# National Information Assurance Partnership
# Common Criteria Evaluation and Validation Scheme


# Validation Report
# Aruba Mobility Controller with ArubaOS 8.10

**Report Number:** CCEVS-VR-VID11333-2023
**Dated:** May 19, 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

Patrick Mallett, Ph.D.
Jerome Myers, Ph.D.
J. David Thompson
Fernando Guzman
*The Aerospace Corporation*

## Common Criteria Testing Laboratory

Tyler Catterton
Cody Cummins
Douglas Kalmus
*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 Mobility Controller with ArubaOS 8.10 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 May 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 Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements of the following PP-Configuration:

- PP-Configuration for Network Devices, Wireless Local Area Network (WLAN) Access Systems, Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways, 2022-06-16. (CFG_NDcPP-WLANAS-FW-VPNGW_V1.0)
    - Base-PP: collaborative Protection Profile for Network Devices, Version 2.2e (CPP_ND_V2.2E)
    - PP-Module: PP-Module for Wireless Local Area Network (WLAN) Access System, Version 1.0 (MOD_WLAN_AS_V1.0)
    - PP-Module: PP-Module for Stateful Traffic Filter Firewalls, Version 1.4 + Errata 20200625 (MOD_CPP_FW_V1.4E)
    - PP-Module: PP-Module for VPN Gateways, Version 1.2 (MOD_VPNGW_V1.2)

The Target of Evaluation (TOE) is the Aruba Mobility Controller with ArubaOS 8.10. The 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 Mobility Controller with ArubaOS 8.10 Security Target, version 0.5, May 19, 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 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 Mobility Controller with ArubaOS 8.10<br>(Specific models identified in Section 8) |
| **Protection Profile** | PP-Configuration for Network Devices, Wireless Local Area Network (WLAN) Access Systems, Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways, 2022-06-16. (CFG_NDcPP-WLANAS-FW-VPNGW_V1.0)<br>• Base-PP: collaborative Protection Profile for Network Devices, Version 2.2e (CPP_ND_V2.2E)<br>• PP-Module: PP-Module for Wireless Local Area Network (WLAN) Access System, Version 1.0 (MOD_WLAN_AS_V1.0)<br>• PP-Module: PP-Module for Stateful Traffic Filter Firewalls, Version 1.4 + Errata 20200625 (MOD_CPP_FW_V1.4E) |

| Item | Identifier |
|---|---|
| | • PP-Module: PP-Module for VPN Gateways, Version 1.2 (MOD_VPNGW_V1.2) |
| **ST** | Aruba Mobility Controller with ArubaOS 8.10 Security Target, version 0.5, May 19, 2023 |
| **Evaluation Technical Report** | Evaluation Technical Report for Aruba Mobility Controller with ArubaOS 8.10, version 1.0, May 19, 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.<br>Columbia, MD |
| **CCEVS Validators** | Patrick Mallett, Jerome Myers, David Thompson, Fernando Guzman |

# 3 Architectural Information

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

The TOE is Aruba Mobility Controller with ArubaOS 8.10. The TOE is a multi-purpose network device that includes WLAN access system, stateful traffic filter firewall and VPN gateway capabilities. The Aruba Mobility Controller platform serves as a gateway between wired and wireless networks and provides command and control over Aruba Access Points (APs) within an Aruba dependent wireless network.

The Aruba Mobility Controllers (MCs) and Aruba Virtual Mobility Controllers (VMCs) are wireless switch hardware and virtual appliances that provide a wide range of security services and features including wireless and wired network mobility, security, centralized management, auditing, authentication, secure remote access, self-verification of integrity and operation, stateful traffic filtering and VPN gateway functionality.

The ArubaOS is a suite of mobility applications that runs on all Aruba controllers and allows administrators to configure and manage the wireless and mobile user environment. The TOE is generally deployed in a configuration consisting of one or more Aruba mobility controllers (MC and/or VMC) and multiple Aruba wireless APs.

The TOE performs stateful packet filtering on network packets processed by the TOE. Filtering rules may be applied to appliance Ethernet interfaces and to user roles (for wireless clients as described above) to allow fine grained control over network traffic.

As a VPN gateway – a device at the edge of a private network that terminates an IPsec tunnel – the TOE provides device authentication, confidentiality, and integrity of information

traversing a public or untrusted network. The TOE provides packet filtering and secure IPsec tunneling. This functionality may be used with VPN clients or with other VPN gateways (i.e. site-to-site VPN).

