National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report
Aruba ClearPass Policy Manager 6.11

Report Number: CCEVS-VR-11324-2023
Dated: March 27, 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

Swapna Katikaneni
Jerome Myers
Mike Quintos
The Aerospace Corporation

Common Criteria Testing Laboratory

Cody Cummins
Matai Spivey
Gossamer Security Solutions, Inc.
Columbia, MD

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Aruba ClearPass Policy Manager 6.11 solution provided by Aruba, a Hewlett Packard Enterprise Company. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation 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 March 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 (NDcPP22e) with the Network Device Collaborative Protection Profile (NDcPP)/Application Software Protection Profile (App PP) Extended Package (EP) for Authentication Servers, Version 1.0, 07 August 2015 (AUTHSRVEP10).

The Target of Evaluation (TOE) is the Aruba ClearPass Policy Manager 6.11.

The Target of Evaluation (TOE) identified in this Validation Report 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 Validation Report 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 and the conclusions of the testing laboratory in the evaluation technical report 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 evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the Aruba ClearPass Policy Manager 6.11 Security Target, version 1.0, March 21, 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 Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (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 ClearPass Policy Manager 6.11 (Specific models identified in Section 8)
Protection Profile	collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 (NDcPP22e) with the Network Device Collaborative Protection Profile (NDcPP)/Application Software Protection Profile (App PP) Extended Package (EP) for Authentication Servers, Version 1.0, 07 August 2015 (AUTHSRVEP10)
ST	Aruba ClearPass Policy Manager 6.11 Security Target, version 1.0, March 21, 2023
Evaluation Technical Report	Evaluation Technical Report for Aruba ClearPass Policy Manager 6.11, version 1.0, March 21, 2023
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 5
Conformance Result	CC Part 2 extended, CC Part 3 extended
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	Jerome Myers, Swapna Katikaneni, Mike Quintos

3 Architectural Information

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

The Aruba ClearPass Policy Manager platform provides role- and device-based network access control for employees, contractors and guests across any wired, wireless and VPN infrastructure. ClearPass implements RADIUS services, as well as profiling, onboarding, guest access, and health checks facilitating centralized management of network access policies. The authentication services are the focus of this evaluation and other services are not evaluated.

ClearPass provides user and device authentication based on 802.1X, non-802.1X and web portal access methods. Multiple authentication protocols like PEAP, EAP-FAST, EAP-TLS, and EAP-TTLS can be used concurrently to strengthen security in any environment. Attributes from multiple identity stores such as Microsoft Active Directory, LDAP-compliant directory, ODBC-compliant SQL database, token servers and internal databases can be used within a single policy for fine-grained control.

For the purpose of evaluation, ClearPass will be treated as a network infrastructure authentication server device offering authentication services, CAVP tested cryptographic functions, security auditing, secure administration, trusted updates, self-tests, and secure connections to other servers (e.g., to transmit audit records).

3.1 TOE Evaluated Platforms

Detail regarding the evaluated configuration is provided in Section 8 below.

3.2 TOE Architecture

The ClearPass Policy Manager is available either as a hardware or virtual network appliance and is designed to support a wide range of network, wireless and security protocols to support a wide range of clients. However, the evaluation is limited to the hardware network appliances and the secure communication protocols specifically identified below.

There are seven TOE appliance models designed to support different numbers of client devices. Each platform differs in CPU performance (e.g., number of cores), available memory, disk performance and storage capacity, and power consumption/supply.

While ClearPass Policy Manager products can be configured as a collection of devices operating in a cluster sharing a common security policy, the TOE configuration subject to this evaluation is limited to a single ClearPass Policy Manager device.

