Certification Report

McAfee Management for Optimized Virtual Environments Antivirus 3.0.0 with ePolicy Orchestrator 5.1.1

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number:	383-4-293-CR
Version:	1.0
Date:	24 November 2014
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 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 CGI IT Security Evaluation & Test Facility.

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).

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

TABLE OF CONTENTS

Executive Summary

McAfee Management for Optimized Virtual Environments Antivirus 3.0.0 with ePolicy Orchestrator 5.1.1 (hereafter referred to as McAfee MOVE), from McAfee, Inc., is the Target of Evaluation. The results of this evaluation demonstrate that McAfee MOVE meets the requirements of Evaluation Assurance Level (EAL) 2 augmented for the evaluated security functionality.

McAfee MOVE is a software antivirus solution for virtual environments that removes the need to install an antivirus application on every virtual machine (VM). McAfee MOVE contains a Security Virtual Appliance (SVA) delivered as an Open Virtualization Format (OVF) package which performs the scanning and detection of file-based viruses.

The ePolicy Orchestrator (ePO) through the MOVE ePO extension manages the SVAs that reside on the host hypervisors and provides the capability to distribute updated security policies and DAT files to the SVA. ePO also centrally manages generated event and log records. Communication between the ePO and the SVAs are protected from disclosure and modification by FIPS approved cryptographic modules.

CGI IT Security Evaluation & Test Facility is the CCEF that conducted the evaluation. This evaluation was completed on 07 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 MOVE, 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 MOVE 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

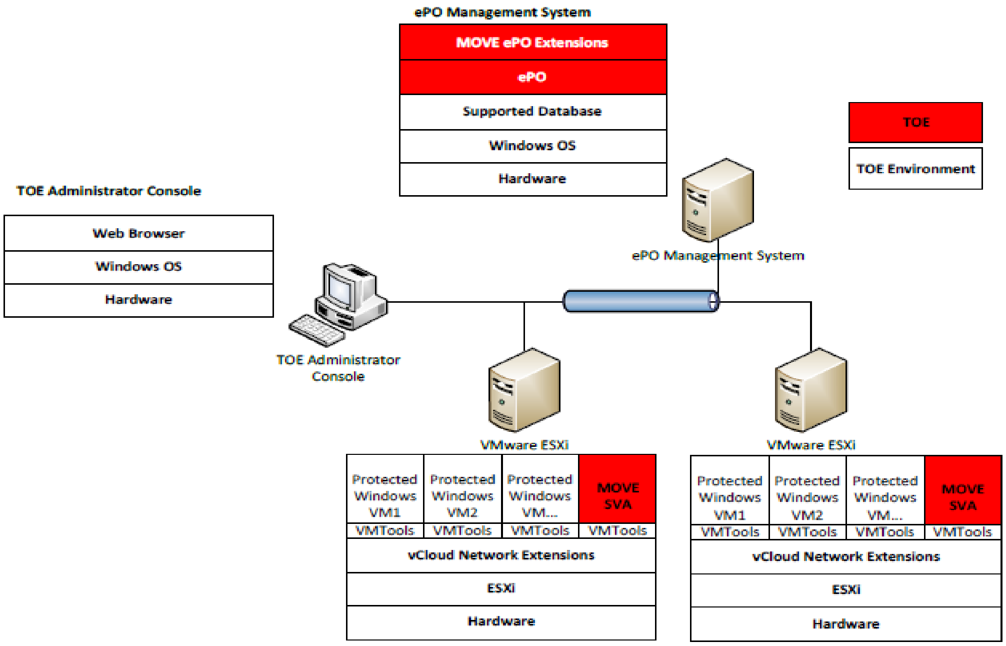
The Target of Evaluation (TOE) for this EAL 2+ evaluation is McAfee Management for Optimized Virtual Environments Antivirus 3.0.0 with ePolicy Orchestrator 5.1.1 (hereafter referred to as McAfee MOVE, from McAfee, Inc.

2 TOE Description

McAfee MOVE is a software antivirus solution for virtual environments that removes the need to install an antivirus application on every virtual machine. McAfee MOVE contains a Security Virtual Appliance (SVA) delivered as an Open Virtualization Format (OVF) package which performs the scanning and detection of file-based viruses on host hypervisors.

The ePolicy Orchestrator (ePO) through the MOVE ePO extension manages the SVAs that reside on the host hypervisors and provides the capability to distribute updated security policies and DAT files to the SVA. ePO also centrally manages generated event and log records. Communication between the ePO and the SVAs is protected from disclosure and modification by FIPS approved cryptographic modules.