In an encrypted WLAN, a wireless client first associates to the Mobility Controller through an AP and then authenticates (IEEE 802.11i[1]) using credentials to obtain access to the network. The authenticated wireless client is then assigned a role based on the configuration in the Mobility Controller or the authentication server. The role, in turn, maps a set of firewall policies to the client's session such that all wireless client traffic passes through a logical firewall component before traffic is forwarded outside of the Mobility Controller. The client's role can also be used to determine VLAN membership.

## 3.1 TOE Evaluated Platforms

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

## 3.2 TOE Architecture

Aruba Mobility Controllers (MCs) are hardware appliances consisting of a multicore network processor, Ethernet interfaces, and required supporting circuitry and power supplies enclosed in a metal chassis. Aruba Virtual Mobility Controllers (VMCs) consist of a 64-bit virtualized software-based managed platform on virtual machine (VM) architecture. The Aruba VMC operates on x86 platforms in a hypervisor environment.

The ArubaOS software running on the MCs and VMCs consists of two main components:

- Control Plane (CP) – implements functions which can be handled at lower speeds such as Mobility Controller system management (CLI and Web GUI), VMC system management (CLI and Web GUI), user authentication (e.g. 802.1X, RADIUS), Internet Key Exchange (IKE), auditing/logging (syslog), Wireless IDS (WIDS), and termination of protocols operating at the system level (e.g. SSH, TLS, NTP, etc.). The Control Plane runs the Linux operating system along with various user-space applications (described below).
- Data Plane (DP) - implements functions that must be handled at high speeds such as high-speed switching functions (forwarding, VLAN tagging/enforcement, bridging), termination of 802.11 associations/sessions, tunnel termination (IPsec), stateful firewall and deep packet inspection functions, and cryptographic acceleration. The Data Plane runs a lightweight, proprietary real-time OS which is known as "SOS" (an acronym which used to mean "SiByte Operating System" for an earlier generation of Mobility Controller that used the SiByte CPU). On the Mobility Controller hardware appliances, SOS runs on separate CPU cores. On the Virtual Mobility Controller appliances, SOS is a process running under Linux.

The Control Plane and Data Plane are inseparable. Administrators install the MC software by loading a single file, identified as "ArubaOS". Administrators install the VMC by creating a virtual machine in the ESXi client interface and then applying the VMC OVF template to the

[1] Implements 802.1X for wireless access points to address the security vulnerabilities found in WEP.

virtual machine, identified as "ArubaOS". Internally, the controllers unpack the ArubaOS software image into its various components. A given ArubaOS software image has a single version number and includes all software components necessary to operate the MC and VMC appliances as well as the APs which are in the operating environment of the TOE.

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

- Monitors and manages critical system resources, including processes, memory, and flash
- Manages system configuration and licensing
- Manages an internal database used to store licenses, user authentication information, etc
- Provides network anomaly detection, hardware monitoring, mobility management, wireless management, and radio frequency management services
- Provides a Command Line Interface (CLI)
- Provides a web-based (HTTPS/TLS) management UI for the MCs and VMCs
- Provides various WLAN station management functions
- Provides authentication services for the system management interfaces (CLI, web GUI) as well as for WLAN users
- Provides IPsec key management services for VPN users, and connections with other Aruba mobility controllers
- Provides network time protocol service, point to point tunneling protocol services for users, layer 2 tunneling protocol services for users, SSH services for incoming management connections, SNMP client/agent services, and protocol independent multicast (routing) services for the controller
- Provides syslog services by sending logs to the operating environment

The Linux OS running on the CP is a version 2.6.32 kernel for the 7xxx models and a version 4.14.181 kernel for the 9xxx models and VMCs. Linux is a soft real-time, multi-threaded operating system that supports memory protection between processes. Only Aruba provided interfaces are used, and the CLI is a restricted command set. Administrators do not have access to the Linux command shell or operating system.

All Aruba Mobility Controller and Virtual Mobility Controller models run the same ArubaOS 8.10 software and include the same ArubaOS Crypto Module. Regardless of the different hardware and virtual platforms, the security functionality remains the same. The differences in the platforms are in the processing speed, throughput, memory capacity, storage, physical interfaces, number of ports, etc., and are based on performance and scalability requirements. All models run the same code with the only differences being the hardware specific code for the differently scaled hardware and the virtual nature of the hardware ports on the VMs.

The Virtual Mobility Controller uses gigabit Ethernet interfaces just as a hardware-based mobility controller does, but these interfaces map to virtual interfaces created in the underlying hypervisor. Those interfaces, in turn, may map directly to physical ports. The device drivers on all VM platforms are identical because the ArubaOS is being run on a hypervisor. Within

the hypervisor, there may be slight differences in device drivers (mostly for network interfaces), however, the device drivers are not used to enforce any TOE security functions.

