Communications Security Establishment | Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

COMMON CRITERIA CERTIFICATION REPORT

McAfee Endpoint Security 10.7.x with ePolicy Orchestrator 5.10.x

28 July 2022

555-EWA

Canada

FOREWORD

This certification report is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE).

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved testing laboratory established under the Canadian Centre for Cyber Security (a branch of CSE). This certification report, and its associated certificate, applies only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the Canadian Common Criteria Program, and the conclusions of the testing laboratory in the evaluation report are consistent with the evidence adduced.

This report, and its associated certificate, are not an endorsement of the IT product by Canadian Centre for Cyber Security, or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the Canadian Centre for Cyber Security, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

If your organization has identified a requirement for this certification report based on business needs and would like more detailed information, please contact:

Canadian Centre for Cyber Security
Contact Centre and Information Services
contact@cyber.gc.ca | 1-833-CYBER-88 (1-833-292-3788)

OVERVIEW

The Canadian Common Criteria Program provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Testing Laboratory (CCTL) under the oversight of the Certification Body, which is managed by the Canadian Centre for Cyber Security.

A CCTL is a commercial facility that has been approved by the Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of ISO/IEC 17025, the General Requirements for the Competence of Testing and Calibration Laboratories.

By awarding a Common Criteria certificate, the Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, the evaluated security functionality, and the testing and analysis conducted by the CCTL.

The certification report, certificate of product evaluation and security target are posted to the Common Criteria portal (the official website of the International Common Criteria Program).

TABLE OF CONTENTS

EXECUTIVE SUMMARY **6**

1 Identification of Target of Evaluation **7**

1.1 Common Criteria Conformance 7

1.2 TOE Description 7

1.3 TOE Architecture 8

2 Security Policy **9**

2.1 Cryptographic Functionality 9

3 Assumptions and Clarification of Scope **10**

3.1 Usage and Environmental Assumptions 10

3.2 Clarification of Scope 10

4 Evaluated Configuration **11**

4.1 Documentation 12

5 Evaluation Analysis Activities **13**

5.1 Development 13

5.2 Guidance Documents 13

5.3 Life-Cycle Support 13

6 Testing Activities **14**

6.1 Assessment of Developer tests 14

6.2 Conduct of Testing 14

6.3 Independent Testing 14

6.3.1 Independent Testing Results 14

6.4 Vulnerability Analysis 15

6.4.1 Vulnerability Analysis Results 15

7 Results of the Evaluation **16**

7.1 Recommendations/Comments 16

8 Supporting Content **17**

8.1 List of Abbreviations 17

8.2 References 17

LIST OF FIGURES

Figure 1: TOE Architecture 8

LIST OF TABLES

Table 1: TOE Identification 7

Table 2: Cryptographic Implementation(s) 9

EXECUTIVE SUMMARY

McAfee Endpoint Security 10.7.x with ePolicy Orchestrator 5.10.x (hereafter referred to as the Target of Evaluation, or TOE), from **Trellix** , was the subject of this Common Criteria evaluation. A description of the TOE can be found in Section 1.2. The results of this evaluation demonstrate that the TOE meets the requirements of the conformance claim listed in Section 1.1 for the evaluated security functionality.

EWA-Canada is the CCTL that conducted the evaluation. This evaluation was completed on **28 July 2022** and was carried out in accordance with the rules of the Canadian Common Criteria Program.

The scope of the evaluation is defined by the Security Target, which identifies assumptions made during the evaluation, the intended environment for the TOE, and the security functional/assurance requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations, and recommendations in this Certification Report.

The Canadian Centre for Cyber Security, as the Certification Body, declares that this evaluation meets all the conditions of the Arrangement on the Recognition of Common Criteria Certificates and that the product is listed on the Certified Products list (CPL) for the Canadian Common Criteria Program and the Common Criteria portal (the official website of the International Common Criteria Program).

1 IDENTIFICATION OF TARGET OF EVALUATION

The Target of Evaluation (TOE) is identified as follows:

Table 1: TOE Identification

TOE Name and Version	McAfee Endpoint Security 10.7.x with ePolicy Orchestrator 5.10.x
Developer	Trellix

1.1 COMMON CRITERIA CONFORMANCE

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5.

The TOE claims the following conformance:

Evaluation Assurance Level 2 augmented by ALC_FLR.2– Flaw Reporting Procedures (EAL2+)

1.2 TOE DESCRIPTION

McAfee Endpoint Security (ENS) is a security management solution that protects computer systems against known and unknown threats. These threats include malware, suspicious communications, unsafe websites, and downloaded files.

In the evaluated configuration the McAfee ePolicy Orchestrator (ePO) 5.10.x is used to manage McAfee Endpoint Security Client (ENS) 10.7.x client software. The platform on which the ePO software is installed must be dedicated to functioning as the management system.

