Communications Security Establishment
Centre de la sécurité des télécommunications

COMMON CRITERIA CERTIFICATION REPORT

McAfee Change Control and Application Control 7.0.0 with ePolicy Orchestrator 5.3.2

383-4-408

5 October 2016

v1.0

Canada

FOREWORD

This certification report is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE). Suggestions for amendments should be forwarded through departmental communications security channels to your Client Services Representative at CSE.

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 Scheme – 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 Canadian CC Scheme, 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.

If your department has identified a requirement for this certification report based on business needs and would like more detailed information, please contact:

ITS Client Services
Telephone: (613) 991-7654
E-mail: itsclientservices@cse-cst.gc.ca

OVERVIEW

The Canadian Common Criteria Scheme 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 Certification Body, which is managed by the Communications Security Establishment.

A CCEF is a commercial facility that has been approved by the 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 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.

The certification report, certificate of product evaluation and security target are posted to the Certified Products list (CPL) for the Canadian CC Scheme, and to the Common Criteria portal (the official website of the International Common Criteria Project).

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

McAfee Change Control and Application Control 7.0.0 with ePolicy Orchestrator 5.3.2 (hereafter referred to as the Target of Evaluation, or TOE), from Intel Corporation, was the subject of this Common Criteria evaluation. The results of this evaluation demonstrate that TOE meets the requirements of the conformance claim listed in Table 1 for the evaluated security functionality.

The TOE provides change control and monitoring on servers and desktops. It also ensures that only authorized code can run on those managed systems. This functionality is managed through the ePolicy Orchestrator (ePO) management software.

The product consists of four logical components:

- Change Control (monitors changes happening on managed systems);
- Application Control (prevents unauthorized execution of program code);
- ePO (for remote management of Change Control and Application Control); and
- McAfee Agent.

The four logical components are implemented via four physical software components:

- Solidcore Service – Manages the policy for the Filesystem Driver and interfaces with the CLI and McAfee Agent.
- Filesystem Driver (swin.sys) – The portion of the product implemented in the Operating System's (OS) kernel space; the filesystem driver intercepts and analyzes all file system, registry, memory, and other critical reads and writes occurring in the OS and implements the core application control and change control and monitoring actions.
- ePO – Used for remote management of the Solidcore Service.
- McAfee Agent – A generic agent used by ePO for communication with a managed endpoint. The agent distributes policies from and reports back to ePO.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 05 October 2016 and was carried out in accordance with the rules of the Canadian Common Criteria Scheme.

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for TOE, 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 Certification Body, declares that the TOE evaluation meets all the conditions of the Arrangement on the Recognition of Common Criteria Certificates and that the product will be listed on the Certified Products list (CPL) and the Common Criteria portal (the official website of the International Common Criteria Project).

1 IDENTIFICATION OF TARGET OF EVALUATION

The Target of Evaluation (TOE) is identified as follows:

Table 1 TOE Identification

TOE Name and Version	McAfee Change Control and Application Control 7.0.0 with ePolicy Orchestrator 5.3.2 5.3.2
Developer	Intel Corporation
Conformance Claim	EAL 2 + ALC_FLR.2

1.1 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.

1.2 TOE DESCRIPTION

The TOE provides change control and monitoring on servers and desktops. It also ensures that only authorized code can run on those managed systems. This functionality is managed through the ePolicy Orchestrator (ePO) management software.

The product consists of four logical components:

- Change Control (monitors changes happening on managed systems);
- Application Control (prevents unauthorized execution of program code);
- ePO (for remote management of Change Control and Application Control); and
- McAfee Agent.

The four logical components are implemented via four physical software components:

- Solidcore Service – Manages the policy for the Filesystem Driver and interfaces with the CLI and McAfee Agent.
- Filesystem Driver (swin.sys) – The portion of the product implemented in the Operating System's (OS) kernel space; the filesystem driver intercepts and analyzes all file system, registry, memory, and other critical reads and writes occurring in the OS and implements the core application control and change control and monitoring actions.
- ePO – Used for remote management of the Solidcore Service.
- McAfee Agent – A generic agent used by ePO for communication with a managed endpoint. The agent distributes policies from and reports back to ePO.

1.3 TOE ARCHITECTURE

A diagram of the TOE architecture is as follows:

