Certification Report

EAL 3+ Evaluation of McAfee Application Control v5.0, Change Control v5.0, and Integrity Monitor v5.0 with McAfee Agent v4.5 and ePolicy Orchestrator v4.5

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Evaluation number:	383-4-153-CR
Version:	1.0
Date:	14 January 2011
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 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, 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 14 January 2011, 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 registered trademark:

- Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

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

TABLE OF CONTENTS

Executive Summary

McAfee Application Control v5.0, Change Control v5.0, and Integrity Monitor v5.0 with McAfee Agent v4.5 and ePolicy Orchestrator v4.5 (hereafter referred to as McAfee AC, CC & IM with Agent & ePO), from McAfee, Incorporated, is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 3 augmented evaluation.

McAfee AC, CC, & IM with Agent & ePO provides application control, change control, and integrity monitoring of servers, desktops, network devices, and databases. It does this by collecting information about the program code, files, directories, and volumes that are to be protected. Each time a program attempts to execute, or a process or user attempts to modify a protected resource, the TOE analyzes the attempted action and determines whether the action should be permitted.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 16 December 2010 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 the McAfee AC, CC, & IM with Agent & ePO, 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)[i] for this product provide sufficient evidence that it meets the EAL 3 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 AC, CC, & IM with Agent & ePO 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) 3 augmented evaluation is McAfee Application Control v5.0, Change Control v5.0, and Integrity Monitor v5.0 with McAfee Agent v4.5 and ePolicy Orchestrator v4.5 (hereafter referred to as McAfee AC, CC, & IM with Agent & ePO), from McAfee, Incorporated.

2 TOE Description

McAfee AC, CC, & IM with Agent & ePO provides application control, change control, and integrity monitoring of servers, desktops, network devices, and databases. It does this by collecting information about the program code, files, directories, and volumes that are to be protected. Each time a program attempts to execute, or a process or user attempts to modify a protected resource, the TOE analyzes the attempted action and determines whether the action should be permitted.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for McAfee AC, CC, & IM with Agent & ePO is identified in Section 1.5.2 of the Security Target (ST).

The following cryptographic module is included in the TOE and was evaluated to the FIPS 140-2 standard:

Cryptographic Module	Certificate #
RSA BSAFE Crypto-C Micro Edition v2.0	608

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in McAfee AC, CC, & IM with Agent & ePO:

Cryptographic Algorithm	Standard	Certificate #
Digital Signature Verification (DSA)	FIPS 186-2	143
Triple-DES (3DES)	FIPS 46-3	378
Advanced Encryption Standard (AES)	FIPS 197	303
Rivest Shamir Adleman (RSA)	FIPS 186-2	96
Secure Hash Algorithm (SHA-1)	FIPS 180-2	380
Keyed-Hash Message Authentication Code (HMAC)	FIPS 198	113

4 Security Target

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

Title: McAfee Application Control v5.0, Change Control v5.0, and Integrity Monitor v5.0
with McAfee Agent v4.5 and ePolicy Orchestrator v4.5 Security Target
Version: 0.6
Date: 14 December 2010

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*.

The McAfee AC, CC, & IM with Agent & ePO is:

a. *Common Criteria Part 2 extended*, with security functional requirements based upon functional components in Part 2, except for the following explicitly stated requirements defined in the ST: EXT_MAC_SDC.1 - Application and Change Control Data Collection; EXT_MAC_ANL.1 - Application and Change Control Analysis; and EXT_MAC_RCT.1 - Application and Change Control React.

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

c. *Common Criteria EAL 3 augmented*, with all the security assurance requirements in the EAL 3, as well as the following: ALC_FLR.2 - Flaw Reporting Procedures.

6 Security Policy

McAfee AC, CC, & IM with Agent & ePO implements policies pertaining to Security Audit, Cryptographic Support, Identification and Authentication, Security Management, Protection of the TOE Security Functions, and McAfee Application and Change Control. Further details on these security policies may be found in Section 6 (Security Requirements) of the ST.

7 Assumptions and Clarification of Scope

Consumers of the McAfee AC, CC, & IM with Agent & ePO product 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:

- 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 the TOE monitors.

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 IT Environment will provide reliable timestamps for the use of the TOE;
- The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access; and
- The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

7.3 Clarification of Scope

The McAfee AC, CC, & IM with Agent & ePO is suitable for use in well-protected environments; it is not intended for environments in which attackers use sophisticated attacks.

8 Evaluated Configuration

The evaluated configuration for McAfee AC, CC, & IM with Agent & ePO comprises:

- McAfee Application Control v5.0, Change Control v5.0, Integrity Monitor v5.0, and McAfee Agent v4.5 running on Windows 2000, Windows XP, Windows Vista, Windows NT Server, Windows Server 2000, Windows Server 2003, or Windows Server 2008; and
- ePolicy Orchestrator v4.5 running with Microsoft SQL Server 2005 on Windows Server 2003 or Windows Server 2008.

