Certification Report

EAL 2+ Evaluation of

McAfee® Enterprise Mobility Management 9.7

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number:	383-4-197-CR
Version:	1.0
Date:	30 August 2012
Pagination:	i to iii, 1 to 8

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, 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 located in Ottawa, 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, 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 30 August 2012, 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 trademarks or registered trademarks:

- McAfee is a registered trademark of McAfee Inc; and
- McAfee EMM is a registered trademark of McAfee Inc.

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

TABLE OF CONTENTS

Executive Summary

McAfee® Enterprise Mobility Management 9.7 (hereafter referred to as EMM), from McAfee, Inc., is the Target of Evaluation for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

EMM is a web-based solution that helps manage mobile devices and the integration of smart phones into enterprise networks.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 03 August 2012 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 EMM, the security requirements, and the level of confidence (evaluation assurance level) to which it is asserted that the product satisfies its 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)[1] for this product provide sufficient evidence that it meets the EAL 2 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 EMM 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] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 augmented evaluation is McAfee® Enterprise Mobility Management 9.7 (hereafter referred to as EMM), from McAfee, Inc.

2 TOE Description

EMM is a web-based solution that provides secure management of mobile devices and allows the integration of smart phones into enterprise networks. With EMM, system administrators have the tools and capabilities to secure mobile devices in the enterprise network, to manage them in a scalable architecture, and assist users when problems arise. The McAfee EMM Portal allows device users to initiate requests for software downloads.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for EMM is identified in Section 6 of the ST.

4 Security Target

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

Title: Security Target McAfee Enterprise Mobility Management 9.7
Version: 0.9
Date: 05 July 2012

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.*

EMM is:

a. *Common Criteria Part 2 conformant*, with security functional requirements based only upon functional components in Part 2;
b. *Common Criteria Part 3 conformant*, with security assurance requirements based only upon assurance components in Part 3; and
c. *Common Criteria EAL 2 augmented*, containing all security assurance requirements in the EAL 2 package, as well as the following: ALC_FLR.2 – Flaw Reporting Procedures.

6 Security Policy

EMM implements an access control policy to control access to the system.

In addition, EMM implements other policies pertaining to security audit, user data protection, identification and authentication, and security management. Further details on these security policies may be found in Section 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of EMM 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:

- The authorized administrators are not careless, wilfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation;
- There will be one or more competent individuals assigned to manage the TOE and security of the information it contains; 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 IT systems and data it needs to perform its functions;
- The Toe is appropriately scalable to the |IT systems it monitors; and
- The TOE hardware and software will be protected from unauthorized physical modification and access.

7.3 Clarification of Scope

EMM offers protection against inadvertent or casual attempts to breach system security by unsophisticated attackers possessing basic attack potential. EMM is not intended for situations which involve determined attempts by hostile or well-funded attackers using sophisticated attack techniques.

8 Evaluated Configuration

The evaluated configuration for EMM comprises McAfee EMM 9.7.0.38202 installed on a host computer with a minimum processor of Intel Pentium III and running Windows Server 2003 x86 or 64 bit, Windows Server 2008 64 bit, or Windows Server 2008 R2 64 bit. The supported platforms for the McAfee Client Apps are iOS and Android.

The publication entitled Installation Guide: McAfee Enterprise Mobility Management® (McAfee EMM®) 9.6[2] describes the procedures necessary to install and operate EMM in its evaluated configuration.

9 Documentation

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

a. Product Guide: McAfee Enterprise Mobility Management® (McAfee EMM®) 9.7; and

b. Installation Guide: McAfee Enterprise Mobility Management® (McAfee EMM®) 9.6

c. Operational User Guidance and Preparative Procedures Supplement: McAfee Enterprise Mobility Management® (McAfee EMM®) 9.7

10 Evaluation Analysis Activities

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

Development: The evaluators analyzed the EMM 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 EMM 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 EMM 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 EMM configuration management system and associated documentation was performed. The evaluators found that the EMM configuration items were clearly marked. The developer’s configuration management system was observed during a site visit, and it was found to be mature and well-developed.

[2] Note that steps for the installation of version 9.7 are the same as version 9.6; as such no updated guide was developed.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of EMM during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by McAfee, Inc. for EMM. 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.

Vulnerability assessment: The evaluators conducted an independent vulnerability analysis of EMM. Additionally, the evaluators conducted a search of public domain vulnerability databases to identify EMM potential vulnerabilities. The evaluators identified potential vulnerabilities for testing applicable to EMM in its operational environment.

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

11 ITS Product Testing

Testing at EAL 2 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[3].

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.

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:

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

a. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests;

b. Independent Evaluator testing: The objective of this test goal is to exercise the TOE’s claimed functionality through evaluator independent testing: Tests covered in this area include:

    - Initialization: The objective of this test goal is to confirm that the system is initialized to a suitable state prior to the start of independent functional testing;

    - Security Management: Demonstrate the use of roles to meet the identification and authentication requirements; and

    - User Data Protection: Verify that Policies are pushed out to the mobile devices properly.

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:

a. Monitor – Information Leak (EMM Console): The purpose of this test case is to verify if the EMM Console leaks any sensitive information;

b. Monitor – Information Leak (Console to Device): The purpose of this test case is to verify if the Console leaks any sensitive information while performing a Policy update; and

c. Misuse: The purpose of this test goal is to attempt to circumvent Policy by installing a camera application.

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

11.4 Conduct of Testing

EMM 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 (ITSET) Facility 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.

11.5 Testing Results

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

12 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.

13 Evaluator Comments, Observations and Recommendations

The TOE has been evaluated for use with Android and iOS cellular phones. It is recommended that TOE users pay particular attention to the options that apply to the mobile operating system in use, as not all policy options are enforceable on all systems.

14 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
EMM	Enterprise Mobility Management
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 Requirements
ST	Security Target
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. Security Target McAfee Enterprise Mobility Management 9.7, version 0.9, 05 July 2012.

e. Evaluation Technical Report for EAL2+ Common Criteria Evaluation of McAfee Inc. McAfee® Enterprise Mobility Management 9.7 version 1.1, 03 August 2012.