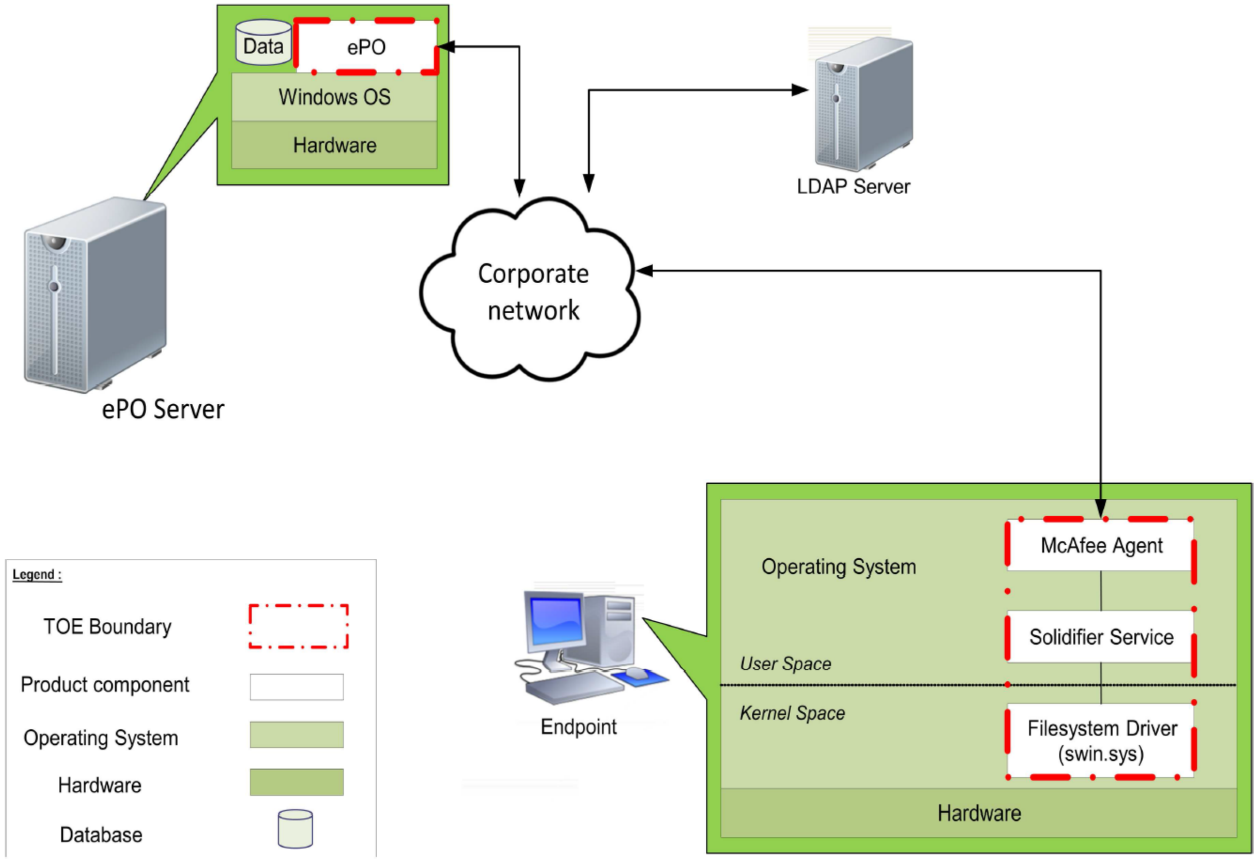

Figure 1 TOE Architecture

2 SECURITY POLICY

The TOE implements policies pertaining to the following security functional classes:

- Security Audit;
- Cryptographic Support;
- Identification and Authentication;
- Security Management;
- Protection of the TOE Security Functionality; and
- McAfee Application and Change Control.

Complete details of the security functional requirements (SFRs) can be found in the Security Target (ST) referenced in section 8.2.

2.1 CRYPTOGRAPHIC FUNCTIONALITY

The following cryptographic modules were evaluated by the CMVP and implemented in the TOE:

Table 2 Cryptographic Module(s)

Cryptographic Module	Certificate Number
OpenSSL v1.0.1r	1747
RSA BSAFE Crypto-C Micro Edition v4.0.1	2097

3 ASSUMPTIONS AND CLARIFICATIONS OF SCOPE

Consumers of the TOE 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.

3.1 USAGE AND ENVIRONMENTAL ASSUMPTIONS

The following assumptions are made regarding the use and deployment of the TOE:

- The TOE has access to all the IT System data it needs to perform its functions;
- The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access;
- The TOE software critical to security policy enforcement, and the hardware on which it runs, will be protected from unauthorized physical modification;
- 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;
- The TOE will be managed in a manner that allows it to appropriately address changes in the IT systems the TOE monitors; and
- The IT environment will provide reliable time stamps for the TOE to use.

4 EVALUATED CONFIGURATION

The evaluated configuration for the TOE comprises:

The following software packages:

- McAfee Solidcore ePO Server Extension 7.0.0-270;
- Solidcore client 7.0.0-646;
- ePO Server 5.3.2-156 with Hotfix 1133331; and
- McAfee Agent 5.0.3-272.

Running on one of the following endpoint platforms:

- Windows 7 (64-bit);
- Windows 8.1;
- Windows 10;
- Windows Server 2008 R2; or
- Windows Server 2012 R2.

