National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report
McAfee Advanced Threat Defense 4.12

Report Number: CCEVS-VR-11219-2021
Dated: December 14, 2021
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

Paul Bicknell
Sheldon Durrant
Randy Heimann
Lisa Mitchell
Linda Morrison
The MITRE Corporation
Bedford, MA and McLean, VA

Common Criteria Testing Laboratory

Chris Keenan
Rizheng Sun
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 McAfee Advanced Threat Defense solution provided by McAfee, 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 December 2021. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements of the collaborative Protection Profile for Network Devices, version 2.2e, 23 March 2020.

The Target of Evaluation (TOE) is the McAfee Advanced Threat Defense 4.12.

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 McAfee Advanced Threat Defense 4.12 Security Target, version 0.4, December 2, 2021 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	McAfee Advanced Threat Defense 4.12 (Specific models identified in Section 8)
Protection Profile	collaborative Protection Profile for Network Devices, version 2.2e, 23 March 2020
ST	McAfee Advanced Threat Defense 4.12 Security Target, version 0.4, December 2, 2021
Evaluation Technical Report	Evaluation Technical Report for McAfee Advanced Threat Defense 4.12, version 0.2, December 7, 2021
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	McAfee, LLC
Developer	McAfee, LLC
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Columbia, MD
CCEVS Validators	Paul Bicknell, Sheldon Durrant, Randy Heimann, Lisa Mitchell, Linda Morrison

3 Architectural Information

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

The Target of Evaluation (TOE) is McAfee Advanced Threat Defense (ATD) running software version 4.12. ATD detects stealthy, zero-day malware with a layered approach. It combines low-touch antivirus signatures, reputation, and real-time emulation defenses with in-depth static code and dynamic analysis (sandboxing) to analyze actual behavior.

The ATD hardware appliance implements dynamic and statistical analysis on data transmitted through a network to provide malware detection, assessment and classification.

The ATD processes the files through the down selectors for statistical analysis and provides a sandbox test environment which includes virtual machines running customer environments, anti-virus, anti-malware, local blacklist and whitelists. Files are executed within virtual machine environments that are monitored by the log file. The log file is then used to generate a security report of the potential malware.

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

3.1 TOE Evaluated Platforms

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

3.2 TOE Architecture

ATD is provided as a hardware network appliance. The product provides a web interface over TLS and a console connection.

There are 2 versions of the ATD product (ATD-3100 and ATD-6100). While there are different models in the TOE, they differ primarily in physical form factor, number and types of connections and slots, and relative performance, but they each provide the same security characteristics as claimed in the security target.

3.3 Physical Boundaries

The ATD evaluated configuration includes software version 4.12 running on one of the following models:

- ATD-3100 with two E5-2609v4 (Broadwell)
- ATD-6100 with two E5-2695v4 (Broadwell)

Since the same software is installed on both platforms and all security functions provided by the TOE are implemented in software, the TOE security behavior is the same on both platforms for each of the SFRs defined by the NDcPP22e. Both platforms are running Linux 4.19 kernel and McAfee OpenSSL FIPS Object Module v1.0.2c which is why the exact same software (version 4.12) operates on both platforms. The differences are related to performance – number of CPUs and amount of memory and HD/SSD storage.

The TOE may be accessed and managed through a PC or terminal in the environment which can be remote from or directly connected to the TOE.

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 audit log storage space on the evaluated appliances. The TOE can also sync its time with a NTP server. DNS is used to resolve names when performing certificate checking.

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. Protection of the TSF
6. TOE access
7. Trusted path/channels

4.1 Security audit

The TOE generates audit events associated with identification and authentication, management, updates, and user sessions. The TOE can store the events in a local log or export them to a syslog server using a TLS protected channel.

4.2 Cryptographic support

The TOE provides CAVP certified cryptography in support of its TLS and NTP implementations. Cryptographic services include key management, random bit generation, encryption/decryption, digital signature and secure hashing.

4.3 Identification and authentication

The TOE requires users to be identified and authenticated before they can use functions mediated by the TOE, except for reading the login banner. It provides the ability to both assign attributes (usernames, passwords, and roles) and to authenticate users against these attributes. The TOE also provides X.509 certificate checking for its TLS connections.

4.4 Security management

The TOE provides a command line management interface as well as a graphical user interface (GUI) accessed via the web. The web interface is protected with TLS. The management interface is limited to the authorized administrator (as defined by a role).

4.5 Protection of the TSF

The TOE provides a variety of means of protecting itself. The TOE performs self-tests that cover the correct operation of the TOE. It provides functions necessary to securely update the TOE. It provides a hardware clock to ensure reliable timestamps and can also sync to an

NTP server if configured. It protects sensitive data such as stored passwords and cryptographic keys so that they are not accessible even by an authorized administrator.

4.6 TOE access

The TOE can be configured to display a logon banner before a user session is established. The TOE also enforces inactivity timeouts for local and remote sessions.

4.7 Trusted path/channels

The TOE provides a local console which is subject to physical protection. For remote access, the web GUI is protected by TLS thus ensuring protection against modification and disclosure.

The TOE also protects its audit records from modification and disclosure by using TLS to communicate with the syslog server.

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

That information has not been reproduced here and the NDcPP22e 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 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 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 Device models was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication, and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the NDcPP22e 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:

- Configuration Guide for Common Criteria Evaluation McAfee Advanced Threat Defense 4.12

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 McAfee Advanced Threat Defense, Version 0.2, December 7, 2021 (DTR), as summarized in the Assurance Activity Report for McAfee Advanced Threat Defense, Version 0.2, December 7, 2021 (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 including the tests associated with optional requirements. The AAR in sections 1.1 lists the tested devices.

8 Evaluated Configuration

The ATD evaluated configuration includes software version 4.12 running on one of the following models:

- ATD-3100 with two E5-2609v4 (Broadwell)
- ATD-6100 with two E5-2695v4 (Broadwell)

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 team determined the Advanced Threat Defense 4.12 TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP22e.

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 McAfee Advanced Threat Defense 4.12 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

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

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 related to the examination of the information contained in the TSS.

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.

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 the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

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

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 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.

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

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

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 on 12/02/2021 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: "ATD 3100", "ATD 6100", "Advanced Threat Defense", "McAfee", "Openssl", "Linux", "TCP", "E5-2609v4 ", "E5-2695v4 ", "MATD 4.12", “NTP v4”, “TLS v1.2”.

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.

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 *Configuration Guide for Common Criteria Evaluation.* All other items and scope issues have been sufficiently addressed elsewhere in this document.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: *McAfee Advanced Threat Defense 4.12 Security Target, Version 0.4, December 2, 2021*.

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, September 2012.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, September 2012.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, September 2102.

[4] collaborative Protection Profile for Network Devices, version 2.2e, 23 March 2020.

[5] McAfee Advanced Threat Defense 4.12 Security Target, Version 0.4, December 2, 2021 (ST).

[6] Assurance Activity Report (NDcPP22e) for McAfee Advanced Threat Defense 4.12, Version 0.2, December 7, 2021 (AAR).

[7] Detailed Test Report (NDcPP22e) for McAfee Advanced Threat Defense 4.12, Version 0.2, December 7, 2021 (DTR).

[8] Evaluation Technical Report for McAfee Advanced Threat Defense, Version 0.2, December 7, 2021 (ETR).