Certification Report

McAfee File and Removable Media Protection 4.3.1 and ePolicy Orchestrator 5.1.2

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-277-CR
Version: 1.0
Date: 25 September 2015
Pagination: i to iii, 1 to 11

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 EWA-Canada.

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 25 September 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 File and Removable Media Protection 4.3.1 and ePolicy Orchestrator 5.1.2 (hereafter referred to as McAfee FRMP 4.3.1 and ePO 5.1.2), from Intel Corporation, is the Target of Evaluation. The results of this evaluation demonstrate that McAfee FRMP 4.3.1 and ePO 5.1.2 meets the requirements of Evaluation Assurance Level (EAL) 2 augmented for the evaluated security functionality.

McAfee FRMP 4.3.1 and ePO 5.1.2 is a file encryption product. The TOE allows selective control of access to data held in file systems and on removable media, based on user permissions. This protection depends on Microsoft Windows user accounts and works in real-time to authenticate the user, to access the encryption keys, and to retrieve the correct policy. The TOE acts as a Persistent Encryption engine. When a file is encrypted and is moved or copied to another location, it remains encrypted. If it is moved out of an encrypted directory, it still remains encrypted.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 25 September 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 FRMP 4.3.1 and ePO 5.1.2, 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 FRMP 4.3.1 and ePO 5.1.2 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).

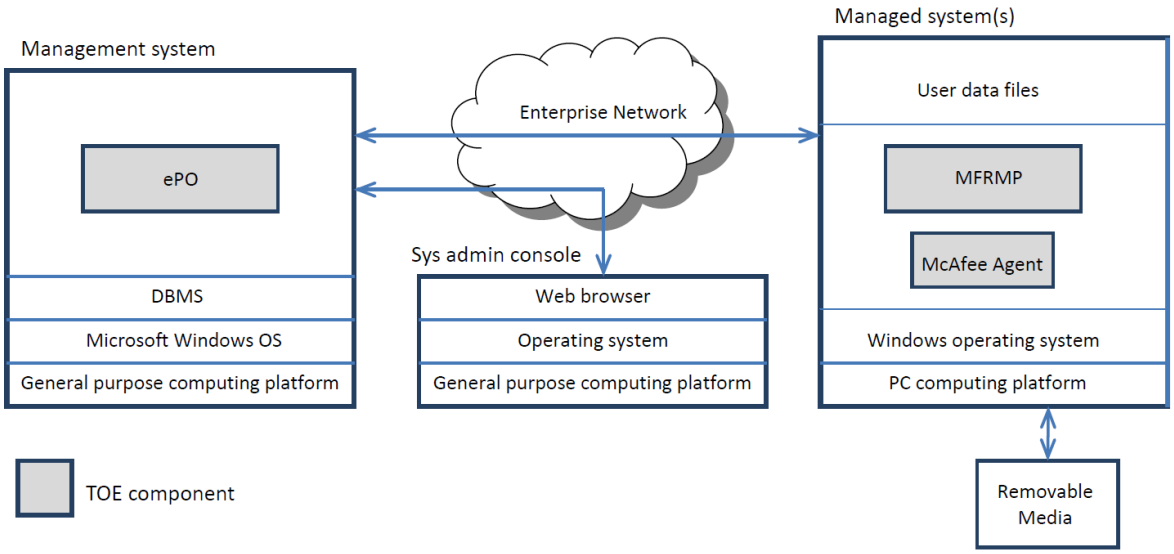
1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this EAL 2+ evaluation is McAfee File and Removable Media Protection 4.3.1 and ePolicy Orchestrator 5.1.2 (hereafter referred to as McAfee FRMP 4.3.1 and ePO 5.1.2), from Intel Corporation.

2 TOE Description

McAfee FRMP 4.3.1 and ePO 5.1.2 is a file encryption product. The TOE allows selective control of access to data held in file systems and on removable media, based on user permissions. This protection depends on Microsoft Windows user accounts and works in real-time to authenticate the user, to access the encryption keys, and to retrieve the correct policy. The TOE acts as a Persistent Encryption engine. When a file is encrypted and is moved or copied to another location, it remains encrypted. If it is moved out of an encrypted directory, it still remains encrypted.

A diagram of the McAfee FRMP 4.3.1 and ePO 5.1.2 architecture is as follows:



3 Security Policy

McAfee FRMP 4.3.1 and ePO 5.1.2 implements a role-based access control policy to control administrative access to the system. In addition, McAfee FRMP 4.3.1 and ePO 5.1.2 implements policies pertaining to the following security functional classes:

- Cryptographic support
- User data protection
- Security Management
- Identification and authentication
- Protection of the TSF

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

Cryptographic Module	**Certificate**
McAfee Core Cryptographic Module (user) (Software Version: 1.0)	*#2239*
McAfee Core Cryptographic Module (kernel) (Software Version: 1.0)	*#2223*
OpenSSL FIPS Object Module (Software Version: 1.2, 1.2.1, 1.2.2, 1.2.3 or 1.2.4)	*#1051*
RSA BSAFE® Crypto-C Micro Edition (Software Version: 4.0.1)	*#2097*