4.1 DOCUMENTATION

The following documents are provided to the consumer to assist in the configuration and installation of the TOE:

McAfee ePolicy Orchestrator:

- Product Guide for McAfee ePolicy Orchestrator 5.3.0 Software; (applies equally to EPO 5.3.2)
- Installation Guide McAfee ePolicy Orchestrator 5.3.0 Software;
- User Guide McAfee ePolicy Orchestrator 5.3.0 Software FIPS Mode; and
- Release Notes for McAfee ePolicy Orchestrator 5.3.2.

McAfee Agent:

- Product Guide McAfee Agent 5.0.1; and (applies equally to MA 5.0.3)
- Release Notes for McAfee Agent 5.0.3.

McAfee Change Control and Application Control

- Product Guide McAfee Change Control and McAfee Application Control 7.0.0 for use with ePolicy Orchestrator;
- Installation Guide McAfee Change Control and McAfee Application Control 7.0.0 for use with ePolicy Orchestrator;
- McAfee Change Control and Application Control 7.0.0 with ePolicy Orchestrator 5.3.2 Guidance Document Supplement;
- McAfee Change Control 7.0.0 Reference Guide;
- McAfee Application Control 7.0.0 Reference Guide;
- Release Notes for McAfee Change Control 7.0.0; and
- Release Notes for McAfee Application Control 7.0.0.

5 EVALUATION ANALYSIS ACTIVITIES

The evaluation analysis activities involved a structured evaluation of the TOE. Documentation and process dealing with Development, Guidance Documents, and Life-Cycle Support were evaluated.

5.1 DEVELOPMENT

The evaluators analyzed the TOE 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 TOE 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.

5.2 GUIDANCE DOCUMENTS

The evaluators examined the TOE 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.

Section 4.1 provides details on the guidance documents.

5.3 LIFE-CYCLE SUPPORT

An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the TOE 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 the TOE during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the TOE. 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 TOE.

6 TESTING ACTIVITIES

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

6.1 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 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.

6.2 CONDUCT OF TESTING

The TOE 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.

6.3 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. The following testing activities were performed:

a. Repeat of Developer's Tests: The evaluator repeated a subset of the developers tests;

b. Security Audit: The objective of this test goal is to confirm that

    a. The TOE creates audit records for start-up and shutdown;

    b. The TOE allows administrators with proper permissions to view, sort and filter on various items when reviewing audit records; and

    c. The TOE allows users with the Global Reviewer and Solidcore Reviewer permission to view the audit records.

c. Security Management: The objective of this test goal is to confirm that the TOE provides the management functionality listed in the ST;

d. Change Control Actions (Read and Write Protected): The objective of this test goal is to confirm that the TOE prevents actions on protected files; and

e. Application Control Monitoring and Data Collection: The objective of this test goal is to confirm that the TOE monitors user management events and collects a whitelist inventory of events.

6.3.1 FUNCTIONAL TEST RESULTS

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

6.4 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 such as Heartbleed, Shellshock, FREAK, POODLE, DROWN and GHOST;

b. Port Scan: The objective of this test goal is to confirm that those ports that are open, should be;

c. Information Leakage: The objective of this test goal is to monitor for data leakage during start-up, shut-down and login; and

d. Security Bypass: The objective of this test goal is to attempt to bypass the TOE's restrictions by uninstalling programs, stopping services, or modifying registry settings and files.

6.4.1 PENETRATION TEST RESULTS

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

7 RESULTS OF THE EVALUATION

This evaluation has provided the basis for the conformance claim documented in Table 1. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

The IT product identified in this report has been evaluated at an approved evaluation facility established under the Canadian Common Criteria Scheme using the Common Methodology for IT Security Evaluation, Version 3.1 Revision 4, for conformance to the Common Criteria for IT Security Evaluation, Version 3.1 Revision 4. These evaluation results apply only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report.

The evaluation has been conducted in accordance with the provisions of the Canadian Common Criteria Scheme and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This is not an endorsement of the IT product by CSE or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by CSE or by any other organization that recognizes or gives effect to this certificate, is expressed or implied.

8 EVALUATOR COMMENTS, OBSERVATIONS AND RECOMMENDATIONS

It is recommended that potential operators of the TOE familiarize themselves with the Security Target, and relevant set-up documentation as identified in section 4.1, before operating the device. In particular, it is important that the device be successfully configured into FIPS mode before its operational use.

9 SUPPORTING CONTENT

9.1 LIST OF ABBREVIATIONS

Term	Definition
CAVP	Cryptographic Algorithm Validation Program
CCEF	Common Criteria Evaluation Facility
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
ePO	ePolicy Orchestrator
ETR	Evaluation Technical Report
GC	Government of Canada
IT	Information Technology
ITS	Information Technology Security
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories – Canada
PP	Protection Profile
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

9.2 REFERENCES

Reference
Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012.
Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012.
Security Target McAfee Change Control and Application Control 7.0.0 with ePolicy Orchestrator 5.3.2, v 0.7, July 2, 2016.
Evaluation Technical Report for McAfee Change Control and Application Control 7.0.0 with ePolicy Orchestrator 5.3.2, v 1.0, October 5, 2016.