Security functionality is enforced on client computers through the following integrated modules working collectively to protect systems:

- Threat Prevention - Checks for viruses, spyware, unwanted programs, and other threats by scanning items automatically when Users access them, or on demand. Threat Prevention detects threats, then takes the actions that have been configured to protect systems.
- Firewall - Monitors communication between the computer and resources on the network and the Internet. Intercepts suspicious communications.
- Web Control – Monitors web searching and browsing activity on client systems, and blocks downloads and access to websites based on safety rating and content.
- Adaptive Threat Protection – Analyzes content from the enterprise, and decides how to respond, based on file reputation, rules and reputation thresholds.

Together, these modules are referred to as the McAfee Endpoint Security Client. In addition, the Common module provides settings for common features, such as interface security and logging. This module is installed automatically if any other module is installed.

In addition to the integrated client modules, the TOE requires the installation of the McAfee Agent on each client computer. McAfee Agent is a vehicle of information and policy exchange between the ePO server and each managed (client) computer.

1.3 TOE ARCHITECTURE

A diagram of the TOE architecture is as follows:

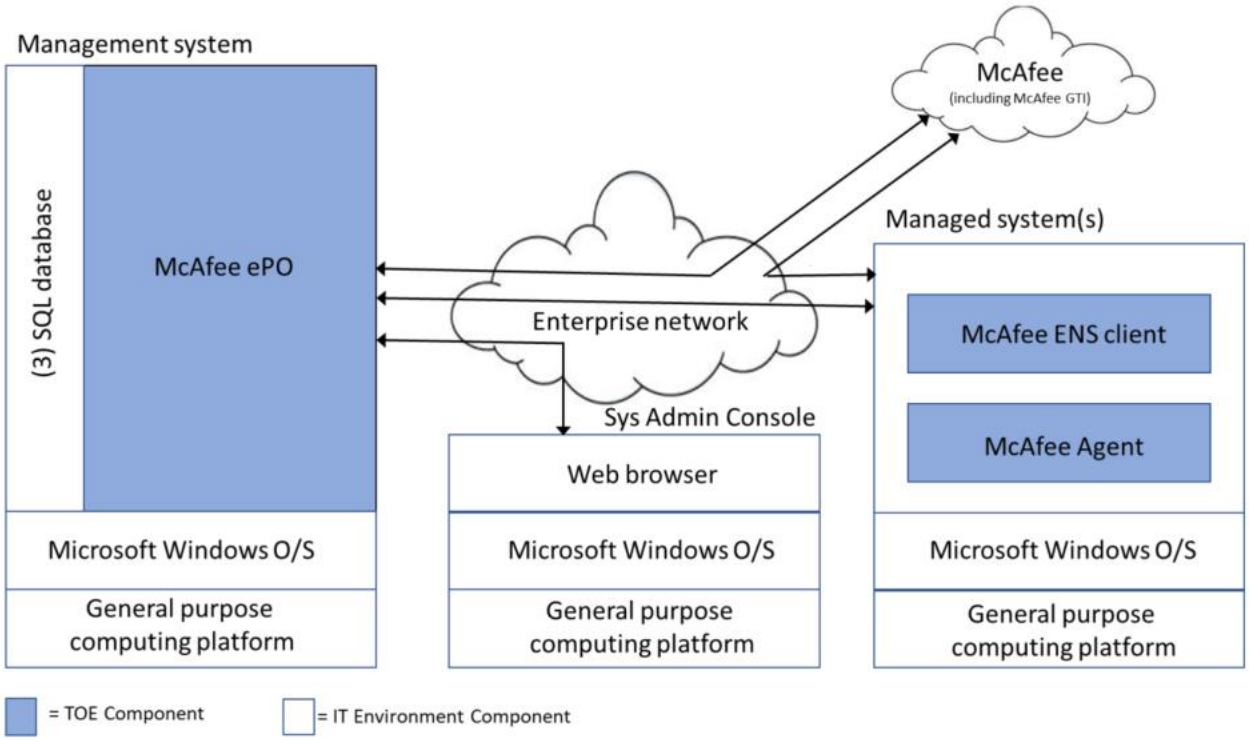

Figure 1: TOE Architecture

2 SECURITY POLICY

The TOE implements and enforces policies pertaining to the following security functionality:

- Security Audit
- Anti-Malware
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- Trusted Path

Complete details of the security functional requirements (SFRs) can be found in the Security Target (ST) referenced in section 8.2.