Although the TOE models have different specifications (in terms of performance and scalability), they all provide the same security functions described in the ST; therefore, they have been considered to be the same for the purposes of the ST description.

## 3.3 Physical Boundaries

The TOE consists of the following components:

- Aruba Mobility Controllers: 9004, 9012, 9240, 7005, 7008, 7010, 7024, 7030, 7205, 7210, 7220, 7240, 7240XM, 7280
- Aruba Virtual Mobility Controllers: MC-VA-50, MC-VA-250, MC-VA-1k
- ArubaOS version 8.10

These components are identified and described in section 1.2 of this ST. The TOE is being evaluated as a physical device.

The ArubaOS consists of a base software package with add-on software modules that can be activated by installing the appropriate licenses. The following SFR-enforcing software modules are required to be licensed and installed in the CC evaluated configuration.

| **Required Software Module** | **Description** |
|---|---|
| Policy Enforcement Firewall Next Generation | Provides identity-based security for wired and wireless clients. Stateful firewall enables classification based on client identity, device type, location, and time of day, and provides differentiated access for different classes of users. |
| RFprotect | Detects, classifies and limits designated wireless security threats such as rogue APs, DoS attacks, malicious wireless attacks, impersonations, and unauthorized intrusions. Eliminates need for separate system of RF sensors and security appliances. Also provides spectrum intelligence and spectrum visibility when used with compatible AP platforms. |
| Advanced Cryptography | Required for SuiteB, AES-GCM and ECDSA functionality. |

The TOE operates with the following components in the Operating Environment:

One or more of the following Aruba Access Points running ArubaOS 8.10:

| **Aruba Access Points** | | |
|---|---|---|
| **300 Series** | **500 Series** | **600 Series** |
| AP-303H Access Point | AP-503H Access Point | AP-635 Access Point |
| AP-304/5 Access Point | AP-504/5 Access Point | AP-655 Access Point |
| AP-314/5 Access Point | AP-514/5 Access Point | |
| AP-318 Access Point | AP-518 Access Point | |
| AP-324/5 Access Point | AP-534/5 Access Point | |

| | | |
|---|---|---|
| AP-334/5 Access Point | AP-555 Access Point | |
| AP-344/5 Access Point | AP-565/7 Access Point | |
| AP-364/5 Access Point | AP-574/5/7 Access Point | |
| AP-374/5/7 Access Point | AP-584/5/7 Access Point | |
| AP-387 Access Point | | |

- Audit Server – The TOE utilizes an external syslog server to store audit records.
- Authentication Server – The TOE utilizes RADIUS and TACACs+ servers to authenticate users.
- Time Server – The TOE uses a Network Time Protocol (NTP) server to synchronize its system clock with a central time source.
- Web Browser – The remote administrator uses a web browser to access the Web GUI interface.
- SSH Client – The remote administrator uses an SSH client to access the CLI.
- VPN Gateway peers/VPN Clients - When acting as a VPN gateway, the TOE may communicate with other VPN gateways or with VPN clients.

# 4 Security Policy

This section summaries the security functionality of the TOE:

1. Security audit
2. Cryptographic support
3. User data protection
4. Firewall
5. Identification and authentication
6. Security management
7. Packet filtering
8. Protection of the TSF
9. TOE access
10. 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 including start-up and shutdown of the TOE, all administrator actions, and all events identified in Table 8 Auditable Events of the Security Target. 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 in the operational environment.

## 4.2 Cryptographic support

The TOE includes cryptographic modules that provide key management, random bit generation, encryption/decryption, digital signature and secure hashing and key-hashing features in support of higher-level cryptographic protocols including IPsec, SSH, and TLS/HTTPS.

## 4.3 User data protection

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

## 4.4 Firewall

The TOE performs stateful packet filtering. Filtering rules may be applied to appliance Ethernet interfaces or to user-roles (wireless clients connecting through APs are placed into user-roles). Stateful packet filter policies are applied to user-roles to allow fine grained control over wireless traffic.

## 4.5 Identification and authentication

The TOE requires administrators to be identified and authenticated before they can access any TOE security functions. The TOE supports role-based authentication, so user accounts are assigned predefined roles which restrict them based on their assigned role. The TOE maintains these administrator and user attributes which can be defined locally with user names and passwords or can be defined in the context of local RADIUS or TACACS+ services. Authentication can be either locally or remotely through an external authentication server, or internally. Wireless clients are identified and authenticated by different authentication mechanisms such as 802.1X, etc. After an administrator-specified number of failed attempts, the user account is locked out. The TOE's password mechanism provides configuration for a minimum password length. The TOE also protects, stores and allows authorized administrators to load X.509.v3 certificates for use to support authentication for IPsec connections.

