Certification Report

McAfee Database Security 5.1 with ePolicy Orchestrator 5.3.1

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-292-CR
Version: 1.0
Date: 16 February 2016
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 16 February 2016, 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 Database Security 5.1 with ePolicy Orchestrator (ePO) 5.3.1, from Intel Corporation, is the Target of Evaluation. The results of this evaluation demonstrate that McAfee Database Security 5.1 with ePO 5.3.1 meets the requirements of Evaluation Assurance Level (EAL) 2 augmented for the evaluated security functionality.

McAfee Database Security 5.1 with ePO 5.3.1 is a software solution that monitors a Database Management System (DBMS) and protects it from both internal and external threats. The TOE provides visibility into DBMS user and application activity by way of analysis of SQL statements and queries interacting with the DBMS. Analysis of DBMS transactions is determined by a monitoring policy consisting of a set of rules (predefined and/or custom) which are configured via the McAfee ePO to generate events and/or terminate suspicious activities.

CGI IT Security Evaluation & Test Facility is the CCEF that conducted the evaluation. This evaluation was completed on 16 February 2016 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 Database Security 5.1 with ePO 5.3.1, 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 TOE short name 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 Database Security 5.1 with ePolicy Orchestrator (ePO) 5.3.1, from Intel Corporation.

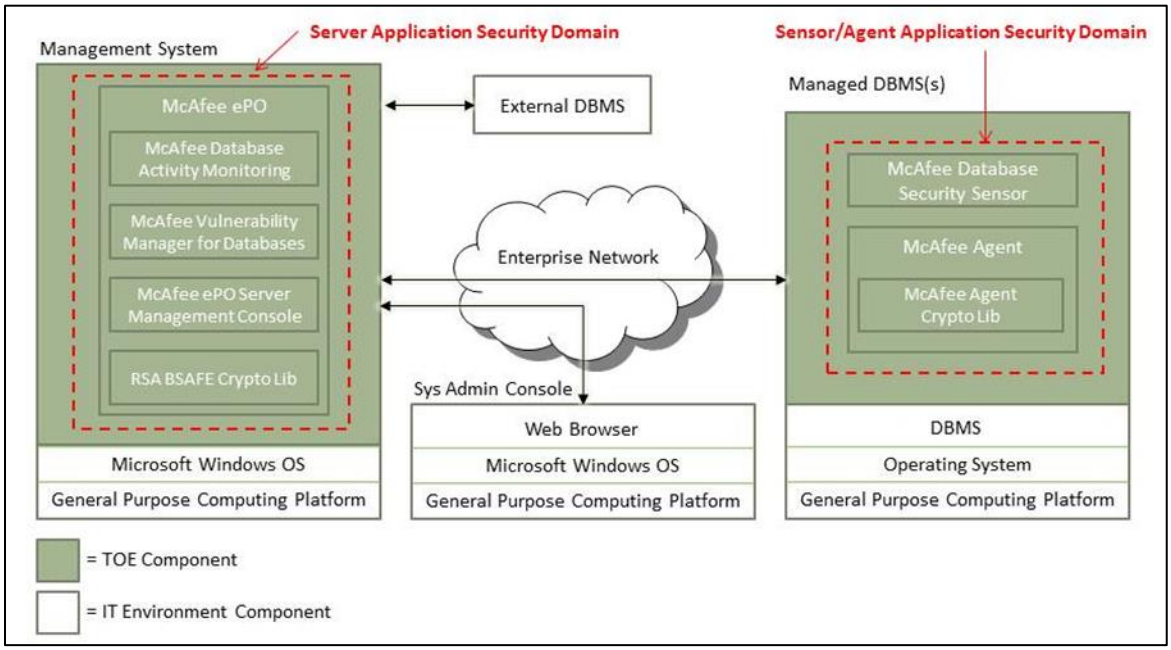
2 TOE Description

McAfee Database Security 5.1 with ePO 5.3.1 is a software solution that monitors a Database Management System (DBMS) and protects it from both internal and external threats. The TOE provides visibility into DBMS user and application activity by way of analysis of SQL statements and queries interacting with the DBMS. Analysis of DBMS transactions is determined by a monitoring policy consisting of a set of rules (predefined and/or custom) which are configured via the McAfee ePO to generate events and/or terminate suspicious activities. The TOE is comprised of the following components:

- McAfee Database Security Sensor which enables the monitoring of all local and network access to the DBMS(s) in real-time;
- McAfee Agent which resides on the DBMS host server and provides secure communication between the sensor on the managed DBMS and the ePO server; and
- McAfee ePO which executes on a dedicated server to manage and securely communicate with all installed sensors via the McAfee Agent.