2.1 CRYPTOGRAPHIC FUNCTIONALITY

The following cryptographic implementations are used by the TOE and have been evaluated by the CAVP/CMVP:

Table 2: Cryptographic Implementation(s)

Cryptographic Module/Algorithm	Certificate Number
McAfee OpenSSL FIPS Object Module v1.0.2	CMVP 2969, CAVP A848
Bouncy Castle FIPS Java API 1.0.2.1	CMVP 3514, CAVP C2204
Windows 10 & Windows Server 2019 Cryptographic Primitives Library	CMVP 3197

3 ASSUMPTIONS AND CLARIFICATION OF SCOPE

Consumers of the TOE should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will ensure the proper and secure operation of the TOE.

3.1 USAGE AND ENVIRONMENTAL ASSUMPTIONS

The following assumptions are made regarding the use and deployment of the TOE:

- The TOE has access to all the IT System data it needs to perform its functions.
- The IT Environment will provide reliable timestamps for the TOE to use.
- The TOE will be managed in a manner that allows it to appropriately address changes in the IT systems the TOE monitors.
- McAfee GTI is present in the IT environment and can be accessed by the TOE.
- Managed computers will securely download reputation values for URLs and domains and safety ratings for websites in real-time through McAfee GTI.
- There will be one or more competent individuals assigned to administer the TOE and the security of the information it contains.
- The Administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
- The TOE, and hardware and software critical to security policy enforcement, will be protected from unauthorized physical modification.
- Management sessions will utilize HTTPS communication between the Administrator's web browser and the ePO web server to protect management session data.
- Administrators will implement secure mechanisms for receiving and validating updated threat information and TOE updates from McAfee, and for distributing the updates via the central management system.

3.2 CLARIFICATION OF SCOPE

The following functions are outside of the logical TOE scope and have not been evaluated:

- Cloud-based ePO deployments;
- ePO in a cluster environment;
- Remote database configuration;
- ePO Web API use; and
- Network IPS protection for Threat Prevention.

4 EVALUATED CONFIGURATION

The evaluated configuration for the TOE comprises:

TOE Software	• McAfee Endpoint Security 10.7.0 February 2022 Update, with the following extensions and installation packages:
	  ○ Platform 10.7.0.3255
	  ○ Platform Extension 10.7.0.1076
	  ○ Threat Prevention 10.7.0.3299
	  ○ Threat Prevention Extension 10.7.0.1248
	  ○ Firewall 10.7.0.2157
	  ○ Firewall Extension 10.7.0.1116
	  ○ Web Control 10.7.0.2581
	  ○ Web Control Extension 10.7.0.1162
	  ○ Adaptive Threat Protection 10.7.0.3437
	  ○ Adaptive Threat Protection Extension 10.7.0.1128
	  ○ Threat Detection Reporting Extension 1.0.0.7202
	• ePO Server 5.10.0 Refresh 6 (download package EPO_510_2428_68_LR6.zip), Update 13 (download package ePO_5.10.0_Update_13.zip)
	• McAfee Agent Version 5.7.5.504
	  ○ McAfee Agent Extension 5.7.5.54

Operating System	• ePO Server
	  ○ Microsoft Windows Server 2019
	• McAfee Agent and ENS Client
	  ○ Windows 10 21H2
	  ○ Windows Server 2019

Environmental Support	• ePO Server
	  ○ Microsoft SQL Server 2017
	  ○ Microsoft Visual C++ 2010 Redistributable Package (x64 and x86)
	  ○ Microsoft Visual C++ 2015 Redistributable Package (x64 and x86)
	  ○ MSXML 3.0 and 6.0

4.1 DOCUMENTATION

The following documents are provided to the consumer to assist in the configuration and installation of the TOE:

a) McAfee Endpoint Security 10.7.x Installation Guide, 2021-11-14
b) McAfee Endpoint Security 10.7.x Product Guide, 2021-11-14
c) McAfee ePolicy Orchestrator 5.10.0 Installation Guide, 2021-12-08
d) McAfee ePolicy Orchestrator 5.10.0 Product Guide, 2021-12-08
e) McAfee Agent 5.7.x Installation Guide, 2021-11-14
f) McAfee Agent 5.7.x Product Guide, 2021-11-14
g) McAfee Endpoint Security 10.7.x with ePolicy Orchestrator 5.10.x Common Criteria Evaluated Configuration Guide, Revision A, 2022-07-22

The TOE Guidance Documentation is also available online from docs.McAfee.com

5 EVALUATION ANALYSIS ACTIVITIES

The evaluation analysis activities involved a structured evaluation of the TOE. Documentation and process dealing with Development, Guidance Documents, and Life-Cycle Support were evaluated.

5.1 DEVELOPMENT

The evaluators analyzed the documentation provided by the vendor; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces and how the TSF implements the security functional requirements. The evaluators determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained.

5.2 GUIDANCE DOCUMENTS

The evaluators examined the TOE preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance and determined that they are complete and sufficiently detailed to result in a secure configuration.