## 4.6 Security management

The TOE provides the administrator role the capability to configure and manage all TOE security functions including cryptographic operations, user accounts, passwords, advisory banner, session inactivity and TOE updates. The management functions are restricted to the administrator role. The role must have the appropriate access privileges or access will be denied. The TOE's cryptographic functions ensure that only secure values are accepted for security attributes.

## 4.7 Packet filtering

The TOE may be used as a VPN gateway – a device at the edge of a private network that terminates an IPsec tunnel, which provides device authentication, confidentiality, and integrity of information traversing a public or untrusted network. The TOE provides packet filtering and secure IPsec tunneling. The tunnels can be established between two trusted VPN peers as well as between remote VPN clients and the TOE. An administrator can configure security policies that determine whether to block, allow, or log a session based on traffic attributes such as the source and destination security zone, the source and destination IP address, the application, user, and the service.

## 4.8 Protection of the TSF

The TOE has its own internal hardware clock that provides reliable time stamps used for auditing. The internal clock may be synchronized with a time signal obtained from an external trusted NTP server. The TOE stores passwords on flash using a SHA1 hash and does not provide any interfaces that allow passwords or keys to be read.

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

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

## 4.9 TOE access

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

In order to limit access to the administrative functions, the TOE can be configured to deny remote VPN clients based on the time/date, IP address (location), as well as information retained in a blacklist. The TOE assigns a private IP address (internal to the trusted network for which the TOE is the headend) to a VPN client upon successful establishment of a session.

## 4.10 Trusted path/channels

The TOE uses IPsec to provide an encrypted channel between itself and third-party trusted IT entities in the operating environment including external syslog server, external authentication server, NTP server and VPN Gateway/Client.

The TOE also provides a protected communication path between itself and wireless users. The TOE protects communication with wireless clients using WPA3 and WPA2 with 802.1x EAP-TLS.

The TOE secures remote communication with administrators by implementing TLS/HTTPS for remote Web UI access and SSHv2 for CLI 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.

# 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)
- PP-Module for Wireless Local Area Network (WLAN) Access System, version 1.0, 19 April 2022 (WLANAS10)
- PP-Module for Stateful Traffic Filter Firewalls, version 1.4 + Errata 20200625, 25 June 2020 (STFFW14e)
- PP-Module for Virtual Private Network (VPN) Gateways, version 1.2, 31 March 2022 (VPNGW12)

That information has not been reproduced here and the NDcPP22e/STFFW14e/ WLANAS10/VPNGW12 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/STFFW14e/WLANAS10/VPNGW12 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 WLAN, FW, and VPNGW PP-Modules 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.
- Apart from the Admin Guide, additional customer documentation for the specific network infrastructure device with WLAN, VPN Gateway, and Firewall capabilities 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/STFFW14e/WLANAS10/VPNGW12 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

Section 3.3 list devices that are required in the environment but have not been evaluated in the scope of this evaluation.

# 6 Documentation

The following documents were available with the TOE for evaluation:

- ArubaOS 8.10.0.0 User Guide
- Common Criteria Configuration Guidance Aruba OS 8.10 Supplemental Guidance, Version 2.0, April 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 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 Mobility Controller with ArubaOS 8.10, Version 1.0, May 19, 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/STFFW14e/WLANAS10/ VPNGW12 including the tests associated with optional requirements. The AAR, in sections 1.1 lists the tested devices, provides a list of test tools, and has diagrams of the test environment.

# 8 Evaluated Configuration

The evaluated configuration consists of the specified hardware and software when configured in accordance with the guidance documents listed in the Documentation Section. The configuration is the Aruba Mobility Controller with ArubaOS version 8.10 and the following required software licenses:

- Policy Enforcement Firewall
- RFprotect
- Advanced Cryptography.

The TOE includes the following hardware and virtual appliance models:

**Mobility Controller Hardware Appliances**

| Product Model | CPU |
|---|---|
| Aruba 9004 Mobility Controller | Intel Atom C3508 (Denverton) |
| Aruba 9012 Mobility Controller | Intel Atom C3508 (Denverton) |
| Aruba 9240 Mobility Controller | Intel Atom C3508 (Denverton) |
| Aruba 7005 Mobility Controller | Broadcom XLP208 (MIPS64) |
| Aruba 7008 Mobility Controller | Broadcom XLP208 (MIPS64) |
| Aruba 7010 Mobility Controller | Broadcom XLP208 (MIPS64) |
| Aruba 7024 Mobility Controller | Broadcom XLP208 (MIPS64) |
| Aruba 7030 Mobility Controller | Broadcom XLP208 (MIPS64) |
| Aruba 7205 Mobility Controller | Broadcom XLP316 (MIPS64) |
| Aruba 7210 Mobility Controller | Broadcom XLP416 (MIPS64) |
| Aruba 7220 Mobility Controller | Broadcom XLP432 (MIPS64) |
| Aruba 7240 Mobility Controller | Broadcom XLP432 (MIPS64) |
| Aruba 7240XM Mobility Controller | Broadcom XLP432 (MIPS64) |
| Aruba 7280 Mobility Controller | Broadcom XLP780 (MIPS64) |

The table below shows the different model series based on maximum number of APs and users supported.

| Product | Max. # of APs | Max. # of Users | Typical Deployment |
|---|---|---|---|
| Aruba 7000 Series | 64 | 4,096 | Branch Office/ Small Campus |
| Aruba 7200 Series | 2,048 | 32,768 | Headquarters / Large Campus |
| Aruba 9000 Series | 32 | 2,048 | Branch Office / Small Campus |

**Mobility Controller Virtual Appliances**

- MC-VA-50
- MC-VA-250
- MC-VA-1k

The table below shows the different virtual models based on maximum number of APs and clients supported.

| Aruba Mobility Controller Virtual Appliance | MC-VA-50 | MC-VA-250 | MC-VA-1K |
|---|---|---|---|
| Maximum AP Count | 50 APs | 250 APs | 1,000 APs |
| Maximum Client Count | 800 | 4,000 | 16,000 |

**VM Platforms**

The Mobility Controller Virtual Appliances are deployed on ESXi version 7. The following virtual machine platforms are included in the evaluated configuration:

| Name | CPU | Memory |
|---|---|---|
| HPE EdgeLine EL8000 | Intel Xeon Gold 6212U (Cascade Lake) | 128GB |
| Pacstar 451/3 | Intel Xeon E-2254ML (Coffee Lake) | 32GB |
| Pacstar 451/3 | Intel Xeon E3 1515 (Skylake) | 32GB |

| | | |
|---|---|---|
| GTS NXGEN-L11/12 | Intel Core i7 (Coffee Lake) | 16GB |

# 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 Aruba Mobility Controller with ArubaOS 8.10 TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP22e/STFFW14e/WLANAS10/VPNGW12.

## 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 Mobility Controller with ArubaOS 8.10 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/STFFW14e/WLANAS10/ VPNGW12 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/STFFW14e/WLANAS10/ VPNGW12 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 that was completed on 4/28/2023. The public search for vulnerabilities did not uncover any residual vulnerability.

The evaluator searched the National Vulnerability Database (https://web.nvd.nist.gov/view/vuln/search) and Vulnerability Notes Database (http://www.kb.cert.org/vuls/) with the following search terms: “aruba 802.1X”, “aruba tcp”, “aruba mobility controller”, “arubaos”, “aruba ipsec”, “aruba ssh”, “aruba tls”, “arubaos openssl”, “arubaos uboot”, “aruba vmc”, “aruba vpn”, “esxi”, “sos”, “sibyte”, “Linux OS v2.6.32 kernel”, “Linux OS v4.14.181 kernel”, "Intel Atom C3508", "Broadcom XLP208", "Broadcom XLP316", "Broadcom XLP416", "Broadcom XLP432", "Broadcom XLP780".

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 evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the Administrator Guide document listed in Section 6. No versions of the TOE and software, either earlier or later were evaluated. Please note 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 Mobility Controller with ArubaOS 8.10 Security Target, Version 0.5, May 19, 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] PP-Module for Wireless Local Area Network (WLAN) Access System, version 1.0, 19 April 2022 (WLANAS10)

[6] PP-Module for Stateful Traffic Filter Firewalls, version 1.4 + Errata 20200625, 25 June 2020 (STFFW14e)

[7] PP-Module for Virtual Private Network (VPN) Gateways, version 1.2, 31 March 2022 (VPNGW12)

[8] Aruba Mobility Controller with ArubaOS 8.10 Security Target, Version 0.5, May 19, 2023 (ST).

[9] Assurance Activity Report for Aruba Mobility Controller with ArubaOS 8.10, Version 1.0, May 19, 2023 (AAR).

[10] Detailed Test Report for Aruba Mobility Controller with ArubaOS 8.10, Version 1.0, May 19, 2023 (DTR).

[11] Evaluation Technical Report for Aruba Mobility Controller with ArubaOS 8.10, Version 1.0, May 19, 2023 (ETR)