Each ClearPass Policy Manager device is a rack-mountable appliance with Intel Atom or Xeon CPUs running a version of RHEL 8 to host the applications designed to provide the network access control capabilities summarized above. ClearPass includes a version of Hewlett Packard Enterprise OpenSSL Cryptographic Module on Red Hat Enterprise Linux

that is used to perform cryptographic functions. This module supports the implementations of IPsec using StrongSwan, TLS/HTTPS using Apache, RadSec using radsecproxy, and SSH using OpenSSH used to secure the communication channels (for remote administration, exporting audit events, syncing with an NTP server and communicating with NAS servers).

3.3 Physical Boundaries

The physical boundaries of the TOE consist of ClearPass Policy Manager device running software version 6.11.

4 Security Policy

This section summarizes the security functionality of the TOE:

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

4.1 Security audit

The TOE is designed to be 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 or alternately to send the logs to a designated syslog server.

4.2 Communication

The TOE implements the RADIUS protocol in order to service authentication requests from associated NAS devices. The TOE requires RADIUS encapsulated EAP Message Authenticators that conform to RFC 3579 and each Access-Request from a NAS must have the correct Message Authenticator so that the NAS can be determined to be authentic. In response, the TOE includes its own identifier, Response Authenticator (conforming to RFC 2865), and the response packet with the requested authentication results.

4.3 Cryptographic support

The TOE includes a version of Hewlett Packard Enterprise OpenSSL Cryptographic Module on Red Hat Enterprise Linux that provides key management, random bit generation, encryption/decryption, digital signature and secure hashing and key-hashing features in support of higher-level cryptographic protocols including IPsec, SSH, and TLS/HTTPS.

4.4 Identification and authentication

The TOE offers no TSF-mediated functions except display of a login banner until the administrator is identified and authenticated. The TOE authenticates administrative users accessing the TOE via the command-line interface (local serial console or SSH) or web interface (Web UI) in the same manner using its own password-based authentication mechanism. The TOE also supports public-key based authentication of users through the SSH-based CLI interface and supports certificate authentication for the Web UI.

The TOE supports certificate authentication for TLS and IPsec and supports pre-shared key authentication for RADIUS and IPsec connections. The TOE uses X.509v3 certificates and validates received authentication certificates. OCSP is supported for X509v3 certificate validation.

4.5 Security management

The TOE provides Command Line (CLI) commands (locally via a serial console or remotely via SSH) and a Web-based Graphical User Interface (Web GUI) to access the available functions to manage the TOE security functions. Security management commands are limited to authorized users (i.e., administrators) only after they have been correctly identified and authenticated. The security management functions are controlled through the use of Admin Privileges that can be assigned to TOE users.

4.6 Protection of the TSF

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

It protects particularly sensitive data such as stored passwords and private 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 audit records).

The TOE includes functions to perform self-tests so that it might detect when it is failing. It also includes 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.

4.7 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 the inactive session (local or remote) will be terminated. The TOE can also reject authentication requests based on time of day, account status, location and role mapping.

4.8 Trusted path/channels

The TOE protects interactive communication with administrators using a console and SSHv2 for CLI access and TLS/HTTPS for Web UI access. In each case, both the integrity and

disclosure protection is ensured via the secure protocol. If the negotiation of a secure session fails or if the user cannot be authenticated for remote administration, the attempted session will not be established.

The TOE protects communication with network peers, such as a syslog server or NTP server, using IPsec connections to prevent unintended disclosure or modification of logs. The TOE uses either RadSec or IPsec to communicate with associated NAS servers for RADIUS requests and responses.

5 Assumptions & Clarification of Scope

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 (NDcPP22e)
- Network Device Collaborative Protection Profile (NDcPP)/Application Software Protection Profile (App PP) Extended Package (EP) for Authentication Servers, Version 1.0, 07 August 2015 (AUTHSRVEP10)

That information has not been reproduced here and the NDcPP22e/AUTHSRVEP10 should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in the NDcPP22e/AUTHSRVEP10 as described for this TOE in the Security Target. 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.