4 Security Target

The ST associated with this Certification Report is identified below:

Security Target McAfee File and Removable Media Protection 4.3.1 and ePolicy Orchestrator 5.1.2, Version 1.0, 6 September 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 FRMP 4.3.1 and ePO 5.1.2 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 extended; with functional requirements based upon functional components in Part 2, except for the following explicitly stated requirements defined in the ST:
    - FCS_RBG_EXT - Cryptographic operation: random bit generation
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 FRMP 4.3.1 and ePO 5.1.2 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:

- Authorized administrators will not leave the machine in a mode where sensitive information persists in non-volatile storage (e.g. power it down or enter a power managed state, such as a "hibernation mode").
- Authorized administrators are appropriately trained and follow all appropriate guidance documentation.
- An authorized administrator will be responsible for ensuring that passwords have sufficient strength and entropy to reflect the sensitivity of the data being protected.

6.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE will be installed on a platform that supports individual user identification and authentication.
- Authorized administrators will exercise due diligence in physically protecting the TOE, and will ensure that the IT environment will sufficiently protect against logical attacks.

6.3 Clarification of Scope

Two of the cryptographic modules used by the TOE (#1051, #2057) have been vendor affirmed as per I.G5 of the CMVP implementation guidance.

7 Evaluated Configuration

The evaluated configuration for McAfee FRMP 4.3.1 and ePO 5.1.2 comprises:

The TOE software;

- FRP 4.3.1.114
- McAfee Agent 5.0.0.2620

Installed on a managed system running one of the following operating systems:

- Windows 8.1 (32/64 bit)
- Windows 7 SP1 (32/64 bit)

And a server PC running the following;

- ePolicy Orchestrator 5.1.2.348 (also TOE software)
- Windows Server 2008 R2

With support from the following in the environment:

- Microsoft SQL Server 2008 R2, 2012
- LDAP server

The publication entitled Intel Security Common Criteria Evaluated Configuration Guide McAfee File and Removable Media Protection 4.3.1 With ePolicy Orchestrator 5.1.1, draft 150315 describes the procedures necessary to install and operate McAfee FRMP 4.3.1 and ePO 5.1.2 in its evaluated configuration.

8 Documentation

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

a. Intel Security Common Criteria Evaluated Configuration Guide McAfee File and Removable Media Protection 4.3.1 With ePolicy Orchestrator 5.1.1, draft 150315

b. Installation Guide McAfee ePolicy Orchestrator 5.1, Revision B, downloaded Nov 27, 2014

c. Product Guide McAfee ePolicy Orchestrator 5.1, Revision B, downloaded Nov 27, 2014

d. Product Guide McAfee File and Removable Media Protection (FRP) 4.3.0 For use with ePolicy Orchestrator 4.6.6, 4.6.7, 5.0.1, 5.1 Software, downloaded Nov 27, 2014; and

e. User Guide McAfee File and Removable Media Protection (FRP) 4.3.0 For use with ePolicy Orchestrator 4.6.6, 4.6.7, 5.0.1, 5.1 Software, downloaded Nov 27, 2014

9 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of McAfee FRMP 4.3.1 and ePO 5.1.2, including the following areas:

Development: The evaluators analyzed the McAfee FRMP 4.3.1 and ePO 5.1.2 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 FRMP 4.3.1 and ePO 5.1.2 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 FRMP 4.3.1 and ePO 5.1.2 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 FRMP 4.3.1 and ePO 5.1.2 configuration management system and associated documentation was performed. The evaluators found that the McAfee FRMP 4.3.1 and ePO 5.1.2 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 FRMP 4.3.1 and ePO 5.1.2 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the McAfee FRMP 4.3.1 and ePO 5.1.2. 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[1].

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. Agent uninstall: The objective of this test goal is to confirm that a user with or without admin privileges cannot uninstall the McAfee agent from their local workstation*;*

c. Key deletion: The objective of this test goal is to confirm that a user with the appropriate privileges to Create, Delete, Edit are unable to delete a regular key in the Active state; and

d. Concurrent administrators: The objective of this test goal is to confirm that changes made in McAfee ePO by two Administrators can be tracked.

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. Information Leakage Verification: The objective of this test goal is to attempt to capture sensitive information during start-up and shutdown of the TOE.

[1] 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 FRMP 4.3.1 and ePO 5.1.2 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 FRMP 4.3.1 and ePO 5.1.2 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
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. Security Target McAfee File and Removable Media Protection 4.3.1 and ePolicy Orchestrator 5.1.2, Version 1.0, 6 September 2015

e. Evaluation Technical Report for EAL 2+ Common Criteria Evaluation of McAfee Inc. McAfee File and Removable Media Protection 4.3.1 with ePolicy Orchestrator 5.1.2, version 1.0, 25 September 2015.