National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report
Apriva MESA VPN v3.0

Report Number:	**CCEVS-VR-VID11363-2023**
Dated:	**July 31, 2023**
Version:	**0.1**

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
Aerospace Corporation

Anne Gugel
Michael Smeltzer
Russell Fink
Robert Wojcik
Richard Toren
Johns Hopkins University - Applied Physics Laboratory

Common Criteria Testing Laboratory

Ryan Hagedorn
Cornelius Haley
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 Apriva MESA VPN v3.0 solution provided by Apriva ISS, LLC. 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 July 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 PP-Configuration for Network Devices and Virtual Private Network (VPN) Gateways, version 1.2, 31 March 2022 (CFG_NDcPP-VPNGW_V1.2) which includes the Base PP: collaborative Protection Profile for Network Devices, version 2.2e, 23 March 2020 with the PP-Module for Virtual Private Network (VPN) Gateways, version 1.2, 31 March 2022.

The Target of Evaluation (TOE) is the Apriva MESA VPN 3.0.

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 Apriva MESA VPN 3.0 Security Target, version 0.4, July 18, 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	Apriva MESA VPN 3.0 (Specific models identified in Section 8)
Protection Profile	PP-Configuration for Network Devices and Virtual Private Network (VPN) Gateways, version 1.2, 31 March 2022 (CFG_NDcPP-VPNGW_V1.2) which includes the Base PP: collaborative Protection Profile for Network Devices, version 2.2e, 23 March 2020 with the PP-Module for Virtual Private Network (VPN) Gateways, version 1.2, 31 March 2022
ST	Apriva MESA VPN 3.0 Security Target, version 0.4, July 18, 2023
Evaluation Technical Report	Evaluation Technical Report for Apriva MESA VPN 3.0, version 0.2, July 18, 2023
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 5
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Apriva ISS, LLC
Developer	Apriva ISS, LLC
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Columbia, MD
CCEVS Validators	Swapna Katikaneni, Jerome Myers, Anne Gugel, Michael Smeltzer, Russell Fink, Robert Wojcik and Richard Toren

3 Architectural Information

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

The Target of Evaluation (TOE) is the Apriva MESA VPN 3.0. The Apriva MESA VPN server is an IPsec VPN gateway designed to provide mobile devices with a secure connection to a protected network. The Apriva MESA VPN is a standards-based VPN concentrator with no proprietary modes of operation, and supporting most native VPN clients in Microsoft, Android, and Apple iOS operating systems.

3.1 TOE Evaluated Platforms

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

3.2 TOE Architecture

The TOE is the Apriva MESA VPN 3.0 consisting of the following hardware and software.

- Dell PowerEdge R750 2U Rackmount Server or Dell PowerEdge R650 1U Rackmount Server
- CPU: Intel® Xeon® CPU listed below:
  - Intel® Xeon® Silver 4309Y
  - Intel® Xeon® Silver 4316
  - Intel® Xeon® Silver 4314
  - Intel® Xeon® Gold 5315Y
  - Intel® Xeon® Gold 5317
  - Intel® Xeon® Gold 5318Y
  - Intel® Xeon® Gold 5318N
  - Intel® Xeon® Gold 5320
  - Intel® Xeon® Gold 6326
  - Intel® Xeon® Gold 6330
  - Intel® Xeon® Gold 6330N
  - Intel® Xeon® Gold 6336Y
  - Intel® Xeon® Gold 6338N
- NICs:
  - Intel X710-T4L Quad Port 10GbE BASE-T Adapter
  - Broadcom 5720 Dual Port 1GbE BASE-T Adapter
- Running Apriva MESA VPN release 3.0

3.3 Physical Boundaries

Each TOE appliance runs the 3.0 version of the Apriva MESA VPN software and has physical network connections to its environment to facilitate managing and filtering network traffic. The TOE appliance can also be the destination of network traffic, where it provides interfaces for its own management. The TOE may be accessed and managed through a PC or terminal which can be remote from or directly connected to the TOE. The TOE can be an IPsec peer or be a server for IPsec clients. The TOE can be configured to forward its audit records to an external syslog server in the network environment. This is generally advisable given the limited audit log storage space on the evaluated appliances.

The TOE is delivered to the customer via courier. The Software is pre-installed on the hardware prior to delivery.

4 Security Policy

This section summaries the security functionality of the TOE:

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

4.1 Security audit

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

4.2 Cryptographic support

The TOE contains a CAVP-tested cryptographic module 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, TLS, and SSH.