Clarification of scope

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 with a certain level of assurance (the assurance activities specified in the collaborative Protection Profile for Network Devices with the Authentication Servers Extended Package and performed by the evaluation team).
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process. The evaluated configuration is limited to the platforms and devices identified in section 8.
- Apart from the Admin Guide, additional customer documentation for the specific Authentication Server models 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 NDcPP22e/AUTHSRVEP10 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 Configuration Guidance Aruba ClearPass Policy Manager, Version 6.11, March 2023

Any additional customer documentation provided with the product, or that is available online 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.

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 ClearPass Policy Manager 6.11, Version 1.0, March 21, 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/AUTHSRVEP10 including the tests associated with optional requirements. The AAR, in section 3.4.1 lists the tested devices, provides a list of test tools, and has diagrams of the test environment. Testing took place from July 2022 to March 2023 at Gossamer.

8 Evaluated Configuration

The evaluated configuration includes the devices listed in the table below and is dependent upon the TOE being configured per the Guidance Documentation identified in section 6. No other versions of the TOE, either earlier or later, were evaluated.

Appliance Model	CPU
C1000	Intel Atom C2758 (Rangeley)
C2000	Intel Xeon E3-1240 v5 (Skylake)
C2010	Intel Xeon E-2274G (Coffee Lake)
C2020	Intel Xeon E-2374G (Rocket Lake)
C3000 (legacy only)	Intel Xeon E5-2620 v3 (Haswell)
C3010	Intel Xeon Gold 5118 (Skylake)
C1000V	ESXi 7.0 on Intel Xeon E-2254ML (Coffee Lake)

TOE Models

9 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 ClearPass Policy Manager TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP22e/AUTHSRVEP10.

9.1 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 ClearPass Policy Manager 6.11 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator 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.

9.2 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 Security Target and Guidance documents. Additionally, the evaluator

performed the assurance activities specified in the NDcPP22e/AUTHSRVEP10 related to the examination of the information contained in the TSS.

The validator 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.

9.3 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 validator 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.

9.4 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 identified.

The validator 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.

9.5 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/AUTHSRVEP10 and recorded the results in a Test Report, summarized in the AAR.

The validator 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.

9.6 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 did not uncover any residual vulnerability.

The evaluator searched the 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), Exploit / Vulnerability Search Engine (http://www.exploitsearch.net), SecurITeam Exploit Search (http://www.securiteam.com), Tenable Network Security (http://nessus.org/plugins/index.php?view=search), Offensive Security Exploit Database (https://www.exploit-db.com/) on 3/21/2023 with the following search terms: "Aruba", "HPE Aruba", "Clearpass", "C1000", "C2000", "C2010", "C2020", "C3000", "C3010", "C1000V", "Atom C2758", "Xeon E3-1240", "Xeon E-2274G", "Xeon E5-2620", "Xeon Gold 5118", "ESXi 7.0", "Xeon E-2254ML", "StrongSwan", "Apache", "radsecproxy", "OpenSSH", "OpenSSL".

The validator 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.

9.7 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 testing 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 correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

The validation team notes that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment, such as the syslog server, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: *Aruba ClearPass Policy Manager 6.11 Security Target, Version 1.0, March 21, 2023.*

13 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.

14 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 (NDcPP22e)

[5] Network Device Collaborative Protection Profile (NDcPP)/Application Software Protection Profile (App PP) Extended Package (EP) for Authentication Servers, Version 1.0, 07 August 2015 (AUTHSRVEP10).

[6] Aruba ClearPass Policy Manager 6.11 Security Target, Version 1.0, March 21, 2023 (ST).

[7] Assurance Activity Report for Aruba ClearPass Policy Manager 6.11, Version 1,0, March 21, 2023 (AAR).

[8] Detailed Test Report for Aruba ClearPass Policy Manager 6.11, Version 1.0, March 21, 2023 (DTR).

[9] Evaluation Technical Report for Aruba ClearPass Policy Manager 6.11, Version 1.0, March 21, 2023 (ETR)