Certification Report

McAfee Data Loss Prevention Endpoint 9.4 and ePolicy Orchestrator 5.1.3

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-342-CR
Version: 1.0
Date: 07 December 2015
Pagination: i to iii, 1 to 10

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved evaluation facility – established under the Canadian Common Criteria Evaluation and Certification Scheme (CCS) – using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4*. 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 CCS, and the conclusions of the evaluation facility 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 the Communications Security Establishment, 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 Communications Security Establishment, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

FOREWORD

The Canadian Common Criteria Evaluation and Certification Scheme (CCS) provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the CCS Certification Body, which is managed by the Communications Security Establishment.

A CCEF is a commercial facility that has been approved by the CCS Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of *ISO/IEC 17025:2005, the General Requirements for the Competence of Testing and Calibration Laboratories*. Accreditation is performed under the Program for the Accreditation of Laboratories - Canada (PALCAN), administered by the Standards Council of Canada.

The CCEF that carried out this evaluation is CGI IT Security Evaluation & Test Facility.

By awarding a Common Criteria certificate, the CCS 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, in order 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 CCEF.

This certification report is associated with the certificate of product evaluation dated 07 December 2015, and the security target identified in Section 4 of this report.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

TABLE OF CONTENTS

Executive Summary

McAfee Data Loss Prevention Endpoint 9.4 and ePolicy Orchestrator 5.1.3 (hereafter referred to as McAfee DLPe v9.4 with ePO v5.1.3), from Intel Corporation, is the Target of Evaluation. The results of this evaluation demonstrate that McAfee DLPe v9.4 with ePO v5.1.3 meets the requirements of Evaluation Assurance Level (EAL) 2 augmented for the evaluated security functionality.

McAfee DLPe v9.4 with ePO v5.1.3 protects enterprises from the risk associated with the unauthorized transfer of data from within the organization to the outside and is comprised of the following components:

- ePolicy Orchestrator (ePO): provides a platform for centralized policy management and enforcement of DLPe on the managed systems.
- DLPe Agents: reside on enterprise computers, which are referred to as managed computers, and enforce the DLP policies and rules defined in the DLP Policy Manager. The agents monitor user activities to record, control, and prevent unauthorized users from copying, printing, uploading to the internet or transferring corporate confidential data outside of the corporate network. The DLPe Agents also generate events that are recorded by the ePO.
- McAfee Agent: retrieves updates, runs client tasks, distributes policies, and forwards events from each managed system back to ePO.

The endpoint components integrate with the RSA BSAFE Crypto-C Micro Edition v4.0.1 to provide cryptographic services, while ePO integrates with OpenSSL v1.0.1m with FIPS module v2.0.8 for cryptographic services.

CGI IT Security Evaluation & Test Facility is the CCEF that conducted the evaluation. This evaluation was completed on 07 December 2015 and was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (CCS).

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for McAfee DLPe v9.4 with ePO v5.1.3, 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.

Communications Security Establishment, as the CCS Certification Body, declares that the McAfee DLPe v9.4 with ePO v5.1.3 evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this EAL 2+ evaluation is McAfee Data Loss Prevention Endpoint 9.4 and ePolicy Orchestrator 5.1.3 (hereafter referred to as McAfee DLPe v9.4 with ePO v5.1.3), from Intel Corporation.

