Certification Report

McAfee Change Control and Application Control 6.1.3 with ePolicy Orchestrator 5.1.1

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-307-CR
Version: 1.0
Date: 24 November 2014
Pagination: i to iii, 1 to 13

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 EWA-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, 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 24 November 2014, 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).

TABLE OF CONTENTS

Executive Summary

McAfee Change Control and Application Control 6.1.3 with ePolicy Orchestrator 5.1.1 (hereafter referred to as McAfee Change Control and Application Control), from McAfee, Inc., is the Target of Evaluation. The results of this evaluation demonstrate that McAfee Change Control and Application Control meets the requirements of Evaluation Assurance Level (EAL) 2 augmented for the evaluated security functionality.

McAfee Change Control and Application Control is a software-only TOE. McAfee Change Control and Application Control v6.1.3 with ePolicy Orchestrator v5.1.1 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.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 03 November 2014 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 Change Control and Application Control, 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 Change Control and Application Control 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 Change Control and Application Control 6.1.3 with ePolicy Orchestrator 5.1.1 (hereafter referred to as McAfee Change Control and Application Control), from McAfee, Inc.

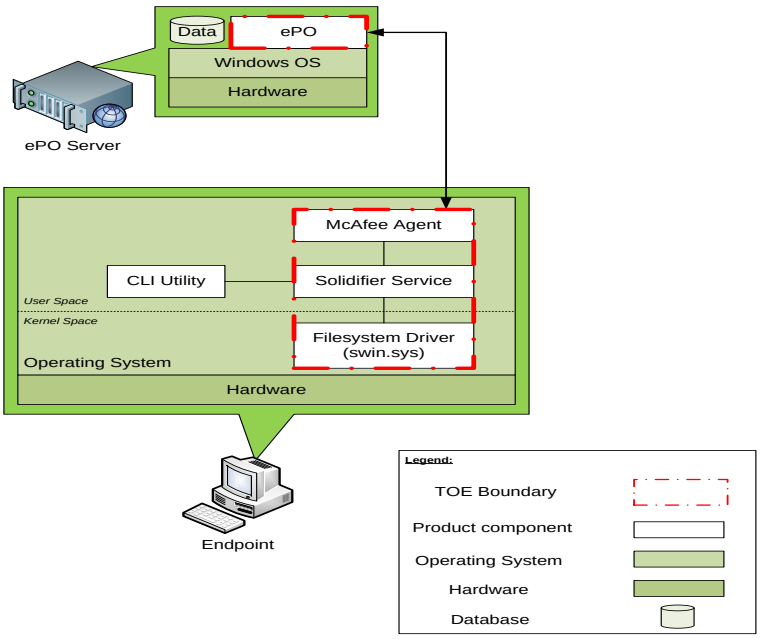
2 TOE Description

McAfee Change Control and Application Control v6.1.3 with ePolicy Orchestrator (ePO) v5.1.1 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 ePO management software. The product consists of three logical components: Change Control, Application Control and the ePO. The logical components are implemented via the following physical software components:

- Filesystem Driver – 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 change control and application control monitoring actions.
- Solidifier Service – manages the policy for the Filesystem Driver and interfaces with the McAfee Agent.
- ePO – provides remote management functionality for the Solidifier Service.
- McAfee Agent – a plug-in to the Solidifier Service used by ePO.

Communication between the ePO and the McAfee Agent is protected from disclosure and modification by FIPS 140-2 validated cryptographic modules.

A diagram of the McAfee Change Control and Application Control architecture is as follows:



3 Security Policy

McAfee Change Control and Application Control implements a role-based access control policy to control administrative access to the system. In addition, McAfee Change Control and Application Control implements policies pertaining to the following security functional classes:

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

The TOE protects communication between the ePO and the McAfee Agent from disclosure and modification with the following FIPS 140-2 validated cryptographic modules:

Cryptographic Module	**Certificate**
OpenSSL FIPS Object Module version 1.2	1051
RSA BSAFE® Crypto-C Micro Edition (ME) version 2.1	828

4 Security Target

The ST associated with this Certification Report is identified below:

McAfee Change Control and Application Control v6.1.3 with ePolicy Orchestrator v5.1.1 Security Target, version 2.0, October 31, 2014

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 Change Control and Application Control 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:*

- *EXT_MAC_SDC.1 - Application and Change Control Data Collection*
- *EXT_MAC_RCT.1- Application and Change Control React*

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 Change Control and Application Control 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.*
- *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 IT Environment will provide reliable timestamps for the TOE to use.*
- *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.*

6.3 Clarification of Scope

- The CLI Utility is excluded from the evaluation and must be disabled.
- The FIPS validation is vendor affirmed and the cryptographic modules have been ported in accordance with FIPS IG G.5.

