report (AAR),* Version 0.11, June 2023, and the proprietary *Aruba Mobility Conductor with ArubaOS 8.10 NDcPP 2.2E Test Plan,* Version 0.5, June 2023 *and Aruba Mobility Conductor with ArubaOS 8.10 NDcPP 2.2E Test Results,* Version 0.4, June 2023.

7.1. Developer Testing

No evidence of developer testing is required in the SARs or Evaluation Activities for this product.

7.2. Evaluation Team Independent Testing

The Evaluation team conducted independent testing at Lightship Security USA in Baltimore, MD from December 2023 until June 2023. The Evaluation team configured the TOE according to vendor installation instructions and as identified in the Security Target.

The Evaluation team confirmed the technical accuracy of the setup and installation guide during installation of the TOE. The Evaluation team confirmed that the TOE version delivered for testing was identical to the version identified in the ST.

The Evaluation team used the Protection Profile test procedures as a basis for creating each of the independent tests as required by the Evaluation Activities.

Each Evaluation Activity was tested as required by the conformant Protection Profile and the evaluation team verified that each test passed.

7.3. Test Configuration

The TOE testing environment components are identified in Figure 1 below.

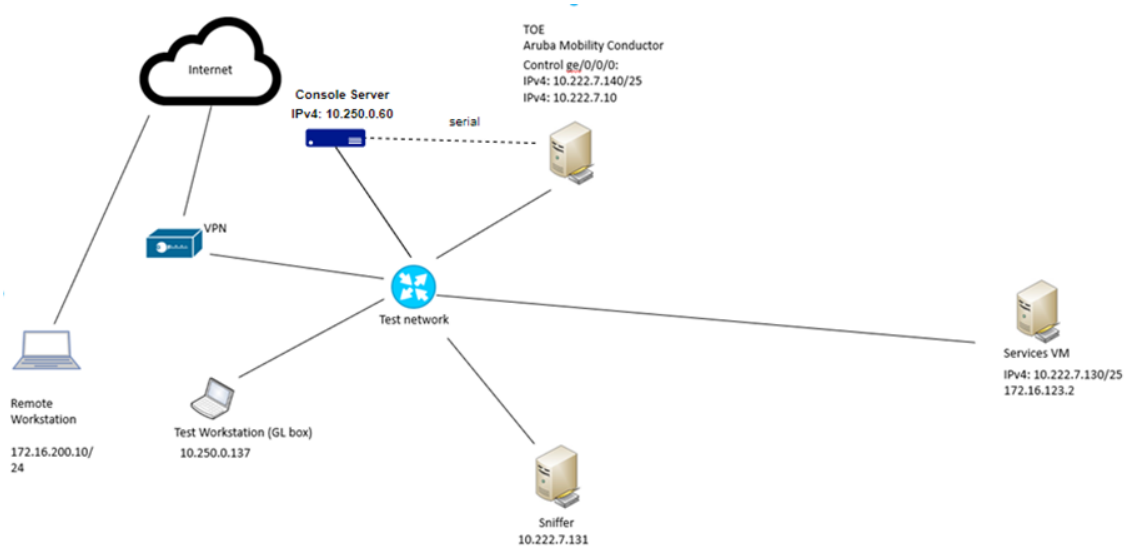

Figure 1: Testing Environment Overview

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 documents: *Aruba Mobility Conductor with ArubaOS 8.10 NDcPP 2.2E Test Plan*, Version 0.5, June 2023, *Aruba Mobility Conductor with ArubaOS 8.10 NDcPP 2.2E Test Results*, Version 0.4, June 2023, and *Aruba Mobility Conductor with ArubaOS 8.10 Evaluation Technical Report*, Version 0.7, June 2023. The reader of this document can assume that all 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 Revision 5 and CEM Version 3.1 Revision 5 and the specific evaluation activities specified in CPP_ND_V2.2-SD.

The Evaluation determined the TOE satisfies the conformance claims made in the *Aruba Mobility Conductor with ArubaOS 8.10 Security Target,* Version 1.2, June 2023 of Part 2 extended and 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 Security Target (ASE)

The Evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains an ST introduction, TOE overview, TOE description, description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Aruba Mobility Conductor with ArubaOS 8.10 that are consistent with the claimed Protection Profile, 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 Development Documentation (ADV)

The Evaluation team performed each ADV assurance activity and applied each ADV_FSP.1 CEM work unit. The Evaluation team assessed the evaluation evidence and found it adequate to meet the requirements specified in the claimed Protection Profile for design evidence. The design documentation consists of a functional specification contained in the ST and Guidance documents. Additionally, the evaluator performed the Evaluation Activities related to the examination of the information contained in the TSS.