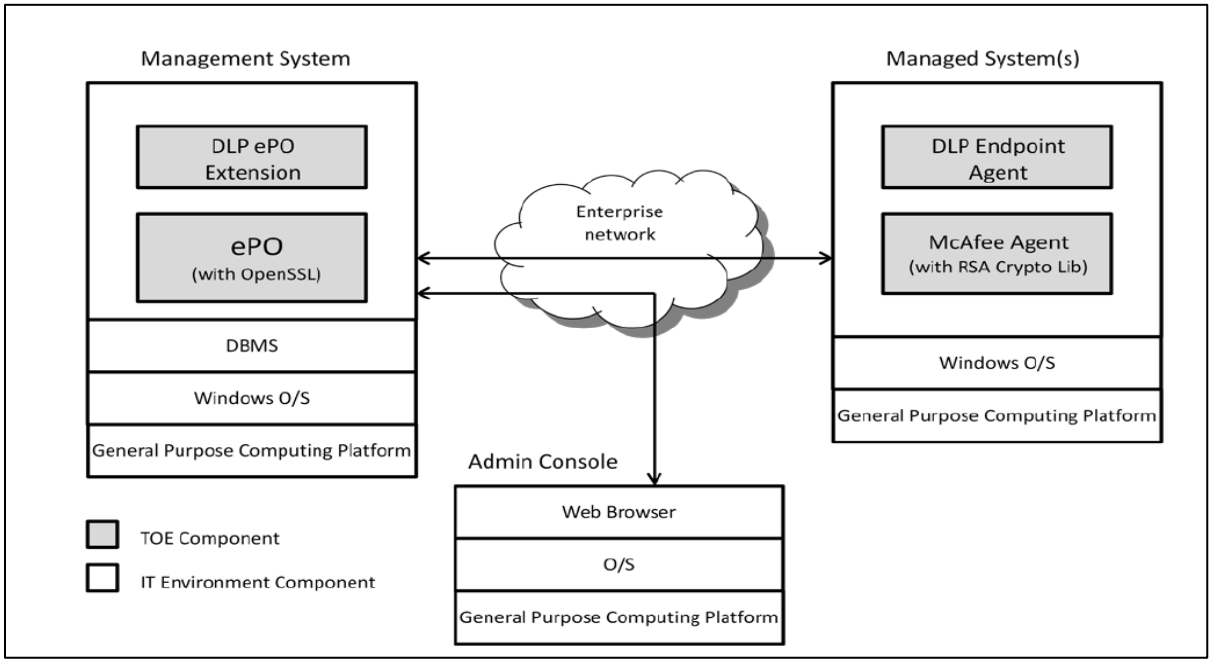
2 TOE Description

McAfee DLPe v9.4 with ePO v5.1.3 protects enterprises from the risk associated with the unauthorized transfer of data from within the organization to the outside and is comprised of the following components:

- ePolicy Orchestrator (ePO): provides a platform for centralized policy management and enforcement of DLPe on the managed systems.
- DLPe Agents: reside on enterprise computers, which are referred to as managed computers, and enforce the DLP policies and rules defined in the DLP Policy Manager. The agents monitor user activities to record, control, and prevent unauthorized users from copying, printing, uploading to the internet or transferring corporate confidential data outside of the corporate network. The DLPe Agents also generate events that are recorded by the ePO.
- McAfee Agent: retrieves updates, runs client tasks, distributes policies, and forwards events from each managed system back to ePO.

The endpoint components integrate with the RSA BSAFE Crypto-C Micro Edition v4.0.1 to provide cryptographic services, while ePO integrates with OpenSSL v1.0.1m with FIPS module v2.0.8 for cryptographic services.

A diagram of the McAfee DLP v9.4 with ePO v5.1.3 architecture is as follows:



3 Security Policy

McAfee DLPe v9.4 with ePO v5.1.3 implements a role-based access control policy to control administrative access to the system. In addition, McAfee DLPe v9.4 with ePO v5.1.3 implements policies pertaining to the following security functional classes:

- *Security Audit*
- *Cryptographic Support*
- *Information Flow Control*
- *Identification and Authentication*
- *Security Management*
- *Protection of the TOE Security Functionality (TSF)*

The following cryptographic modules were evaluated to the FIPS 140-2 standard:

Cryptographic Module	**Certificate**
OpenSSL v1.0.1m with FIPS module v2.0.8	1747
RSA BSAFE Crypto-C Micro Edition v4.0.1	2097

4 Security Target

The ST associated with this Certification Report is identified below:

McAfee Data Loss Prevention Endpoint 9.4 and ePolicy Orchestrator 5.1.3 Security Target, Version 1.0, November 24, 2015

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4.*

McAfee DLPe v9.4 with ePO v5.1.3 is:

a. EAL 2 augmented, containing all security assurance requirements listed, as well as the following:
   - *ALC_FLR.2 – Flaw Reporting Procedures*

b. Common Criteria Part 2 conformant; with security functional requirements based only upon functional components in Part 2;

c. Common Criteria Part 3 conformant, with security assurance requirements based only upon assurance components in Part 3.

6 Assumptions and Clarification of Scope

Consumers of McAfee DLPe v9.4 with ePO v5.1.3 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.

6.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- *The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.*
- *There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.*
- *The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.*

6.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- *The TOE has access to all the IT System data it needs to perform its functions.*
- *The TOE is appropriately scalable to the IT Systems the TOE monitors.*
- *Access to the database used by the TOE via mechanisms outside the TOE boundary is restricted to use by authorized users.*
- *The processing resources of the TOE server will be located within controlled access facilities, which will prevent unauthorized physical access.*
- *The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.*

7 Evaluated Configuration

The evaluated configuration for McAfee DLPe v9.4 with ePO v5.1.3 comprises the following:

- DLP ePO Extension 9.4.0.73 running on Windows Server 2008 R2
- DLP Endpoint Agent 9.4.0.532 running on Windows 7, Windows 2008 R2 Server, and Windows 2012 R2 Server
- ePolicy Orchestrator 5.1.3.188 running on Windows Server 2008 R2
- McAfee Agent 5.0.2.132 with MA ePO Server extension 5.0.2.118 running on Windows 7, Windows 2008 R2 Server, and Windows 2012 R2 Server

The publication entitled Common Criteria Evaluated Configuration Guide for McAfee Data Loss Prevention Endpoint 9.4 describes the procedures necessary to install and operate McAfee DLPe v9.4 with ePO v5.1.3 in its evaluated configuration.

