Certification Report

McAfee Enterprise Mobility Management 12.0

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-275-CR
Version: 1.0
Date: 04 September 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 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 04 September 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 Enterprise Mobility Management 12.0 (hereafter referred to as McAfee EMM v12.0), from McAfee, Inc., is the Target of Evaluation. The results of this evaluation demonstrate that McAfee EMM v12.0 meets the requirements of Evaluation Assurance Level (EAL) 2 augmented for the evaluated security functionality.

McAfee EMM v12.0 provides secure management of mobile devices, allowing the integration of smart mobile devices into enterprise networks with the same level of security protection enabled on laptops and desktops. With McAfee EMM v12.0, System Administrators have the tools and capabilities needed to secure mobile devices in the enterprise network, manage them in a scalable architecture, and assist users when problems arise.

McAfee EMM v12.0 is a web-based solution that helps manage the life cycle of the mobile device. McAfee EMM's combination of device management, network control and compliance reporting delivers a mobile device security solution.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 15 August 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 EMM v12.0, 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 EMM v12.0 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

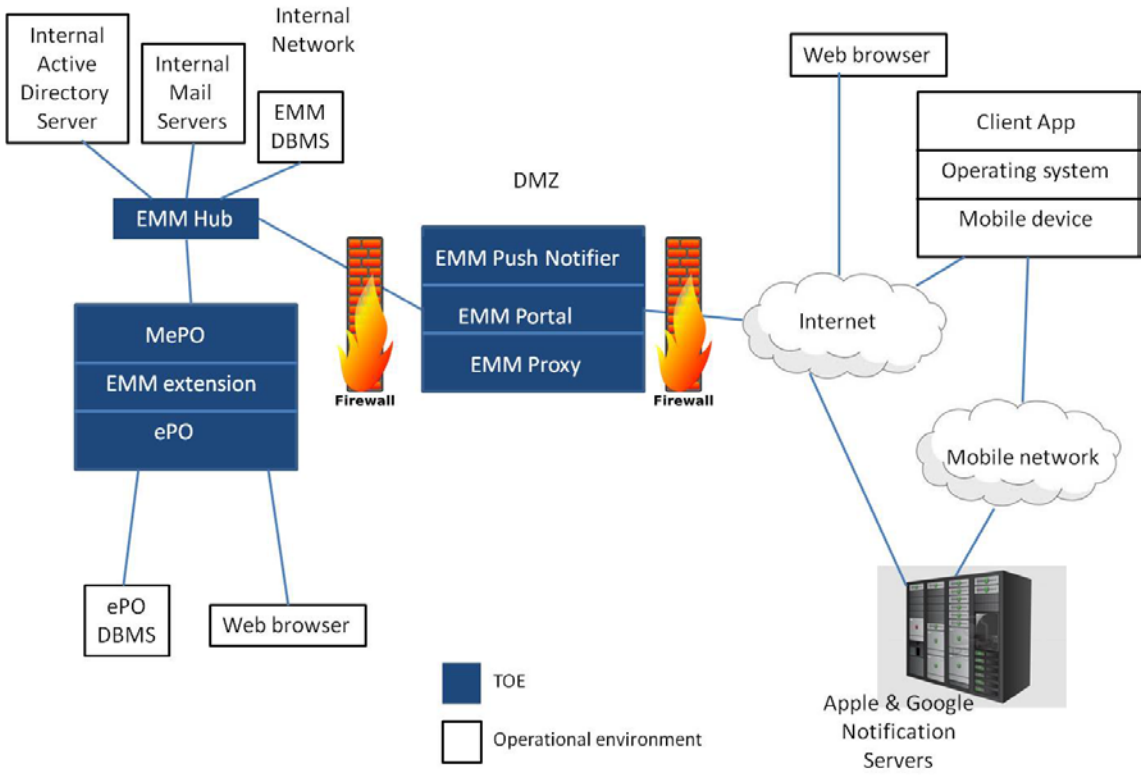
The Target of Evaluation (TOE) for this EAL 2+ evaluation is McAfee Enterprise Mobility Management 12.0 (hereafter referred to as McAfee EMM v12.0), from McAfee, Inc..

2 TOE Description

McAfee EMM v12.0 provides secure management of mobile devices, allowing the integration of smart mobile devices into enterprise networks with the same level of security protection enabled on laptops and desktops. With McAfee EMM v12.0, System Administrators have the tools and capabilities needed to secure mobile devices in the enterprise network, manage them in a scalable architecture, and assist users when problems arise.

McAfee EMM v12.0 is a web-based solution that helps manage the life cycle of the mobile device. McAfee EMM's combination of device management, network control and compliance reporting delivers a mobile device security solution.

