Certification Report

EAL 2+ Evaluation of McAfee® Deep Defender™ 1.0.1 and ePolicy Orchestrator 4.6.1

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number:	383-4-220-CR
Version:	1.0
Date:	12 October 2012
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 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, Ontario.

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 12 October 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).

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

- McAfee® is a registered trademark of McAfee, Inc.

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

TABLE OF CONTENTS

Executive Summary

McAfee® Deep Defender™ 1.0.1 and ePolicy Orchestrator 4.6.1 (hereafter referred to as MDD), from McAfee, Inc., is the Target of Evaluation for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

MDD is a software package designed to protect Microsoft Windows-based desktop computers from unwanted code and programs, specifically root kits. MDD monitors the memory and CPU registers:

- Protecting against loading of known hostile code, and

- Preventing access to protected areas.

The CPU is responsible for controlling access between User Mode and Kernel Mode components and, with part of the MDD solution residing under the kernel, MDD is able to monitor and control access to kernel memory, preventing the loading of known hostile code, and protecting unauthorized access to memory locations that require protection. Known malicious code and new attack agents can be identified, reported and removed.

The management capabilities for MDD are provided by the ePolicy Orchestrator (ePO). ePO manages McAfee Agents and MDD software that reside on client systems. By using ePO a large enterprise network can be managed from a centralized system. ePO also provides scheduling capabilities to distribute updated MDD security policies and signature files, and maintains audit files.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 1 October 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 MDD, the security requirements, and the level of confidence (evaluation assurance level) to which it is asserted that the product satisfies its 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

[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.

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 augmentations are claimed: ALC_FLR.2 – Flaw Reporting Procedures

Communications Security Establishment Canada, as the CCS Certification Body, declares that the MDD 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 Evaluation Assurance Level (EAL) 2 augmented evaluation is McAfee® Deep Defender™ 1.0.1 and ePolicy Orchestrator 4.6.1 (hereafter referred to as MDD), from McAfee, Inc.

2 TOE Description

MDD is a software package designed to protect Microsoft Windows-based desktop computers from unwanted code and programs, specifically root kits. MDD monitors the memory and CPU registers:

- Protecting against loading of known hostile code, and

- Preventing access to protected areas.

The CPU is responsible for controlling access between User Mode and Kernel Mode components and, with part of the MDD solution residing under the kernel, MDD is able to monitor and control access to kernel memory, preventing the loading of known hostile code, and protecting unauthorized access to memory locations that require protection. Known malicious code and new attack agents can be identified, reported and removed.

The management capabilities for MDD are provided by the ePolicy Orchestrator (ePO). ePO manages McAfee Agents and MDD software that reside on client systems. By using ePO a large enterprise network can be managed from a centralized system. ePO also provides scheduling capabilities to distribute updated MDD security policies and signature files, and maintains audit files.

A detailed description of the MDD architecture is found in Section 1.7 of the Security Target (ST).

3 Evaluated Security Functionality

The complete list of evaluated security functionality for MDD is identified in Section 1.7 of the ST.

4 Security Target

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

Title: Security Target McAfee Deep Defender 1.0.1 and ePolicy Orchestrator 4.6.1
Version: 1.0

Date: 1 October 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.*

MDD is:

a. *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:
   - FAM_SCN_(EXT).1 Anti-malware scanning and
   - FAM_ALR_(EXT).1 Anti-malware alerts

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

MDD 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 7.3 of the ST.

In addition, MDD implements policies pertaining to security audit, malicious code identification and alerts, identification and authentication, and security management. Further details on these security policies may be found in Section 7 of the ST.

7 Assumptions and Clarification of Scope

Consumers of MDD 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:

- Administrators will back up audit files and monitor disk usage to ensure audit information is not lost.

- Administrators are non-hostile, appropriately trained, and follow all administrative guidance.

- Administrators will implement secure mechanisms for receiving and validating updated signature files from McAfee, and for distributing the updates to the central management systems.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The appropriate physical security is provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.

- The IT environment will provide a secure line of communications between distributed portions of the TOE and between the TOE and remote administrators.

- The hardware platform used for ePO will not be used to host other applications.

