Certification Report

McAfee Policy Auditor 6.2 and McAfee ePolicy Orchestrator® 5.1.3

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number:	383-4-345-CR
Version:	1.0
Date:	8 December 2015
Pagination:	i to iii, 1 to 9

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 8 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).

This certification report makes reference to the following trademarks or registered trademark:

- ePolicy Orchestrator® is a registered trademark of Intel Corporation;

Reproduction of this report is authorized provided the report is reproduced in its entirety.

TABLE OF CONTENTS

Executive Summary

McAfee Policy Auditor 6.2 and McAfee ePolicy Orchestrator® 5.1.3 (hereafter referred to as McAfee PA 6.2 and EPO 5.1.3), from Intel Corporation, is the Target of Evaluation. The results of this evaluation demonstrate that McAfee PA 6.2 and EPO 5.1.3 meets the requirements of Evaluation Assurance Level (EAL) 2 augmented for the evaluated security functionality.

McAfee PA 6.2 EPO 5.1 is an agent-based, purpose-built IT policy audit solution that leverages security standards to automate the processes required for internal and external IT audits. McAfee Policy Auditor evaluates the status of managed systems relative to audits that contain benchmarks.

McAfee ePolicy Orchestrator® (ePO) provides the user interface for the TOE via a GUI accessed from remote systems using web browsers. The ePO web dashboard represents policy compliance by benchmark. Custom reports can be fully automated, scheduled, or exported. ePO requires user to identify and authenticate themselves before access is granted to any data or management functions. Audit records are generated to record configuration changes made by users. The audit records may be reviewed via the GUI

CGI IT Security Evaluation & Test Facility is the CCEF that conducted the evaluation. This evaluation was completed on 8 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 PA 6.2 and EPO 5.1.3, 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 PA 6.2 and EPO 5.1.3 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 Policy Auditor 6.2 and McAfee ePolicy Orchestrator® 5.1.3 (hereafter referred to as McAfee PA 6.2 and EPO 5.1.3), from Intel Corporation.

2 TOE Description

McAfee PA 6.2 EPO 5.1 is an agent-based, purpose-built IT policy audit solution that leverages security standards to automate the processes required for internal and external IT audits. McAfee Policy Auditor evaluates the status of managed systems relative to audits that contain benchmarks.

McAfee ePolicy Orchestrator® (ePO) provides the user interface for the TOE via a GUI accessed from remote systems using web browsers. The ePO web dashboard represents policy compliance by benchmark. Custom reports can be fully automated, scheduled, or exported. ePO requires user to identify and authenticate themselves before access is granted to any data or management functions. Audit records are generated to record configuration changes made by users. The audit records may be reviewed via the GUI.

A diagram of the McAfee PA 6.2 and EPO 5.1.3 architecture is as follows:

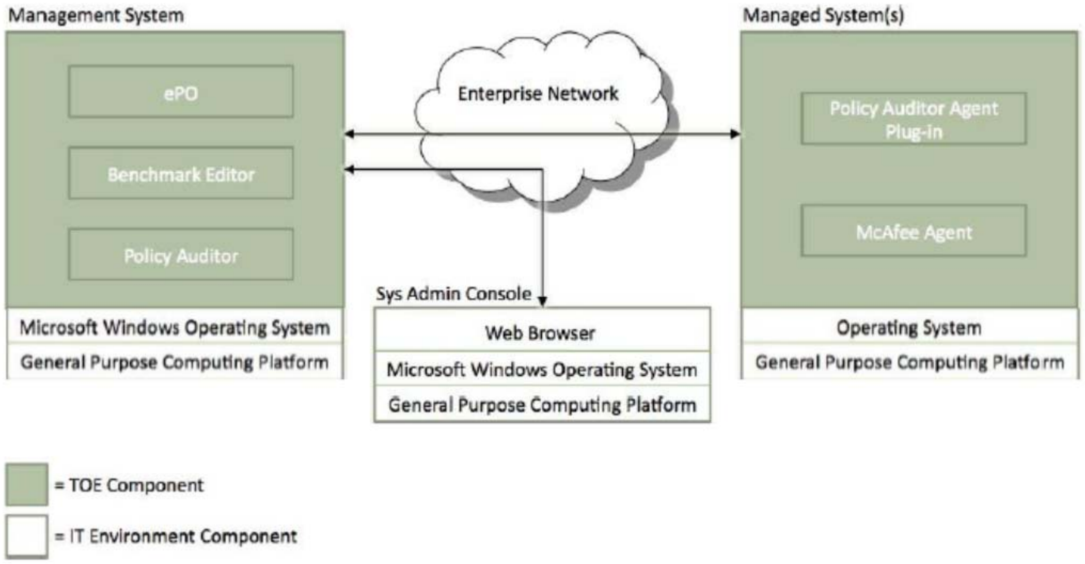
Management System
ePO
Benchmark Editor
Policy Auditor
Microsoft Windows Operating System
General Purpose Computing Platform
Enterprise Network
Sys Admin Console
Web Browser
Microsoft Windows Operating System
General Purpose Computing Platform
Managed System(s)
Policy Auditor Agent Plug-in
McAfee Agent
Operating System
General Purpose Computing Platform
= TOE Component
= IT Environment Component

Figure 1 – TOE Boundary

3 Security Policy

McAfee PA 6.2 and EPO 5.1.3 implements a role-based access control policy to control administrative access to the system. In addition, McAfee PA 6.2 and EPO 5.1.3 implements policies pertaining to the following security functional classes:

- *Security Audit;*
- *Cryptographic Support;*
- *Identification and Authentication;*
- *Security Management;*
- *Protection of TOE Security Functions; and*
- *TOE Access.*

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:

Security Target McAfee Policy Auditor 6.2 and McAfee ePolicy Orchestrator® 5.1.3, version 1.7, January 5, 2016.

