Certification Report

McAfee Enterprise Security Manager with Event Receiver, Enterprise Log Manager, Advanced Correlation Engine, Application Data Monitor and Database Event Monitor 9.1

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number:	383-4-246-CR
Version:	1.0
Date:	27 November 2013
Pagination:	i to iii, 1 to 9

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.

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 27 November 2013, 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.

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

TABLE OF CONTENTS

Executive Summary

McAfee Enterprise Security Manager with Event Receiver, Enterprise Log Manager, Advanced Correlation Engine, Application Data Monitor and Database Event Monitor 9.1 (hereafter referred to as McAfee Enterprise Security Manager), from McAfee, Inc., is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

McAfee Enterprise Security Manager is a suite of software components aggregated to provide a Security Information and Event Management (SIEM) solution to the enterprise. It uses a single environment to consolidate, correlate, and report on security information. The TOE sets policies, rules, and thresholds that will generate alerts and launch mitigations.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 20 November 2013 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 Enterprise Security Manager, 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 McAfee Enterprise Security Manager 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 Security Manager with Event Receiver, Enterprise Log Manager, Advanced Correlation Engine, Application Data Monitor and Database Event Monitor 9.1 (hereafter referred to as McAfee Enterprise Security Manager), from McAfee, Inc.

2 TOE Description

McAfee Enterprise Security Manager is a suite of software components aggregated to provide a Security Information and Event Management (SIEM) solution to the enterprise. It uses a single environment to consolidate, correlate, and report on security information. The TOE sets policies, rules, and thresholds that will generate alerts and launch mitigations.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for McAfee Enterprise Security Manager 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: McAfee Enterprise Security Manager with Event Receiver, Enterprise Log Manager, Advanced Correlation Engine, Application Data Monitor and Database Event Monitor 9.1
Version: 1.1
Date: 25 March 2013

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.*

McAfee Enterprise Security Manager is:

a. *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:
    - SIEM_ANL.1 (EXP) – event analysis; and

- SIEM_RES.1 (EXP) – Incident Resolution.

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: e.g. ALC_FLR.2 – Flaw Reporting Procedures.

6 Security Policy

McAfee Enterprise Security Manager implements an administrative Access Control policy to control user access to the system. Details of this security policy can be found in Section 6 of the ST.

In addition, McAfee Enterprise Security Manager implements policies pertaining to security audit, user data protection, identification and authentication, incident management 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 McAfee Enterprise Security Manager 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:

- There will be one or more competent and appropriately trained individuals assigned to manage the TOE and the security of the information it contains;

- The authorized administrators are not careless, wilfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation; and

- The TOE is configured to receive all events from network-attached devices.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The IT environment will provide the TOE with the necessary reliable timestamp; and

- The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

8 Evaluated Configuration

The evaluated configuration for McAfee Enterprise Security Manager comprises the following components:

- McAfee Enterprise Security Manager 9.1.3 Build 20121030211720 with Event Receiver 9.1.3 Build 20121030211720;
- McAfee Database Event Monitor 9.1.3 Build 20121030211720;
- McAfee Application Data Monitor 9.1.3 Build 20121030211720;
- McAfee Advanced Correlation Engine 9.1.3 Build 20121030211720; and
- McAfee Enterprise Log Manager 9.1.3 Build 20121030211720.

The components are deployed on virtual machines running VMware vSphere Hypervisor (ESXi) 4.1 or 5.0 or on dedicated hardware appliances running a McAfee-customized Linux Operating System.

The publication entitled McAfee Enterprise Security Manager Interface 9.1.3 ESMI Setup and Installation Guide, 2012 describes the procedures necessary to install and operate McAfee Enterprise Security Manager in its evaluated configuration.

9 Documentation

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

a. McAfee Enterprise Security Manager Interface 9.1.3 ESM/Event Receiver VM Users Guide, 2012;
b. McAfee Enterprise Security Manager Interface 9.1.3 ESMI Users Guide, 2012;
c. McAfee Enterprise Security Manager Interface 9.1.3 ESMI Quick Start Guide 2012; and
d. McAfee Enterprise Security Manager Interface 9.1.3 ESMI Setup and Installation Guide 2012.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of McAfee Enterprise Security Manager, including the following areas:

Development: The evaluators analyzed the McAfee Enterprise Security Manager 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 Enterprise Security Manager 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 Enterprise Security Manager 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 Enterprise Security Manager configuration management system and associated documentation was performed. The evaluators found that the McAfee Enterprise Security Manager 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.

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

The evaluators reviewed the flaw remediation procedures used by developer for the McAfee Enterprise Security Manager. 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 McAfee Enterprise Security Manager. Additionally, the evaluators conducted a search of public domain vulnerability databases to identify McAfee Enterprise Security Manager potential vulnerabilities. The evaluators identified potential vulnerabilities; subsequent to follow-on penetration testing (ref: section 11.3) it was verified that none of the potential vulnerabilities were exploitable in the operational environment for McAfee Enterprise Security Manager.

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

11 ITS Product Testing

Testing 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[2].

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:

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

b. Initialization: The objective of this test goal is to confirm that the TOE can be installed and configured into the evaluated configuration.

c. Windows Service Event: The objective of this test goal is to confirm that a monitored server is logging events to the TOE;

d. User Privilege Escalation: The objective of this test case is to demonstrate that account creation and granting of privileges is tracked;

e. Restarting TOE Components: The objective of this test case is to confirm that TOE components can be stopped, started and rebooted and return to operation correctly; and

f. FIPS Testing: The objective of this test goal is to confirm that the TOE is running in FIPS mode.

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

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. Port Scan: The objective of this test case is to confirm which ports are available;

b. Information Leakage Verification: The objective of this test goal is to monitor for data leakage during startup, shutdown, login and other scenarios;

c. Multi-Admin: The objective of this test case is to verify that multiple administrative sessions can make changes to the TOE correctly at the same time;

d. Tampering: The objective of this test case is to sever connections with monitored devices, then re-establish connection and verify that event information is not lost; and

e. SSH Port: The objective of this test case is to verify that an intruder cannot gain access to the TOE using SSH.

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

11.4 Conduct of Testing

McAfee Enterprise Security Manager 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 McAfee Enterprise Security Manager 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 customer is reminded to follow all supplied guidance documentation when installing the TOE in its intended environment, and ensure it is operating in FIPS mode and using a strong password policy.

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
ETR	Evaluation Technical Report
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories - Canada
SIEM	Security Information and Event Management
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functional Requirements

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. McAfee Enterprise Security Manager with Event Receiver, Enterprise Log Manager, Advanced Correlation Engine, Application Data Monitor and Database Event Monitor 9.1, Security Target v1.1, 25 March 2013.

e. Evaluation Technical Report for McAfee Inc. McAfee Enterprise Security Manager 9.1, v1.0, 20 November 2013.