7.3 Clarification of Scope

MDD offers protection against inadvertent or casual attempts to breach system security by unsophisticated attackers possessing basic attack potential. The MDD 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 MDD comprises:

For the EPO;

Processor	Intel Pentium 4-class ; 1.3 GHz
Memory	4 GB RAM
Operating System	Windows Server 2003 Enterprise with SP2 Windows Server 2003 Standard with SP2 Windows Server 2003 Datacenter with SP2 Windows Server 2008 R2 Enterprise Windows Server 2008 R2 Standard Windows Server 2008 R2 Datacenter Windows Server 2008 Enterprise with SP2 Windows Server 2008 Standard with SP2 Windows Server 2008 Datacenter with SP2 Windows 2008 Small Business Server
DBMS	SQL Server 2005 with SP3 SQL 2008 Express with SP1 SQL 2008 Standard with SP2

	SQL 2008 R2 Work Group Edition
Additional Software	RSA Crypto-C ME 2.0 RSA Crypto-J 4.0

For the MDD and Client;

Processor	Intel i3, i5 or i7 (Intel VT must be enabled in BIOS)
Memory	2GB (32-bit, 4GB (64-bit)
Free Disk Space	240 MB
Browser	Microsoft Internet Explorer version 7.0 or 8.0
Operating System	Microsoft Windows 7 Home Premium, Professional, Enterprise or Ultimate (32 and 64 bit) inc SP1

The publication entitled Common Criteria Evaluated Configuration Guide McAfee® Deep Defender 1.0.1 Software for use with ePolicy Orchestrator 4.6.1 describes the procedures necessary to install and operate MDD in its evaluated configuration.

9 Documentation

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

a. Common Criteria Evaluated Configuration Guide McAfee® Deep Defender 1.0.1 Software for use with ePolicy Orchestrator 4.6.1;

b. McAfee Deep Defender 1.0.1 Product Guide;

c. Installation Guide McAfee® ePolicy Orchestrator® 4.6.0 Software; and

d. Product Guide McAfee® ePolicy Orchestrator® 4.6.0 Software.

10 Evaluation Analysis Activities

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

Development: The evaluators analyzed the MDD 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 MDD 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 MDD 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 MDD configuration management system and associated documentation was performed. The evaluators found that the MDD 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 MDD during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by McAfee, Inc. for the MDD. 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.

Vulnerability assessment: The evaluators conducted an independent vulnerability analysis of MDD. Additionally, the evaluators conducted a search of public domain vulnerability databases to identify MDD potential vulnerabilities. The evaluators identified potential vulnerabilities for testing applicable to MDD 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 ETR[2].

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;

b. Review of log entries: The objective of this test goal is to confirm that new entries are created in the audit log for the independent test activities;

c. Creation, assignment and enforcement of new permission sets: The objective of this test goal is to test the creation, assignment and enforcement of new permission sets;

d. Concurrent users: The objective of this test goal is to test the effects of concurrent users on the TOE;

e. Creation and enforcement of blacklist/white list policies: The objective of this test goal is to test the creation and enforcement of blacklist/whitelist policies; and

[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.

f. Disabling/bypassing the TOE: The objective of this test goal is to determine the effects of bypassing/disabling 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. Port Scan: The objective of this test goal is to scan the TOE using a port scanner;

b. Vulnerability Identification: Tool Scanning: The objective of this test goal is to scan the TOE for vulnerabilities using automated tools; and

c. Information Leakage Verification: The objective of this test goal is to monitor the TOE for leakage during start-up, shutdown, login, and other scenarios using a packet sniffer.

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

11.4 Conduct of Testing

MDD 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 MDD 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 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
ETR	Evaluation Technical Report
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories - Canada
ST	Security Target
TOE	Target of Evaluation

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 3, July 2009.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 3, July 2009.

d. Security Target McAfee Deep Defender 1.0.1 and ePolicy Orchestrator 4.6.1, 1.0, 1 October 2012.

e. Evaluation Technical Report for EAL 2+ Common Criteria Evaluation of McAfee, Inc. McAfee Deep Defender 1.0.1 and ePolicy Orchestrator 4.6.1 Version 1.2, 1 October 2012.