The TOE protects transmissions between the ePO and the McAfee Agent from disclosure and modification by encrypting the transmissions under TLS.

A diagram of the McAfee Database Security 5.1 with ePO 5.3.1 architecture is as follows:



3 Security Policy

McAfee Database Security 5.1 with ePO 5.3.1 implements a role-based access control policy to control administrative access to the system. In addition, McAfee Database Security 5.1 with ePO 5.3.1 implements policies pertaining to the following security functional classes:

- Security Audit
- Cryptographic Support
- Identification and Authentication
- Security Management
- Protection of TOE Security Functions (TSF)
- Intrusion Detection

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

Cryptographic Module	**Certificate**
OpenSSL v1.0.1m with FIPS module v2.0.8	1747
RSA BSAFE Crypto-C Micro Edition v2.1.0	828

4 Security Target

The ST associated with this Certification Report is identified below:

McAfee Database Security 5.1 (Database Activity Monitoring 5.1.2 and Vulnerability Manager for Databases 5.1.3) with ePolicy Orchestrator 5.3.1 Security Target, Version 2.2, February 16, 2016.

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 Database Security 5.1 with ePO 5.3.1 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:
    - IDS_SDC.1- System Data Collection
    - IDS_ANL.1- Analyzer Analysis
    - IDS_RDR.1- Restricted Data Review
    - IDS_RCT.1 - Analyzer React
    - IDS_STG.1 - Guarantee of System Data Availability

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 Database Security 5.1 with ePO 5.3.1 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.

6.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE has access to all the DBMS data it needs to perform its functions and administrators will install as many TOE servers as necessary to support the number of sensors and DBMSs.
- Access to the DBMSs managed by the TOE is restricted to authorized users.
- The TOE and its users are capable of managing an evolving threat landscape relative to the DBMSs monitored by the TOE.
- The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
- The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
- The authorized administrator's web browser will use HTTPS to protect management sessions.

7 Evaluated Configuration

The evaluated configuration for McAfee Database Security 5.1 with ePO 5.3.1 comprises McAfee Database Security 5.1 build 16864 with ePO 5.3.1 build 188, with the following extensions installed:

- McAfee Database Activity Monitoring extension Version 5.1.3 build 52329
- McAfee Vulnerability Manager for Databases extension Version 5.1.3 build 52327[1]
- McAfee Rogue Database Detection extension Version 1.0.9 build 52304
- McAfee Advanced Management Core extension Version 1.0.9 build 52317
- McAfee Database Security Sensor Version 5.1.2 build 16864
- McAfee Agent Version 4.8.0 build 1990
- McAfee Virtual Patching for Databases Version 5.1.3[2]

In the evaluated configuration the ePO is running on Windows Server 2008 R2. The supported platforms for the McAfee Database Security Sensor and the McAfee Agent components are as follows:

SUPPORTED OS	OS VERSION	DBMS
Windows (Intel x86, 64-bit)	Windows Server 2003	Oracle 10.2, 11 Sybase ASE 15, 15.5, 15.7 DB2 9, 10
	Windows Server 2008	Microsoft SQL Server 2005, 2008, 2012 Oracle 10.2, 11.1, 12
	Windows Server 2008 R2	Microsoft SQL Server 2008
	Windows Server 2012	Microsoft SQL Server 2012
Linux (Intel x86, 64-bit)	CentOS 5	Oracle 12
	CentOS 5.5	MySQL 5.1, 5.5, 5.6
Solaris (SPARC, 64-bit)	Solaris 10	Oracle 8, 9, 10, 11, 12 Sybase ASE 15, 15.5, 15.7 DB2 9.5, 9.7, 10.1, 10.5

The publication McAfee Database Security 5.1 (Database Activity Monitoring 5.1.2 and Vulnerability Manager for Databases 5.1.3) with ePolicy Orchestrator 5.3.1 Operational User Guidance and Preparative Procedures Supplement, Version 1.3 describes the procedures necessary to install and operate McAfee Database Security 5.1 with ePO 5.3.1 in its evaluated configuration.