8 Documentation

The Intel Corporation documents provided to the consumer are as follows:

a. McAfee Data Loss Prevention Endpoint 9.4 Product Guide

b. McAfee ePolicy Orchestrator 5.1.0 Software Installation Guide[1]

c. McAfee ePolicy Orchestrator 5.1.0 Software Product Guide

d. McAfee Agent 5.0.0 Product Guide[2]

e. Common Criteria Evaluated Configuration Guide for McAfee Data Loss Prevention Endpoint 9.4

f. Release Notes McAfee ePolicy Orchestrator 5.1.3

g. Release Notes McAfee Agent 5.0.2

[1] Guidance documents for ePO 5.1.0 apply equally to 5.1.3

[2] Guidance documents for McAfee Agent 5.0.0 apply equally to 5.0.2

9 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of McAfee DLPe v9.4 with ePO v5.1.3, including the following areas:

Development: The evaluators analyzed the McAfee DLPe v9.4 with ePO v5.1.3 functional specification and design documentation; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces, the TSF subsystems and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the McAfee DLPe v9.4 with ePO v5.1.3 security architectural description and determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the McAfee DLPe v9.4 with ePO v5.1.3 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.

Life-cycle support: An analysis of the McAfee DLPe v9.4 with ePO v5.1.3 configuration management system and associated documentation was performed. The evaluators found that the McAfee DLPe v9.4 with ePO v5.1.3 configuration items were clearly marked.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of McAfee DLPe v9.4 with ePO v5.1.3 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the McAfee DLPe v9.4 with ePO v5.1.3. During a site visit, the evaluators also examined the evidence generated by adherence to the procedures. The evaluators concluded that the procedures are adequate to track and correct security flaws, and distribute the flaw information and corrections to consumers of the product.

All these evaluation activities resulted in **PASS** verdicts.

10 ITS Product Testing

Testing consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

10.1 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 ETR[3].

The evaluators analyzed the developer's test coverage analysis and found it to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the functional specification was complete.

10.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional 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. Resulting from this test coverage approach is the following list of test goals:

a. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests;

b. ePO User Based Authentication: The objective of this test goal is to verify that the TOE will operate correctly utilizing the ePO local user to authenticate;

c. NT Domain System Data Import: The objective of this test goal is to ensure TOE is able to import system information from an NT Domain; and

d. Disable DLPe Ruleset: The objective of this test case to verify that an authorized user can disable a ruleset in the ePO and that the changes can be deployed to and enforced on the managed systems.

10.3 Independent Penetration Testing

Subsequent to the independent review of public domain vulnerability databases and all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on:

a. Use of automated vulnerability scanning tools to discover potential network, platform and application layer vulnerabilities; and

b. Session Management: The objective of this test goal is to attempt to access a closed Administrator's web session.

[3] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

The independent penetration testing did not uncover any exploitable vulnerabilities in the intended operating environment.

10.4 Conduct of Testing

McAfee DLPe v9.4 with ePO v5.1.3 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.

10.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, providing assurance that McAfee DLPe v9.4 with ePO v5.1.3 behaves as specified in its ST and functional specification.

11 Results of the Evaluation

This evaluation has provided the basis for a EAL 2+ level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

12 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
DLPe	McAfee Data Loss Prevention Endpoint
EAL	Evaluation Assurance Level
ePO	ePolicy Orchestrator
ETR	Evaluation Technical Report
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories - Canada
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

13 References

This section lists all documentation used as source material for this report:

a. CCS Publication #4, Technical Oversight, Version 1.8, October 2010.

b. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012.

d. McAfee Data Loss Prevention Endpoint 9.4 and ePolicy Orchestrator 5.1.3 Security Target, Version 1.0, November 24, 2015

e. McAfee Data Loss Prevention Endpoint 9.4 and ePolicy Orchestrator 5.1.3 Common Criteria EAL 2+ Evaluation Technical Report, Version 1.2, December 7, 2015.