7 Evaluated Configuration

The evaluated configuration for McAfee Change Control and Application Control comprises:

- *McAfee Change Control and Application Control version 6.1.3 with McAfee Solidcore ePO Server Extension 6.1.3-131, Solidcore client 6.1.3-353 and McAfee Agent 4.8.0-1500 running on Windows 7 (64-bit), Windows Server 2008 R2 and Windows Server 2012 endpoint clients*
- *ePO version 5.1.1-357 running on Windows Server 2008 R2 (64-bit)*

The following third-party products are used by the TOE in the CC-evaluated configuration:

- *Active Directory (LDAP) Server*
- *MS SQL Server 2008 R2 database*

The publication entitled McAfee Change Control and Application Control 6.1.3 with ePolicy Orchestrator 5.1.1 Guidance Document Supplement version 1.4 describes the procedures necessary to install and operate McAfee Change Control and Application Control in its evaluated configuration.

8 Documentation

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

a. Product Guide for McAfee ePolicy Orchestrator 5.1.0 Software, 2013;

b. Installation Guide McAfee ePolicy Orchestrator 5.1.0 Software, 2013;

c. Reference Guide McAfee ePolicy Orchestrator 5.1.0 Software Log Files, 2013;

d. User Guide McAfee ePolicy Orchestrator 5.1.0 Software FIPS Mode, 2014;

e. Product Guide McAfee Agent 4.8.0, 2013;

f. Product Guide McAfee Change Control and Application Control 6.1.3 for use with ePolicy Orchestrator 4.6.0 – 5.1.0 Software, 2014;

g. Installation Guide McAfee Change Control and Application Control 6.1.3 for use with ePolicy Orchestrator 4.6.0 – 5.1.0 Software, 2014;

h. McAfee Change Control and Application Control 6.1.3 with ePolicy Orchestrator 5.1.1 Guidance Document Supplement version 1.4;

i. McAfee Change Control 6.1.0 Command Line Reference Guide, 2012;

j. Command Line Interface Guide McAfee Application Control 6.1.0, 2012;

k. Release Notes for McAfee Application Control 6.1.3, 2014;

l. Release Notes for McAfee Change Control 6.1.3, 2014;

m. Release Notes for McAfee Agent 4.8.0 Patch 2, 2013; and

n. *Release Notes for McAfee ePolicy Orchestrator 5.1.1, 2014.*

9 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of McAfee Change Control and Application Control, including the following areas:

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

The evaluators reviewed the flaw remediation procedures used by developer for the McAfee Change Control and Application Control. 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. Security Audit: The objective of this test goal is to confirm that the TOE will create audit records for start-up and shutdown and will only allow administrators with proper permissions to view, sort and filter when reviewing the audit records;

c. User Attributes: The objective of this test goal is to confirm that the TOE maintains security attributes belonging to individual users;

d. FIPS Mode: The objective of this test goal is to confirm that the TOE is operating in FIPS mode;

e. Security Management: The objective of this test goal is to confirm the management functionality provided by the TOE;

f. Change Control Actions: The objective of this test goal is to confirm that the TOE will enforce change control rules on any file listed as write-protected;

g. Application Control Actions: The objective of this test goal is confirm that the TOE will enforce application control rules on any file listed as read-protected;

h. Change Control Monitoring: The objective of this test goal is to confirm that the TOE monitors events indicating the success or failure of user logon or logoff attempts and user

[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.

account management activities such as user account creation, user account deletion, user account modification (account enabled, account disabled, and password changed);

i. Application Control Data Collection: The objective of this test goal is to confirm that the TOE collects events indicative of unauthorized execution of program code and prevented attempts to modify files;

j. Change Control Data Collection: The objective of this test goal is to confirm that the TOE collects events indicating access to write-protected files, read-protected files and write-protected registry keys; and

k. Application Control Allow by Publisher/Certificate: The objective of this test case is to confirm that that TOE will allow the execution of a signed application based on publisher/certificate.

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. Information Leakage: The objective of this test goal is to verify if any sensitive information is disclosed during startup, shutdown and login;

c. Concurrent User Login: The objective of this test goal is to verify that the TOE manages concurrent sessions successfully;

d. Password Requirement Bypass: The objective of this test goal is to attempt to change the permissions on the password file to read-only and attempt to access the command line interface without presenting a password;

e. OpenSSL ChangeCipherSpec Vulnerability: The objective of this test goal is to determine if the implementation of OpenSSL is susceptible to the ChangeCipherSpec injection vulnerability; and

f. Security Bypass: The objective of this test goal is to attempt to override TOE security policies on an endpoint workstation.

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

10.4 Conduct of Testing

McAfee Change Control and Application Control 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 Facility. 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.

10.5 Testing Results

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

11 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.

12 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
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

13 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. Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program.

e. McAfee Change Control and Application Control v6.1.3 with ePolicy Orchestrator v5.1.1 Security Target, version 2.0, October 31, 2014.

f. Evaluation Technical Report for EAL 2+ Common Criteria Evaluation of McAfee Inc. McAfee Change Control and Application Control v6.1.3 with ePolicy Orchestrator v5.1.1 Document No. 1863-000-D002, Version 1.0, 3 November 2014.