A diagram of the McAfee MOVE architecture is as follows:



3 Security Policy

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

- *Security Audit*
- *Antivirus*
- *Cryptographic Support*
- *Identification and Authentication*
- *Security Management*
- *Protection of TOE Security Functionality (TSF)*
- *TOE Access*

The following cryptographic modules were evaluated to the FIPS 140-2 standard:

Cryptographic Module	**Certificate**
McAfee Agent Cryptographic Module	1588
RSA BSAFE® Crypto-C Micro Edition	2056
RSA BSAFE® Crypto-J JSAFE and JCE Software Module	2057

4 Security Target

The ST associated with this Certification Report is identified below:

McAfee Management for Optimized Virtual Environments (MOVE) Antivirus 3.0 with ePolicy Orchestrator 5.1.1 Security Target, v1.3, November 7, 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 MOVE 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:*
    - *FAV_ACT_EXT.1 - Antivirus Actions*
    - *FAV_SCN_EXT.1- Antivirus Scanning*

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 MOVE 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 Assumption is listed in the ST:

- *Administrators, including administrators of the IT environment, are non-hostile, appropriately trained, and follow all administrative guidance.*

6.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- *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 the TOE and the authentication server.*
- *Administrators will implement secure mechanisms for receiving and validating updated signature files from the antivirus vendors, and for distributing the updates to the central management systems.*

6.3 Clarification of Scope

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 MOVE comprises:

- *McAfee MOVE SVA version 3.0.0 installed on VMware ESXi version 5.0 with Patch 1, ESXi version 5.1, and ESXi version 5.5*
- *ePO version 5.1.1 with hotfix 983758 running on Windows Server 2008 R2*

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

- *VMware vCenter 5.0, 5.1, 5.5*
- *VMware vShield Manager 5.0,5.1, 5.5*
- *VMware vShield Endpoint 5.0, 5.1, 5.5*
- *VMware vSphere Client 5.0, 5.1, 5.5*
- *Active Directory (LDAP) Server*
- *MS SQL Server 2008 database*

The publication entitled Operational User Guidance and Preparative Procedures McAfee Management for Optimized Virtual Environments (MOVE) Antivirus Agentless 3.0 with ePolicy Orchestrator 5.1.1, Version: 0.8 describes the procedures necessary to install and operate McAfee Move in its evaluated configuration.

8 Documentation

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

a. McAfee MOVE AntiVirus 3.0.0 For use with ePolicy Orchestrator 4.6.0, 5.0.0 Software Product Guide;
b. ePolicy Orchestrator 5.1.0 Product Guide;
c. Supported Platforms, Environments and Operating Systems for ePolicy Orchestrator KB51569;
d. McAfee ePolicy Orchestrator 5.1.0 Software FIPS Mode User Guide;
e. ePO 5.x installation/patch upgrade checklist for known issues KB76739;
f. McAfee ePolicy Orchestrator 5.1.0 Software Installation Guide;
g. Release Notes Hotfix 983758-2 McAfee ePolicy Orchestrator 5.1.1
h. MOVE Agentless fix for BASH/Shellshock KB83017; and

i. Operational User Guidance and Preparative Procedures McAfee Management for Optimized Virtual Environments (MOVE) Antivirus Agentless 3.0 with ePolicy Orchestrator 5.1.1, Version: 0.8.

9 Evaluation Analysis Activities

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

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

The evaluators reviewed the flaw remediation procedures used by developer for the McAfee MOVE. 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. Authentication Using an External Authentication Server: The objective of this test goal is to verify that the TOE will properly authenticate authorized users and deny unauthorized users when using an external authentication server;

c. Update Scan Signatures File: The objective of this test goal is to verify that the TOE can successfully transfer updated scan signature files from the ePO server to the SVA;

d. Audit Generation: The objective of this test goal is to verify that required audit records are generated;

e. Antivirus Functionality: The objective of this test goal is to verify that the TOE will update antivirus policies and transfer the updated policies to the SVA. This test goal will also verify that the traffic is encrypted and the policy update is audited;

f. Union Permission Set: The objective of this test goal is to verify that multiple permission sets assigned to a user are enforced and that the removal of a permission set is properly enforced; and

[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.

g. SVA Audit: The objective of this test case is to verify that, in the event that the SVA is unable to communicate with the ePO, audit events will be queued until communication is successful.

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. Remote Access to SVA Command Line Interface (CLI): The objective of this test goal is to attempt to access the SVA CLI remotely; and

c. Exhaust Audit Log Storage: The objective of this test goal is to attempt to exhaust audit log storage.

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

10.4 Conduct of Testing

McAfee MOVE 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 MOVE 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
CLI	Command Line Interface
CPL	Certified Products list
CM	Configuration Management
EAL	Evaluation Assurance Level
ePO	ePolicy Orchestrator
ETR	Evaluation Technical Report
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
MOVE	Management for Optimized Virtual Environments
OVF	Open Virtualization Format
PALCAN	Program for the Accreditation of Laboratories - Canada
SFR	Security Functional Requirement
SSH	Secure Shell
ST	Security Target
SVA	Security Virtual Appliance
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 Management for Optimized Virtual Environments (MOVE) Antivirus 3.0 with ePolicy Orchestrator 5.1.1 Security Target, v1.3, November 7, 2014.

f. McAfee Management for Optimized Virtual Environments (MOVE) Antivirus 3.0 with ePO 5.1.1 Common Criteria EAL 2+ Evaluation Technical Report, v1.2, November 7, 2014.