



Certification Report

EAL 2+ Evaluation of McAfee Host Data Loss Prevention 9.2 and ePolicy Orchestrator 4.6

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

© Government of Canada, Communications Security Establishment Canada, 2012

Document number: 383-4-171-CR
Version: 1.0
Date: 14 March 2012
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 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3*. This certification report, and its associated certificate, apply 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 Canada, 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 Canada, 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 Canada.

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 located in Ottawa, 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, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 14 March 2012, 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).

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

TABLE OF CONTENTS

Disclaimer i

Foreword..... ii

Executive Summary 1

1 Identification of Target of Evaluation..... 2

2 TOE Description 2

3 Evaluated Security Functionality 2

4 Security Target..... 2

5 Common Criteria Conformance..... 2

6 Security Policy 3

7 Assumptions and Clarification of Scope 3

 7.1 SECURE USAGE ASSUMPTIONS..... 3

 7.2 ENVIRONMENTAL ASSUMPTIONS 3

 7.3 CLARIFICATION OF SCOPE..... 4

8 Evaluated Configuration 4

9 Documentation 5

10 Evaluation Analysis Activities 5

11 ITS Product Testing..... 6

 11.1 ASSESSMENT OF DEVELOPER TESTS 6

 11.2 INDEPENDENT FUNCTIONAL TESTING 6

 11.3 INDEPENDENT PENETRATION TESTING..... 7

 11.4 CONDUCT OF TESTING 7

 11.5 TESTING RESULTS..... 7

12 Results of the Evaluation..... 8

13 Evaluator Comments, Observations and Recommendations 8

14 Acronyms, Abbreviations and Initializations..... 8

15 References..... 8

Executive Summary

McAfee Host Data Loss Prevention 9.2 and ePolicy Orchestrator 4.6 (hereafter referred to as McAfee HDLP), from McAfee, Inc., is the Target of Evaluation for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

McAfee HDLP is a Host based Data Loss Prevention product. It is a content-based agent solution that inspects enterprise users' actions concerning sensitive content in their own work environment, their computers. It protects enterprises from the risk associated with unauthorized transfer of data from within or outside the organization. It is a distributed software TOE that is composed of 4 components; ePO application, Host DLP monitor, McAfee agent, and HDLP agent.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 27 February 2012 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 HDLP, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security 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 results documented in the Evaluation Technical Report (ETR)¹ for this product provide sufficient evidence that it meets the EAL 2 augmented assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3*. The following augmentation is claimed: ALC_FLR.2 – Flaw Reporting Procedures.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the McAfee HDLP 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 The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 augmented evaluation is McAfee Host Data Loss Prevention 9.2 and ePolicy Orchestrator 4.6 (hereafter referred to as McAfee HDLP), from McAfee, Inc.

2 TOE Description

McAfee HDLP is a Host based Data Loss Prevention product. It is a content-based agent solution that inspects enterprise users' actions concerning sensitive content in their own work environment, their computers. It protects enterprises from the risk associated with unauthorized transfer of data from within or outside the organization. It is a distributed software TOE that is composed of 4 components; ePO application, Host DLP monitor, McAfee agent, and HDLP agent.

A detailed description of the McAfee HDLP architecture is found in Sections 1.6 and 1.7 of the Security Target (ST).

3 Evaluated Security Functionality

The complete list of evaluated security functionality for McAfee HDLP is identified in Sections 1 and 6.1 of the ST.

4 Security Target

The ST associated with this Certification Report is identified by the following nomenclature:

Title: Security Target: McAfee Host Data Loss Prevention 9.2 and ePolicy Orchestrator 4.6

Version: v1.0

Date: 21 February 2012

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3*.

McAfee HDLP is:

- a. *Common Criteria Part 2 conformant*, with security functional requirements based only upon functional components in Part 2;
- b. *Common Criteria Part 3 conformant*, with security assurance requirements based only upon assurance components in Part 3; and

- c. *Common Criteria EAL 2 augmented*, containing all security assurance requirements in the EAL 2 package, as well as the following: ALC_FLR.2 – Flaw Reporting Procedures

6 Security Policy

McAfee HDLP implements a role-based access control policy to control user access to the system, as well as an information flow control policy to control information entering the system; details of these security policies can be found in Section 7 of the ST.

In addition, McAfee HDLP implements policies pertaining to policy enforcement, security audit, identification and authentication, security management, and system information import. Further details on these security policies may be found in Section 7 of the ST.

7 Assumptions and Clarification of Scope

Consumers of McAfee HDLP 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.

7.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- The authorized administrators are neither careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the TOE documentation.
- 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.