A diagram of the McAfee EMM v12.0 architecture is as follows:



3 Security Policy

McAfee EMM v12.0 implements a role-based access control policy to control administrative access to the system. In addition, McAfee EMM v12.0 implements policies pertaining to the following security functional classes:

- *Identification and Authentication*
- *Management*
- *Audit*
- *Policy Management*

4 Security Target

The ST associated with this Certification Report is identified below:

Security Target: McAfee Enterprise Mobility Management 12.0, v1.16, 20 July 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 EMM v12.0 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 conformant; with security functional requirements based only upon functional components in Part 2;*

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 EMM v12.0 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:

- *The TOE has access to all the IT System data it needs to perform its functions;*
- *Access to the database used by the TOE via mechanisms outside the TOE boundary is restricted to authorized persons;*
- *The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors;*
- *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*
- *A public key infrastructure is in place that allows the TOE to verify the authenticity of communications with a mail server.*

6.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- *Access to the database used by the TOE via mechanisms outside the TOE boundary is restricted to authorized persons; and*
- *The TOE software critical to security policy enforcement will be protected from unauthorized physical modification.*

6.3 Clarification of Scope

The scope of the TOE covers the management element only, and does not include the software on the mobile devices themselves. The security functions of the TOE are limited to creating and pushing policy to the mobile device client, which is responsible for policy enforcement.

7 Evaluated Configuration

The evaluated configuration for McAfee EMM v12.0 comprises:

- EMM Server Version 12.0.780.52882
- McAfee ePO 5.1.0 build 509 with hotfixes 1, 960279-2, 962156 and 973112
- McAfee EMM 12.0 build 12.0.0.1073
- McAfee EMM help 12.0.0.022

Installed on a GPC with the following requirements;

Processor: Dual core CPU

Memory: 4 GB RAM

Free Disk Space: 1 GB

Operating System

- Windows Server 2008 64-bit with Service Pack 2; or
- Windows Server 2008 R2 64-bit with Service Pack 1

DBMS

- Microsoft SQL Server 2005 with Service Pack 3; or
- Microsoft SQL Server 2008 R2 32- and 64-bit with Service Pack 1

Web Browser

Internet Explorer 8.0 ; Firefox 10.0; or Chrome 17

The mobile device to be managed needs to have the following software installed;

- McAfee EMM App (iOS and Android devices) Version 4.9.1
- McAfee EMM Secure Container (Android devices) App Version 2.3.93

The publication entitled Operational User Guidance and Preparative Procedures Supplement McAfee Enterprise Mobility Management 12.0, Document Version 1.3, June 11, 2014 describes the procedures necessary to install and operate McAfee EMM v12.0 in its evaluated configuration.

8 Documentation

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

a. Installation Guide McAfee Enterprise Mobility Management 12.0 Software for use with ePolicy Orchestrator 4.6.7-5.1 Software, 12.0, 2014;

b. Product Guide McAfee Enterprise Mobility Management 12.0 Software for use with ePolicy Orchestrator 4.6.7-5.1 Software, 12.0, 2014;

c. Product Guide McAfee ePolicy Orchestrator 5.1.0 Software, 5.1.0, 2013; and

d. Installation Guide McAfee ePolicy Orchestrator 5.1.0 Software, 5.1.0, 2013

9 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of McAfee EMM v12.0, including the following areas:

Development: The evaluators analyzed the McAfee EMM v12.0 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 EMM v12.0 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 EMM v12.0 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 EMM v12.0 configuration management system and associated documentation was performed. The evaluators found that the McAfee EMM v12.0 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 EMM v12.0 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the McAfee EMM v12.0. 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. Portal User Attributes: The objective of this test goal is to verify that the TOE maintains portal user attributes such as user name and locked status;

c. User permissions: The objective of this test goal is to confirm that the TOE enforces system administrator and report viewer, permissions;

d. Lock Non-Compliant Device: The objective of this test goal is confirm that the TOE can request that a non-compliant device be locked;

e. Removal and wipe: The objective of this test goal is to confirm that the TOE can request the removal of EMM profiles from a device and/or wipe corporate/all information on a device; and

f. Unlock device: The objective of this test goal is to confirm that the TOE can unlock users and request devices to be unlocked.

[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.

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 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; and

c. Concurrent logins: The objective of this test goal is to attempt to compromise the TOE by having multiple administrator logins.

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

10.4 Conduct of Testing

McAfee EMM v12.0 was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place 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.

10.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, providing assurance that McAfee EMM v12.0 behaves as specified in its ST and functional specification.

11 Results of the Evaluation

This evaluation has provided the basis for a EAL 2+ level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

12 Evaluator Comments, Observations and Recommendations

In order to avoid unintentional loss of functionality, implementers of McAfee EMM 12.0 must ensure that the effects of the security policy are fully understood for all end user platforms.

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
ePO	ePolicy Orchestrator
ETR	Evaluation Technical Report
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
MePO	Mobile ePO
PALCAN	Program for the Accreditation of Laboratories - Canada
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

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 4, September 2012.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012.

d. Security Target: McAfee Enterprise Mobility Management 12.0, v1.16, 20 July 2014

e. Evaluation Technical Report for EAL 2+ Common Criteria Evaluation of McAfee, Inc. McAfee Enterprise Mobility Management 12.0, Version 0.3, 15 August 2014.