National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

Aruba Virtual Intranet Access (VIA) Client Version 4.3

Report Number: CCEVS-VR-VID11303-2022
Dated: 31 August 2022
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

Sheldon Durrant

Randy Heimann

Linda Morrison

The MITRE Corporation

Common Criteria Testing Laboratory

Leidos Inc.
Columbia, MD

Contents

List of Tables

1 Executive Summary

This Validation Report (VR) documents the National Information Assurance Partnership (NIAP) assessment of the Aruba Virtual Intranet Access (VIA) Client, Version 4.3 (the Target of Evaluation (TOE)) evaluation. It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

The evaluation was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America, and was completed in August 2022. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report written by Leidos. The evaluation determined that the TOE is Common Criteria Part 2 Extended and Common Criteria Part 3 Extended meets the assurance requirements of the *PP-Configuration for Application Software and Virtual Private Network (VPN) Clients*, Version 1.0, 13 August 2021. This PP-Configuration includes the following components:

- Base-PP: *Protection Profile for Application Software*, Version 1.3, 01 March 2019
- PP-Module: *PP-Module for Virtual Private Network (VPN) Clients*, Version 2.3, 10 August 2021

The TOE is the Aruba VIA Client, Version v4.3. 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 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 Virtual Intranet Access (VIA) Client Version 4.3 Security* Target, Version 1.0, August 23, 2022, 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—the document describing the security features, claims, and assurances of the product
- The conformance result of the evaluation
- The PP/PP-Modules 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 Virtual Intranet Access (VIA) Client, version 4.3
Protection Profile	*PP-Configuration for Application Software and Virtual Private Network (VPN) Clients*, Version 1.0, 13 August 2021 This PP-Configuration includes the following components: • Base-PP: *Protection Profile for Application Software*, Version 1.3, 01 March 2019 • PP-Module: *PP-Module for Virtual Private Network (VPN) Clients*, Version 2.3, 10 August 2021
Security Target	*Aruba Virtual Intranet Access (VIA) Client Version 4.3 Security Target*, Version 1.0, August 23, 2022
Evaluation Technical Report	*Evaluation Technical Report for Aruba, a Hewlett Packard Enterprise company Virtual Intranet Access (VIA) Client Version 4.3*, Version 1.1, August 23, 2022
Sponsor & Developer	Aruba, a Hewlett Packard Enterprise Company 3333 Scott Boulevard Santa Clara, CA 95054
CC Version	*Common Criteria for Information Technology Security Evaluation*, Version 3.1, Rev 5, April 2017
Conformance Result	CC Part 2 extended, CC Part 3 extended

Item	Identifier
CCTL	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Evaluation Personnel	Justin Fisher, Allen Sant
Validation Personnel	Jenn Dotson, Sheldon Durrant, Randy Heimann, Linda Morrison

3 TOE Architecture

The Target of Evaluation (TOE) is the Aruba Virtual Intranet Access (VIA) Client version 4.3. The TOE is a software application with IPsec Virtual Private Network (VPN) client capability. The TOE boundary includes Windows, Linux, and Android versions of the application. Each version of the application is identical with respect to the capabilities it offers the user; the security-relevant implementation differences between each version only include those functions where different mechanisms are used to interact with the platform, depending on the platform being claimed (e.g., the platform mechanism used for any storage of credential data and configuration settings will differ based on the platform version).

VIA is a part of the Aruba remote networks solution intended for teleworkers and mobile users. VIA detects the network environment (trusted and untrusted) of the user and connects the users to the enterprise network. The VIA Client interacts with an environmental Aruba Mobility Controller, which functions as its VPN gateway as well as the authorized source of its IPsec configuration settings.

3.1 Evaluated Configuration

The TOE is Aruba Virtual Intranet Access (VIA) v4.3, deployed on Windows 10 (64-bit), Android 11, or Ubuntu 18.04. The TOE is a third-party application that is installed onto a general-purpose operating system or mobile device. The TOE is evaluated as a software application with VPN client capability.