7.2 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 hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
- The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
- Access to the database used by the TOE via mechanisms outside the TOE boundary is restricted to use by authorized users.

7.3 Clarification of Scope

McAfee HDLP offers protection against inadvertent or casual attempts to breach system security by unsophisticated attackers possessing basic attack potential. McAfee HDLP is not intended for situations which involve determined attempts by hostile or well-funded attackers using sophisticated attack techniques.

8 Evaluated Configuration

The evaluated configuration for McAfee HDLP comprises:

TOE Software

- Host DLP Monitor 9.2 Build 506
- HDLP Agent Plug-In 9.2 Build 522
- ePolicy Orchestrator 4.6.1 Build 1192
- McAfee Agent 4.62 Build 1694

The requirements for the IT environment are detailed in Section 1.7.2 of the ST.

The publication entitled: Operational User Guidance and Preparative Procedures Supplement: McAfee Host Data Loss Prevention 9.2 and ePolicy Orchestrator 4.6 describes the procedures necessary to install and operate McAfee HDLP in its evaluated configuration.

9 Documentation

The McAfee, Inc. documents provided to the consumer are as follows:

- a. Operational User Guidance and Preparative Procedures Supplement: McAfee Host Data Loss Prevention 9.2 and ePolicy Orchestrator 4.6;
- b. Installation Guide: McAfee® Data Loss Prevention 9.2 Software For Use with ePolicy Orchestrator® 4.6.0 Software;
- c. Product Guide: McAfee Data Loss Prevention 9.2 Software For Use with ePolicy Orchestrator® 4.6.0 Software; and
- d. Installation Guide McAfee ePolicy Orchestrator 4.6.0 Software.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of McAfee HDLP, including the following areas:

Development: The evaluators analyzed the McAfee HDLP 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 HDLP 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 HDLP 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 HDLP configuration management system and associated documentation was performed. The evaluators found that the McAfee HDLP configuration items were clearly marked. The developer's configuration management system was observed during a site visit, and it was found to be mature and well-developed.

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

The evaluators reviewed the flaw remediation procedures used by McAfee, Inc. for McAfee HDLP. 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 report, track and correct security flaws, and distribute the flaw information and corrections to consumers of the product.

Vulnerability assessment: The evaluators conducted an independent vulnerability analysis of McAfee HDLP. Additionally, the evaluators conducted a search of public domain vulnerability databases to identify McAfee HDLP potential vulnerabilities. The evaluators identified potential vulnerabilities for testing applicable to McAfee HDLP in its operational environment.

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

11 ITS Product Testing

Testing at EAL 2 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

11.1 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 ETR².

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.

11.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation, examining the developer's test documentation, executing a sample of the developer's test cases, and creating test cases that augmented the developer tests.

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 EWA-Canada test goals:

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

² The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

- b. Agent Installation: The objective of this test goal is to verify the HDLP server can push an agent install to a host on the network;
- c. Policy creation/enforcement: The objective of this test goal is to verify that the TOE can create/enforce protection rules for file systems and removable storage used by host machines; and
- d. Identification and Authentication: The objective of this test goal is to verify that strong passwords can be used by the TOE.

11.3 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. Search of public domain security sites to determine if there are any known or potential vulnerabilities that could be exploited;
- b. Attempting to bypass host agent polices by an end user;
- c. Initiating a connection failure to avoid rule/policy enforcement; and
- d. Attempt to cause a buffer overflow using authentication credentials.

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

11.4 Conduct of Testing

McAfee HDLP was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the Information Technology Security Evaluation and Test (ITSET) Facility at EWA-Canada. The CCS Certification Body witnessed a portion of the independent testing. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

11.5 Testing Results

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

12 Results of the Evaluation

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

13 Evaluator Comments, Observations and Recommendations

The TOE comes with a complete set of easy to follow guidance documentation.

14 Acronyms, Abbreviations and Initializations

<u>Acronym/Abbreviation/ Initialization</u>	<u>Description</u>
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
DLP	Data Loss Prevention
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
MLOS	McAfee Linux Operating System
PALCAN	Program for the Accreditation of Laboratories - Canada
ST	Security Target
TOE	Target of Evaluation

15 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 3, July 2009.
- c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 3, July 2009.
- d. Security Target: McAfee Host Data Loss Prevention 9.2 and ePolicy Orchestrator 4.6, v1.0, 21 February 2012.
- e. Evaluation Technical Report for EAL 2+ Common Criteria Evaluation of McAfee, Inc. McAfee Host Data Loss Prevention 9.2 and ePolicy Orchestrator 4.6, v1.3, 21 February 2012.