4.3 Identification and authentication

The TOE requires users to be identified and authenticated before they can use functions mediated by the TOE, with the exception of specific ICMP response. It provides the ability to perform password and public key authentication for administrative users.

4.4 Security management

The TOE implements a limited command line interface (CLI) to allow authorized administrators to configure the TOE. This interface restricts the administrator to executing commands required to configure and administer the TOE. All administrative activity and functions including security management commands are limited to authorized users (i.e., administrators) only after they have provided acceptable user identification and authentication data to the TOE.

4.5 Packet filtering

The TOE provides extensive packet filtering capabilities for IPv4, IPv6, TCP, and UDP. The authorized administrator can define packet filtering rules that apply to most every field within the identified packet types. The authorized administrator can define each rule to permit, deny, and log each decision.

4.6 Protection of the TSF

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

It protects particularly sensitive data such as stored passwords and 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 log accountability).

The TOE includes functions to perform self-tests so that it might detect when it is failing. It also includes mechanisms (i.e., verification of the digital signature of each new image) 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 a login 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 restrict VPN clients based on location and time and can assign a private VPN address to a client.

4.8 Trusted path/channels

The TOE protects interactive communication with administrators using SSH for CLI access to ensure both integrity and disclosure protection. If the negotiation of an encrypted session fails or if the user does not have authorization for remote administration, an attempted connection will not be established.

The TOE protects communication with the audit log server using TLS connections to prevent unintended disclosure or modification of logs. The TOE can establish IPsec connections with clients and peers.

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 Virtual Private Network (VPN) Gateways, version 1.2, 31 March 2022 (VPNGW12)

That information has not been reproduced here and the NDcPP22e/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/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 VPNGW PP-Module 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 VPN 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/VPNGW12 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:

- Apriva® MESA VPN Common Criteria Guidance, Version 3.11, July 18, 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 Apriva MESA VPN 3.0, Version 0.2, July 18, 2023 (DTR) and DTR Supplement for Apriva MESA VPN v3.0 Version 0.1, July 24, 2023, 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/VPNGW12 including the tests associated with optional requirements. The AAR, in sections 3.4.1 lists the tested configuration, tested devices and test tools.

8 Evaluated Configuration

The TOE is the Apriva MESA VPN 3.0 consisting of the following hardware and software.

- Dell PowerEdge R750 2U Rackmount Server or Dell PowerEdge R650 1U Rackmount Server
- CPU: Intel® Xeon® CPU listed below:
    - Intel® Xeon® Silver 4309Y
    - Intel® Xeon® Silver 4310
    - Intel® Xeon® Silver 4316
    - Intel® Xeon® Silver 4314
    - Intel® Xeon® Gold 5315Y
    - Intel® Xeon® Gold 5317
    - Intel® Xeon® Gold 5318Y
    - Intel® Xeon® Gold 5318N
    - Intel® Xeon® Gold 5320
    - Intel® Xeon® Gold 6326
    - Intel® Xeon® Gold 6330

    - Intel® Xeon® Gold 6330N
    - Intel® Xeon® Gold 6336Y
    - Intel® Xeon® Gold 6338N

- NICs:
    - Intel X710-T4L Quad Port 10GbE BASE-T Adapter
    - Broadcom 5720 Dual Port 1GbE BASE-T Adapter
- Running Apriva MESA VPN release 3.0.

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 Apriva MESA VPN 3.0 TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP22e/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 Apriva MESA VPN 3.0 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/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/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. 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/) on 7/12/2023 with the following search terms: “Apriva”, “Mesa”, “Broadcom+5720”, “Intel+X710-T4L”, “ssh”, “tls”, “ipsec”, “ike”, “Intel+Xeon+Silver”, “Intel+Xeon+Gold” and “Ice+Lake”.

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

All of the validators concerns are adequately captured in Section 5, Assumptions, Threats, and Clarification of Scope.

11 Annexes

Not applicable.

12 Security Target

The Security Target is identified as: *Apriva MESA VPN 3.0 Security Target, version 0.4, July 18, 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 protection 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.

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

[6] Apriva MESA VPN 3.0 Security Target, version 0.4, July 18, 2023 (ST).

[7] Assurance Activity Report for Apriva MESA VPN 3.0, Version 0.2, July 18, 2023 (AAR).

[8] Detailed Test Report for Apriva MESA VPN 3.0, Version 0.2, July 18, 2023 (DTR).

[9] Evaluation Technical Report for Apriva MESA VPN 3.0, Version 0.2, July 18, 2023 (ETR)