Beyond the underlying OS/device platform that the TOE is installed on, and for which it relies on for some security functions, the operational environment includes an Aruba Mobility Controller that functions both as a VPN gateway for IPsec connections as well as the source of the TOE's configuration for IPsec channels. The operational environment also requires a public key infrastructure that is able to issue leaf certificates that chain to a valid Certificate Authority so that X.509 validation can occur. The public key infrastructure must also include an OCSP responder for managing the revocation status of certificates.

3.2 Excluded Functionality

The list below identifies features or protocols that are not evaluated or must be disabled and the rationale why.

Feature	Description
iOS and macOS platform versions	The TOE is a Windows/Linux/Android application. iOS and macOS versions of the product are available but were not tested.
Non-FIPS mode of operation	The product does not enable the use of FIPS compliant algorithms by default; this is configured by the VPN gateway and applied by the TOE when it receives configuration information. Operational guidance instructs the administrator to ensure that FIPS mode is enabled because the product was not evaluated when it is not.

4 Security Policy

The TOE enforces the following security functionality as claimed in the ST.

4.1 Cryptographic Support

The TOE includes a cryptographic library with NIST-validated algorithm implementations that is used to perform the cryptographic functions needed for IPsec. The TOE implements IPsec with support for either IKEv1 or IKEv2. Authentication is performed using X.509 certificates, and in the case of IKEv1, pre-shared keys can be used as well. VPN connection settings are configured by the environmental Mobility Controller gateway; the gateway configures the connection settings that the client must use, such as the ESP and IKE encryption algorithms, the Diffie-Hellman group, and the mechanism used for authentication. The TOE ensures the secure storage and destruction of key and credential data using a combination of its own mechanisms and reliance on appropriate platform functionality.

4.2 User Data Protection

The TOE leverages platform-provided functionality to encrypt sensitive data and allows network communications to be initiated by the user to connect to the VPN Gateway. The TOE can also provide always-on functionality for application-initiated network communication.

The TOE ensures that residual information is protected from potential reuse in accessible objects such as network packets.

4.3 Identification and Authentication

The TOE provides the ability to use, store, and protect X.509 certificates that are used for IPsec VPN connections. The TOE performs peer authentication using pre-shared keys or certificates.

Pre-shared keys apply to IKEv1 only. Character limits and character set are not enforced programmatically; therefore, the administrative guidance includes instructions on setting strong pre-shared keys.

4.4 Security Management

The TOE and its IPsec VPN are fully configurable by a combination of functions provided directly by the TOE and those available to the associated VPN gateway. The TOE is not provided with any default credentials or pre-shared keys. All external configuration comes from the Mobility Controller. The configuration options for the TOE consists of the URL of the gateway and the credentials used for the connection. The configuration options are stored and set using the mechanisms supported by the platform.

4.5 Privacy

The TOE does not transmit personally identifiable information (PII) over a network.

4.6 Protection of the TSF

The TOE performs self-tests that cover the TOE as well as the functions necessary to securely update the TOE.

The TOE includes the use of only documented platform APIs.

For each platform, the application does not allocate any memory region with both write and execute permissions nor does the TOE request to map memory to an explicit address. The TOE does not write user-

modifiable files to directories that contain executable files. The application is built with stack-based buffer overflow protection enabled.

Aruba provides a version control system for its software components. The TOE has a unique software versioning that identifies major versions and their subsequent maintenance releases.

The TOE platforms support loading updates by the administrator. For Windows and Linux platforms, the administrator obtains the update in the form of an installer through the Aruba Mobility Controller or the Aruba Support Portal. The update is verified using a RSA 2048 with SHA-1 digital signature. For Android versions, the application and signature are provided to and verified by the Google Play Store.

The TOE does not download, modify, replace, or update its own binary code. The application is packaged such that its removal results in the deletion of all traces of the application, except for configuration settings and output files.

4.7 Trusted Path/Channels

The cryptography for the initial HTTPS connection is provided by the platform and is therefore outside the scope of the TOE. The IKE/IPsec transversal is secured using the TOE cryptography.

The TOE acts as a VPN client using IPsec to established secure channels to the corresponding VPN gateways.