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 PA 6.2 and EPO 5.1.3 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 extended; with functional requirements based upon functional components in Part 2, except for the following explicitly stated requirements defined in the ST:*

IDS_SDC - System Data Collection;

IDS_ANL - Analyzer Analysis;

IDS_RDR - Restricted Data Review; and

IDS_STG - Guarantee of Data Availability.

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 PA 6.2 and EPO 5.1.3 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:

- 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; and
- The TOE will be managed in a manner that allows it to appropriately address changes in the IT System it monitors.

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 is restricted to use by authorized users;
- The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access; and
- The TOE software critical to security policy enforcement, and the hardware on which it runs, will be protected from unauthorized physical modification.

7 Evaluated Configuration

The evaluated configuration for McAfee PA 6.2 and EPO 5.1.3 is software only and comprises:

- Policy auditor 6.2;
- Benchmark Editor 6.2; and
- ePolicy Orchestrator 5.1.3.

running on a Windows 2008 R2 with MS SQL Server 2008 R2,

and with the following agents:

- McAfee Policy Auditor Agent Plug-In 6.2; and
- McAfee Agent 5.0.2.

running on one of the following:

- Windows 2012 Server R2 (64 bit);
- Windows 2008 Server R2 (64 bit); and
- Windows 7 (64 bit).

The publication entitled McAfee Policy Auditor 6.2 and ePolicy Orchestrator 5.1.3 Operational User Guidance and Preparative Procedures Guidance Addendum v1.4 describes the procedures necessary to install and operate McAfee PA 6.2 and EPO 5.1.3 in its evaluated configuration.

8 Documentation

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

- McAfee Policy Auditor 6.2 Software Installation Guide;
- McAfee Policy Auditor 6.2 Software (Product Guide);
- Release Notes McAfee Policy Auditor 6.2.0;
- McAfee Benchmark Editor 6.2.0;
- Installation Guide Revision B McAfee ePolicy Orchestrator 5.1.0 Software;
- Product Guide Revision B McAfee ePolicy Orchestrator 5.1.0 Software;
- Best Practices Guide McAfee ePolicy Orchestrator 5.1.1 Software;
- McAfee Policy Auditor 6.2 and ePolicy Orchestrator 5.1.3 Operational User Guidance and Preparative Procedures Guidance Addendum v1.4;
- Release Notes McAfee ePolicy Orchestrator 5.1.3 Software;
- McAfee Agent Product Guide 5.0; and
- Release Notes McAfee Agent 5.0.2.

9 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of McAfee PA 6.2 and EPO 5.1.3, including the following areas:

Development: The evaluators analyzed the McAfee PA 6.2 and EPO 5.1.3 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 PA 6.2 and EPO 5.1.3 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 PA 6.2 and EPO 5.1.3 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 PA 6.2 and EPO 5.1.3 configuration management system and associated documentation was performed. The evaluators found that the McAfee PA 6.2 and EPO 5.1.3 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 PA 6.2 and EPO 5.1.3 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the McAfee PA 6.2 and EPO 5.1.3. 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[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. Audit Generation: The objective of this test goal is to confirm that the defined set of auditable events are generated;

c. Audit Protection: The objective of this test goal is to confirm the audit log is protected against unauthorized modification;

d. Permissions: The objective of this test goal is to confirm that an evaluator defined subset of permissions are correctly applied;

[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.

e. Management Functions: The objective of this test goal is to confirm that specified management functions are present;

f. SCAP: The objective of this test goal is to confirm SCAP (Security Content Automation Protocol) results;

g. System Data Collection: The objective of this test goal is to confirm that all details are included in collected data; and

h. Analyzer: The objective of this test goal is to confirm signature and scoring functionality in Analyzer.

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.

b. Port Scan: The objective of this test goal is to scan for open ports using nmap; and

c. OpenVAS Scan: The objective of this test goal is to determine if the TOE is vulnerable to Heartbleed, Poodle, Shellshock, Ghost or Freak.

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

10.4 Conduct of Testing

McAfee PA 6.2 and EPO 5.1.3 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 PA 6.2 and EPO 5.1.3 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 Evaluator Comments, Observations and Recommendations

While the administrator of the TOE is expected to familiarize themselves with all the TOE documents provided before they install and configure the TOE, the administrator should follow the procedures described in “McAfee Policy Auditor 6.2 and ePolicy Orchestrator 5.1.3 Operational User Guidance and Preparative Procedures Guidance Addendum v1.4” to ensure the TOE is installed and configured in its evaluated configuration.

The consumers of the TOE shall ensure the operational environment of the TOE uphold all assumptions that are specified in the section 3.3 of the ST.

13 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	McAfee ePolicy Orchestrator®
ETR	Evaluation Technical Report
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PA	Policy Auditor
PALCAN	Program for the Accreditation of Laboratories - Canada
SCAP	Security Content Automation Protocol
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

14 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 Policy Auditor 6.2 and McAfee ePolicy Orchestrator® 5.1.3, version 1.7, January 5, 2016.

e. Evaluation Technical Report McAfee Policy Auditor 6.2 and McAfee ePolicy Orchestrator® 5.1.3, version 1.1, January 7, 2016.