9 Documentation

The McAfee documents provided to the consumer are as follows:

McAfee ePolicy Orchestrator 4.5 Product Guide;

McAfee ePolicy Orchestrator 4.5 Evaluation Guide;

McAfee ePolicy Orchestrator 4.5 Installation Guide;

McAfee ePolicy Orchestrator 4.5 Reporting Guide;

McAfee ePolicy Orchestrator 4.5 Log Files Reference Guide;

Release Notes for McAfee ePolicy Orchestrator 4.5;

McAfee Application Control Quick Start Guide for use with ePO 4.0 and 4.5;

McAfee Change Control Quick Start Guide for use with ePO 4.0 and 4.5;

McAfee Integrity Monitor Quick Start Guide for use with ePO 4.0 and 4.5;

McAfee Solidcore Extension Installation Guide 5.0.0 for use with ePO 4.0 and 4.5;

McAfee Solidcore Extension Product Guide for use with ePO 4.0 and 4.5;

Release Notes for McAfee Solidcore Extension 5.0.0;

Solidcore S3 Control Solidifier User's Guide;

Solidcore S3 Control Solidifier for Windows Runtime Control User's Guide;

Solidcore S3 Control Solidifier for Windows Installation Guide; and

Solidcore S3 Control Solidifier for Windows 5.0 Release Notes.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the McAfee AC, CC, & IM with Agent & ePO, including the following areas:

Development: The evaluators analyzed the McAfee AC, CC, & IM with Agent & ePO 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 AC, CC, & IM with Agent & ePO security architectural description and determined that the initialization process was secure and that the security functions are protected against tamper and bypass. The evaluators also independently verified that the correspondence mappings between the design documents were correct.

Guidance Documents: The evaluators examined the McAfee AC, CC, & IM with Agent & ePO preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously described 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 were complete and sufficiently detailed to result in a secure configuration.

Life-Cycle Support: An analysis of the McAfee AC, CC, & IM with Agent & ePO configuration management system and associated documentation was performed. The evaluators found that the McAfee AC, CC, & IM with Agent & ePO configuration items were clearly marked and that the access control measures as described in the configuration management documentation are effective in preventing unauthorized access to the configuration items. The developer's configuration management system was also observed during the site visit, and it was found to be mature and well developed.

During the site visit the evaluator examined the development security procedures and determined that they detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the McAfee AC, CC, & IM with Agent & ePO design and implementation. The evaluator confirmed that the developer used a documented model of the TOE life-cycle and that the life-cycle model provides for the necessary control over the development and maintenance of the TOE.

The evaluator examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of McAfee AC, CC, & IM with Agent & ePO during distribution to the consumer.

The evaluator reviewed the flaw remediation procedures used by McAfee, Incorporated for McAfee AC, CC, & IM with Agent & ePO. During a site visit, the evaluator examined the evidence generated by adherence to the procedures. The evaluator 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 McAfee AC, CC, & IM with Agent & ePO. Additionally, the evaluators conducted a review of public domain vulnerability databases, and a search of all evaluation deliverables. The evaluators identified potential vulnerabilities for testing applicable to the McAfee AC, CC, & IM with Agent & ePO in its operational environment.

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

11 ITS Product Testing

Testing at EAL 3 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.

The evaluators analyzed the developer’s test coverage and depth analysis and found them to be complete and accurate. The correspondence between the tests identified in the developer’s test documentation and the functional specification and TOE design 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:

- Initialization: The objective of this test goal is to confirm that the TOE can be installed and configured into the evaluated configuration following the guidance provided with the product;

- Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests on the evaluator’s TOE installation;

- Endpoint setup: The objective of this test goal is to use the ePO Orchestrator to create groups, add workstations to these groups, and push the agent installation out to the workstations;

- Application control alert: The objective of this test goal is to verify policy enforcement on endpoints and ePolicy alert handling of policy circumventing;

- Application code modification alert: The objective of this test goal is to verify policy enforcement on endpoints for executable file protection and ePolicy alert handling of policy circumventing;

- Dashboard event reporting: The objective of this test goal is to verify events are registered and sent to the Dashboard;

- Application run control: The objective of this test goal is to use the ePO Orchestrator to create and enforce an application run control policy;

- Change control test: The objective of this test goal is to use the ePO Orchestrator to create change control rules that disallow editing key files;

- Integrity monitor: The objective of this test goal is to use the ePO Orchestrator to add integrity monitoring and reporting on the C:\temp folder of the agent workstation;

- Show agent log: The objective of this test goal is to enable audit logging from the client endpoint to be visible at the ePO management console; and

- Secure communications: The objective of this test goal is to determine that communications are encrypted.

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:

- Misuse: The objectives of these tests were to determine that the TOE continues to operate when a communications failure occurs and that duplicate user names could not be created.

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

11.4 Conduct of Testing

McAfee AC, CC & IM + Agent and ePO was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the McAfee development site and at the Information Technology Security Evaluation and Testing (ITSET) Facility at EWA-Canada. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Procedures and Test Results document.

11.5 Testing Results

The developer’s tests and the independent functional tests yielded the expected results, giving assurance that the McAfee AC, CC, & IM with Agent & ePO behaves as specified in its ST, functional specification, TOE design, and security architecture description.

12 Results of the Evaluation

This evaluation has provided the basis for an EAL 3+ 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 complete documentation for the McAfee AC, CC, & IM with Agent & ePO includes comprehensive Evaluation, Installation, and Users Guides with searchable context-sensitive Help available to the user from the user console.

McAfee AC, CC, & IM with Agent & ePO is straightforward to configure, use and integrate into a corporate network.

14 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
AC	Application Control
CC	Change Control
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
EAL	Evaluation Assurance Level
ePO	ePolicy Orchestrator
ETR	Evaluation Technical Report
IM	Integrity Monitor
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories Canada
ST	Security Target
SQL	Structured Query Language
TOE	Target of Evaluation
TSF	TOE Security Functionality

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. McAfee Application Control v5.0, Change Control v5.0, and Integrity Monitor v5.0 with McAfee Agent v4.5 and ePolicy Orchestrator v4.5 Security Target, Revision No. 0.6, 14 December 2010.

e. Evaluation Technical Report (ETR) McAfee Application Control v5.0, Change Control v5.0, and Integrity Monitor v5.0 with McAfee Agent v4.5 and ePolicy Orchestrator v4.5, EAL 3+ Evaluation, Common Criteria Evaluation Number: 383-4-153, Document No. 1657-000-D002, Version 1.3, 16 December 2010.

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