[1] The McAfee Vulnerability Manager for Databases will only execute VA scans on Microsoft SQL Server 2000, 2005, 2008, 2012 on all supported OS platforms; Oracle 9g, 10g, 11g on all supported OS platforms; Sybase ASE 15.0 on all supported OS platforms; DB2 9.1, 9.5, 9.7 on all supported OS platforms; and MySQL 5.5 on all supported OS platforms.

[2] McAfee Virtual Patching for Databases is a content deliverable managed through the McAfee Database Activity Monitoring extension. It is activated through a separate license which is needed to comply with the evaluated configuration.

8 Documentation

The Intel Corporation documents provided to the consumer are as follows:

a. McAfee Database Security 5.1 (Database Activity Monitoring 5.1.2 and Vulnerability Manager for Databases 5.1.3) with ePolicy Orchestrator 5.3.1 Operational User Guidance and Preparative Procedures Supplement, Version 1.3;

b. McAfee Database Activity Monitoring 5.1.0 Product Guide, May 2014;

c. McAfee Vulnerability Manager for Databases 5.1.0 Product Guide, May 2014;

d. McAfee ePolicy Orchestrator 5.3.0 Software Product Guide, May 2015;

e. McAfee Agent 4.8.0 Product Guide, March 2013;

f. McAfee ePolicy Orchestrator 5.3.0 Software Installation Guide, May 2015; and

g. McAfee ePolicy Orchestrator 5.3.0 Software FIPS Mode User Guide, May 2015.

9 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of McAfee Database Security 5.1 with ePO 5.3.1, including the following areas:

Development: The evaluators analyzed the McAfee Database Security 5.1 with ePO 5.3.1 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 Database Security 5.1 with ePO 5.3.1 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 Database Security 5.1 with ePO 5.3.1 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 Database Security 5.1 with ePO 5.3.1 configuration management system and associated documentation was performed. The evaluators found that the McAfee Database Security 5.1 with ePO 5.3.1 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 Database Security 5.1 with ePO 5.3.1 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the McAfee Database Security 5.1 with ePO 5.3.1. 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[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.

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. Restricted Data Access: The objective of this test case is to verify that the TSF prevents any interaction with the TOE until the user has been identified and authenticated;

c. Queries and Reports: The objective of this test case is to demonstrate that system data is provided in a manner suitable for the user to interpret it;

d. Reaction to Malicious Code detection: The objective of this test case is to confirm that the TOE will detect and react to malicious SQL code while ensuring that the malicious code is not executed; and

e. Verification of Cryptographic Modules: The objective of this test goal is to confirm the versions of the cryptographic modules implemented in the TOE.

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 such as Heartbleed, Shellshock, POODLE, GHOST, and FREAK;

[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.

b. Session Management: The objective of this test goal is to attempt to bypass administrator authentication; and

c. Disrupt Sensor: The objective of this test goal is to attempt to disable the sensor using malformed data.

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

10.4 Conduct of Testing

McAfee Database Security 5.1 with ePO 5.3.1 was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. 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 TOE short name 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 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
DBMS	Database Management System
EAL	Evaluation Assurance Level
ePO	ePolicy Orchestrator
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
SQL	Structured Query Language
ST	Security Target
TLS	Transport Layer Security
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. McAfee Database Security 5.1 (Database Activity Monitoring 5.1.2 and Vulnerability Manager for Databases 5.1.3) with ePolicy Orchestrator 5.3.1 Security Target, Version 2.2, February 16, 2016.

e. McAfee Database Security 5.1 (Database Activity Monitoring 5.1.2 and Vulnerability Manager for Database 5.1.3) with ePolicy Orchestrator 5.3.1 Common Criteria EAL 2+ Evaluation Technical Report, Version 2.2, February 16, 2016.