5 Assumptions and Clarification of Scope

5.1 Assumptions

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

- *Protection Profile for Application Software*, Version 1.3, 01 March 2019
- *PP-Module for Virtual Private Network (VPN) Clients*, Version 2.3, 10 August 2021

That information has not been reproduced here and PP_APP_V1.3/MOD_VPNC_V2.3 should be consulted if there is interest in that material.

5.2 Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in the PP_APP_V1.3/MOD_VPNC_V2.3 as described for this TOE in the ST. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation shows only that the evaluated configuration meets the security claims made, with a certain level of assurance (the assurance activities specified in the PP_APP_V1.3/MOD_VPNC_V2.3 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 Virtual Intranet Access (VIA) Client Version 4.3 Security Target*, version 1.0, 23 August 2022, and not any earlier or later versions released or in process.
- Apart from the Admin Guide 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 PP_APP_V1.3/MOD_VPNC_V2.3 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

6 Documentation

The vendor offers guidance documents describing the installation process for the TOE as well as guidance for subsequent administration and use of the applicable security features. The guidance documentation examined during the evaluation and delivered with the TOE is as follows:

- *Aruba Virtual Intranet Access (VIA) 4.x Client Common Criteria Guidance*, version 1.2, March 2022

To use the product in the evaluated configuration, the product must be configured as specified in this documentation.

7 IT Product Testing

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

- *Aruba Virtual Intranet Access (VIA) Client version 4.3 Common Criteria Test Report and Procedures*, Version 1.2., August 24, 2022 (DTR)

A non-proprietary description of the tests performed, and their results is provided in the following document:

- *Assurance Activities Report for Aruba Virtual Intranet Access (VIA) Client Version 4.3*, Version 1.1, August 24, 2022 (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 PP_APP_V1.3/MOD_VPNC_V2.3 including the tests associated with optional requirements.

8 Results of the Evaluation

The results of the evaluation of the TOE against its target assurance requirements are generally described in this section and are presented in detail in the proprietary *Evaluation Technical Report for Aruba Virtual Intranet Access (VIA) Client v4.3* (ETR). The reader of this VR can assume that all assurance activities and work units received passing verdicts.

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 the claimed PP and PP-Module. The evaluation determined the TOE satisfies the conformance claims made in the Security Target, which are Part 2 extended and Part 3 extended.

8.1 Evaluation of the Security Target (ASE)

The Evaluation team performed each TSS assurance activity and ASE CEM work unit. The ST evaluation ensured the ST contains an ST introduction, TOE overview, TOE description, security problem definition in terms of threats, policies and assumptions, description of security objectives for the operational environment, a statement of security requirements claimed to be met by the product that are consistent with the claimed Protection Profile, and security function descriptions that satisfy the requirements.

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

8.2 Evaluation of the Development (ADV)

The Evaluation team 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 ADV evidence consists of the TSS descriptions provided in the ST and product guidance documentation providing descriptions of the TOE external interfaces.

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

8.3 Evaluation of the Guidance Documents (AGD)

The Evaluation team performed each guidance assurance activity and applied each AGD work unit. The evaluation team determined the adequacy of the operational user guidance in describing how to operate the TOE in accordance with the descriptions in the ST. The Evaluation team followed the guidance in the TOE preparative procedures to test the installation and configuration procedures to ensure the procedures result in the evaluated configuration. The guidance documentation was assessed during the design and testing phases of the evaluation to ensure it was complete.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in

accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

8.4 Evaluation of the Life Cycle Support Activities (ALC)

The Evaluation team performed each ALC assurance activity (including those for the extended SAR ALC_TSU_EXT.1) and applied each ALC_CMC.1 and ALC_CMS.1 CEM work unit, to the extent possible given the evaluation evidence required by the claimed Protection Profile. The Evaluation team ensured the TOE is labeled with a unique identifier consistent with the TOE identification in the evaluation evidence, and that the ST describes how timely security updates are made to the TOE.