The Validation 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 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 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 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 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 Test Evaluation Activities 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 *Aruba Mobility Conductor with ArubaOS 8.10 Vulnerability Assessment*, Version 0.4, June 2023, report prepared by the Evaluation team. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities conducted on June 16, 2023, did not uncover any residual vulnerability.

The Evaluation team searched:

- NIST National Vulnerabilities Database: https://web.nvd.nist.gov/view/vuln/search
- Common Vulnerabilities and Exposures:
  - http://cve.mitre.org/cve/
  - https://www.cvedetails.com/vulnerability-search.php
- US-CERT: http://www.kb.cert.org/vuls/html/search

- Tenable Network Security: https://www.tenable.com/cve
- Tipping Point Zero Day Initiative: http://www.zerodayinitiative.com/advisories
- Offensive Security Exploit Database: https://www.exploit-db.com/
- Rapid7 Vulnerability Database: https://www.rapid7.com/db/vulnerabilities

The Evaluation team performed a search using the following keywords:

- Aruba Mobility Conductor
- Aruba OpenSSL Module
- Aruba Crypto Module
- Aruba Bootloader Module
- ArubaOS 8.10
- MCR-HW-1K-F1
- MCR-HW-5K-F1
- MCR-HW-10K-F1
- MM-HW-1K-F1
- MM-HW-5K-F1
- MM-HW-10K-F1
- Intel Xeon E5-2609v4
- Intel Xeon E5-2620v4
- Intel Xeon E5-2650v4
- FreeRADIUS
- Ntp.org
- Mocana
- OpenSSH
- OpenSSL

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

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 *ArubaOS 8.10 Supplemental Guidance (Common Criteria Configuration Guidance for Aruba Mobility Conductor with ArubaOS 8.10-FIPS).* 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 ST for this product's evaluation is *Aruba Mobility Conductor with ArubaOS 8.10 Security Target,* Version 1.2, June 2023.

12. GLOSSARY

- **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.
- **Threat:** Means through which the ability or intent of a threat agent to adversely affect the primary functionality of the TOE, facility that contains the TOE, or malicious operation directed towards the TOE. A potential violation of security.
- **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.
- **Vulnerabilities:** A vulnerability is a hardware, firmware, or software flaw that leaves an Automated Information System (AIS) open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, which could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

13. Acronym List

CAVP	Cryptographic Algorithm Validation Program (CAVP)
CCEVS	Common Criteria Evaluation and Validation Scheme
CCIMB	Common Criteria Interpretations Management Board
CCTL	Common Criteria Testing Laboratories
CEM	Common Evaluation Methodology for IT Security Evaluation
LS	Lightship Security USA CCTL
DHCP	Dynamic Host Configuration Protocol
ETR	Evaluation Technical Report
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MFD	Multi-Function Device
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
OS	Operating System
OSP	Organizational Security Policies
PCL	Products Compliant List
ST	Security Target
TOE	Target of Evaluation
VR	Validation Report

14. Bibliography

1. *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2017-04-001*, Version 3.1 Revision 5, April 2017
2. *Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, CCMB-2017-04-002*, Version 3.1 Revision 5, April 2017
3. *Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, CCMB-2017-04-003*, Version 3.1 Revision 5, April 2017
4. *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2017-04-004*, Version 3.1, Revision 5, April 2017
5. *collaborative Protection Profile for Network Devices, v2.2E, 23-March-2020*
6. *Aruba Mobility Conductor with ArubaOS 8.10 Security Target*, Version 1.2, June 2023
7. *Aruba OS 8.10 Supplemental Guidance (Common Criteria Configuration Guidance for Aruba Mobility Conductor with ArubaOS 8.10-FIPS),* Version 2.6, June 2023
8. *ArubaOS 8.10.0.0 User Guide*, Revision 02, 2022
9. *ArubaOS 8.10 Getting Started Guide*, Revision 01, 2022
10. *ArubaOS 8.x Command-Line Interface Reference Guide, 2023*
11. *ArubaOS 8.10.0.0 Syslog Reference Guide, Revision 01*
12. *Aruba Mobility Conductor with ArubaOS 8.10 Evaluation Technical Report*, Version 0.7, June 2023
13. *Aruba Mobility Conductor with ArubaOS 8.10 Assurance Activity Report (AAR)*, Version 0.11, June 2023
14. *Aruba Mobility Conductor with ArubaOS 8.10 NDcPP 2.2E Test Plan*, Version 0.5, June 2023,
15. *Aruba Mobility Conductor with ArubaOS 8.10 NDcPP 2.2E Test Results,* Version 0.4, June 2023
16. *Aruba Mobility Conductor with ArubaOS 8.10 Vulnerability Assessment*, Version 0.4, June 2023