Section 4.1 provides details on the guidance documents.

5.3 LIFE-CYCLE SUPPORT

An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the TOE configuration items were clearly marked.

The evaluators examined the delivery documentation and determined that it described all the procedures required to maintain the integrity of the TOE during distribution to the consumer.

6 TESTING ACTIVITIES

Testing consists of the following three steps: assessing developer tests, performing independent tests, and performing a vulnerability analysis.

6.1 ASSESSMENT OF DEVELOPER TESTS

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the Evaluation Test Report (ETR). The correspondence between the tests identified in the developer's test documentation and the functional specification was complete.

6.2 CONDUCT OF TESTING

The TOE was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

6.3 INDEPENDENT TESTING

During this evaluation, the evaluator developed independent functional & penetration tests by examining design and guidance documentation.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The following testing activities were performed:

a. Repeat of Developer's Tests: The evaluator repeated a subset of the developer's tests
b. Audit: The evaluator verified that the action of purging all audit records is audited.
c. Audit: The evaluator verified that a user without explicit permission cannot access audit records.
d. Access Control: The evaluator verified that policy configuration using the ENS Client was not available.
e. Access Control: The evaluator verified that user's permission changes take effect immediately.
f. Access Control: The evaluator confirmed that Web API interface requires authentication.
g. Secure Communication: The evaluator verified TLS cipher suites negotiated between ePO and Agent.
h. Secure Communication: The evaluator confirmed Agent checks ePO certificate.
i. Secure Communication: The evaluator verified that the TOE provides secure communication with remote administrators.

6.3.1 INDEPENDENT TESTING RESULTS

The developer's tests and the independent tests yielded the expected results, providing assurance that the TOE behaves as specified in its ST and functional specification.

6.4 VULNERABILITY ANALYSIS

The vulnerability analysis focused on 4 flaw hypotheses.

- Public Vulnerability based (Type 1)
- Technical community sources (Type 2)
- Evaluation team generated (Type 3)
- Tool Generated (Type 4)

The evaluators conducted an independent review of all evaluation evidence, public domain vulnerability databases and technical community sources (Type 1 & 2). Additionally, the evaluators used automated vulnerability scanning tools to discover potential network, platform, and application layer vulnerabilities (Type 4). Based upon this review, the evaluators formulated flaw hypotheses (Type 3), which they used in their vulnerability analysis.

Type 1 & 2 searches were conducted on **22 February 2022** and on **8 March 2022** included the following search terms:

ePO	ENS	ePolicy Orchestrator
McAfee Endpoint Security	McAfee Agent	Apache 2.4
Apache Tomcat 9	JRE 1.8.0	Java SE 8
log4j-core 2.17.1	Openssl 1.0.2	Bouncy Castle

Vulnerability searches were conducted using the following sources:

Common Vulnerabilities and Exposures (CVE) http://cve.mitre.org	Apache Tomcat 9.x Vulnerabilities https://tomcat.apache.org/security-9.html
Apache HTTP Server Project – 2.4 https://httpd.apache.org/security/vulnerabilities_24.html	OpenSSL Security Vulnerabilities https://www.openssl.org/news/vulnerabilities-1.0.2.html
McAfee Knowledge Center – Security Bulletins https://support.mcafee.com/webcenter/portal/supportportal/pages_knowledgecenter	

6.4.1 VULNERABILITY ANALYSIS RESULTS

The vulnerability analysis did not uncover any security relevant residual exploitable vulnerabilities in the intended operating environment.

7 RESULTS OF THE EVALUATION

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved testing laboratory established under the Canadian Centre for Cyber Security. This certification report, and its associated certificate, apply only to the specific version and release of the product in its evaluated configuration.

This evaluation has provided the basis for the conformance claim documented in Table 1. The overall verdict for this evaluation is **PASS**. These results are supported by evidence in the ETR.

7.1 RECOMMENDATIONS/COMMENTS

It is recommended that all guidance outlined in Section 4.1 be followed to configure the TOE in the evaluated configuration.

8 SUPPORTING CONTENT

8.1 LIST OF ABBREVIATIONS

Term	Definition
CAVP	Cryptographic Algorithm Validation Program
CCTL	Common Criteria Testing Laboratory
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITS	Information Technology Security
PP	Protection Profile
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

8.2 REFERENCES

Reference
Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.
Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 5, April 2017.
Security Target McAfee Endpoint Security 10.7.x with ePolicy Orchestrator 5.10.x, Document Version 1.0, July 22, 2022
Evaluation Technical Report for Common Criteria Evaluation of McAfee Endpoint Security 10.7.x with ePolicy Orchestrator 5.10.x, Version 1.2, 28 July 2022