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

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

The Evaluation team performed each test activity and applied each ATE_IND.1 CEM work unit. The evaluation team ran the set of tests specified by the claimed PP and PP-Module and recorded the results in the 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 (AVA)

The Evaluation team performed each AVA assurance activity and applied each AVA_VAN.1 CEM work unit. The Evaluation team performed a vulnerability analysis following the processes described in the claimed PP. This comprised a search of public vulnerability databases.

Searches of public vulnerability repositories were performed several times, most recently on 08 August 2022.

The evaluation team performed a search of the following public vulnerability databases:

- National Vulnerability Database (https://nvd.nist.gov/)
- Aruba Security Advisories (https://www.arubanetworks.com/support-services/security-bulletins/)

Searches were performed using the following search terms:

- aruba
- arubanetworks
- aruba via
- Virtual Intranet Client
- IPSec VPN Client

The Evaluation team determined that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential. Note that a security-relevant and potentially exploitable vulnerability was disclosed by Aruba on 26 July 2022. Per the Vendor, this vulnerability was addressed by a new build

released on 15 August 2022 (reference https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-011.txt.)

Aside from the mitigated vulnerability, the results of these searches did not identify unmitigated vulnerabilities that are applicable to the TOE. The conclusion drawn from the vulnerability analysis is that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential as defined by the Certification Body in accordance with the guidance in the CEM.

The Evaluation team conducted virus scanning on Windows and Linux and observed that no potential malicious findings were present. Scanning was done on McAfee Endpoint Security 10.7, with virus definitions updated as of 6/21/2022.

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, sufficient to satisfy the assurance activities specified in the claimed Protection Profile and PP-Module. 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.

9 Validator Comments/Recommendations

As noted in Section 8.6, a vulnerability was disclosed on July 26, 2022, and an updated build was released on August 15, 2022. Customers should ensure that they are operating Version 4.3.0 build 2208101, released August 15, 2022

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 *Aruba Virtual Intranet Access (VIA) 4.x Client Common Criteria Guidance,* version 1.2, March 2022. 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 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. Note, however, that since the TOE generally receives configuration information from the Mobility Controller gateway, the administrator is assumed to have existing familiarity with the configuration of the gateway and is also capable of referencing documentation for it as needed.

10 Security Target

The ST for this product's evaluation is *Aruba Virtual Intranet Access (VIA) Client Version 4.3 Security Target*, Version 1.0, 23 August 2022.

11 Abbreviations and Acronyms

This section identifies abbreviations and acronyms used in this document.

FIPS	Federal Information Processing Standard
OCSP	Online Certificate Status Protocol
OE	Operational Environment
OS	Operating System
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
VIA	Virtual Intranet Access [Client] (the TOE)
VPN	Virtual Private Network

12 Bibliography

The validation team used the following documents to produce this VR:

[1] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017.

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

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

[4] Common Criteria Project Sponsoring Organisations. Common Evaluation Methodology for Information Technology Security, Version 3.1, Revision 5, April 2017.

[5] Protection Profile for Application Software, Version 1.3, 01 March 2019

[6] PP-Module for Virtual Private Network (VPN) Clients, Version 2.3, 10 August 2021

[7] PP-Configuration for Application Software and Virtual Private Network Clients, Version 1.0, 13 August 2021

[8] *Aruba Virtual Intranet Access (VIA) Security Target*, Version 1.0, 23 August 2022

[9] *Aruba Virtual Intranet Access (VIA) 4.x Client Common Criteria Guidance*, Version 1.2, March 2022

[10] *Evaluation Technical Report for Aruba Virtual Intranet Access (VIA) Client Version 4.3* (Leidos Proprietary), Version 1.1, 23 August 2022

[11] *Assurance Activities Report for Aruba Virtual Intranet Access (VIA) Client Version 4.3*, Version 1.1, 24 August 2022

[12] *Aruba Virtual Intranet Access (VIA) Client version 4.3 Common Criteria Test Report and Procedures* (Leidos Proprietary), Version 1.2, 24 August 2022

[13] *Aruba Virtual Intranet Access (VIA) Client Version 4.3- Vulnerability Analysis* (Leidos Proprietary), Version 1.3, 24 August 2022