



COMMON CRITERIA CERTIFICATION REPORT

McAfee Threat Intelligence Exchange 2.0.0 and Data Exchange
Layer 3.0.0 with ePolicy Orchestrator 5.3.2

383-4-396

30 November 2016

v1.0





FOREWORD

This certification report is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE). Suggestions for amendments should be forwarded through departmental communications security channels to your Client Services Representative at CSE.

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 Scheme – 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 Canadian CC Scheme, 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.

If your department has identified a requirement for this certification report based on business needs and would like more detailed information, please contact:

ITS Client Services

Telephone: (613) 991-7654

E-mail: itsclientservices@cse-cst.gc.ca



OVERVIEW

The Canadian Common Criteria Scheme 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 Certification Body, which is managed by the Communications Security Establishment.

A CCEF is a commercial facility that has been approved by the 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 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.

The certification report, certificate of product evaluation and security target are posted to the Certified Products list (CPL) for the Canadian CC Scheme, and to the Common Criteria portal (the official website of the International Common Criteria Project).



TABLE OF CONTENTS

Executive Summary	1
1 Identification of Target of Evaluation	2
1.1 Common Criteria Conformance.....	2
1.2 TOE description	2
1.3 TOE architecture.....	3
2 Security policy	4
2.1 Cryptographic functionality.....	4
3 Assumptions and Clarifications of Scope	5
3.1 Usage and Environmental assumptions	5
3.2 Clarification of Scope.....	5
4 Evaluated Configuration	6
4.1 Documentation.....	6
5 Evaluation Analysis Activities	7
5.1 Development.....	7
5.2 Guidance Documents	7
5.3 Life-cycle Support	7
6 Testing Activities	8
6.1 Assessment of Developer Tests.....	8
6.2 Conduct of Testing.....	8
6.3 Independent Functional Testing.....	8
6.4 Independent Penetration Testing	9
7 Results of the Evaluation	10
7.1 Recommendations/Comments.....	10
8 Supporting Content	11
8.1 List of Abbreviations.....	11
8.2 References	12



LIST OF FIGURES

Figure 1 TOE Architecture3

LIST OF TABLES

Table 1 TOE Identification2

Table 2 Cryptographic Module(s).....4



EXECUTIVE SUMMARY

McAfee Threat Intelligence Exchange 2.0.0 and Data Exchange Layer 3.0.0 with ePolicy Orchestrator 5.3.2(hereafter referred to as the Target of Evaluation, or TOE), from Intel Corporation, was the subject of this Common Criteria evaluation. The results of this evaluation demonstrate that TOE meets the requirements of the conformance claim listed in Table 1 for the evaluated security functionality.

The TOE is a distributed software-only product that analyses files and certificates found on the network and makes informed security decisions. These decisions are based on a file's security reputation, and on criteria set by the administrator using the ePolicy Orchestrator (ePO) component and product related extensions.

The TOE uses the communication framework provided by Data Exchange Layer (DXL) component to support this activity. It is possible to identify the system where a threat was first detected, where it went from there, and to take policy based action to prevent further spread.

CGI IT Security Evaluation & Test Facility is the CCEF that conducted the evaluation. This evaluation was completed on 30 November 2016 and was carried out in accordance with the rules of the Canadian Common Criteria Scheme.

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for TOE, 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 Certification Body, declares that the TOE evaluation meets all the conditions of the Arrangement on the Recognition of Common Criteria Certificates and that the product will be listed on the Certified Products list (CPL) and the Common Criteria portal (the official website of the International Common Criteria Project).



1 IDENTIFICATION OF TARGET OF EVALUATION

The Target of Evaluation (TOE) is identified as follows:

Table 1 TOE Identification

TOE Name and Version	McAfee Threat Intelligence Exchange 2.0.0 and Data Exchange Layer 3.0.0 with ePolicy Orchestrator 5.3.2
Developer	Intel Corporation
Conformance Claim	EAL 2+ (ALC_FLR.2)

1.1 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.

1.2 TOE DESCRIPTION

The TOE is a distributed software-only product that analyses files and certificates found on the network and makes informed security decisions. These decisions are based on a file's security reputation, and on criteria set by the administrator using the ePolicy Orchestrator (ePO) component and product related extensions.

The TOE uses the communication framework provided by Data Exchange Layer (DXL) component to support this activity. It is possible to identify the system where a threat was first detected, where it went from there, and to take policy based action to prevent further spread.

1.3 TOE ARCHITECTURE

A diagram of the TOE architecture is as follows:

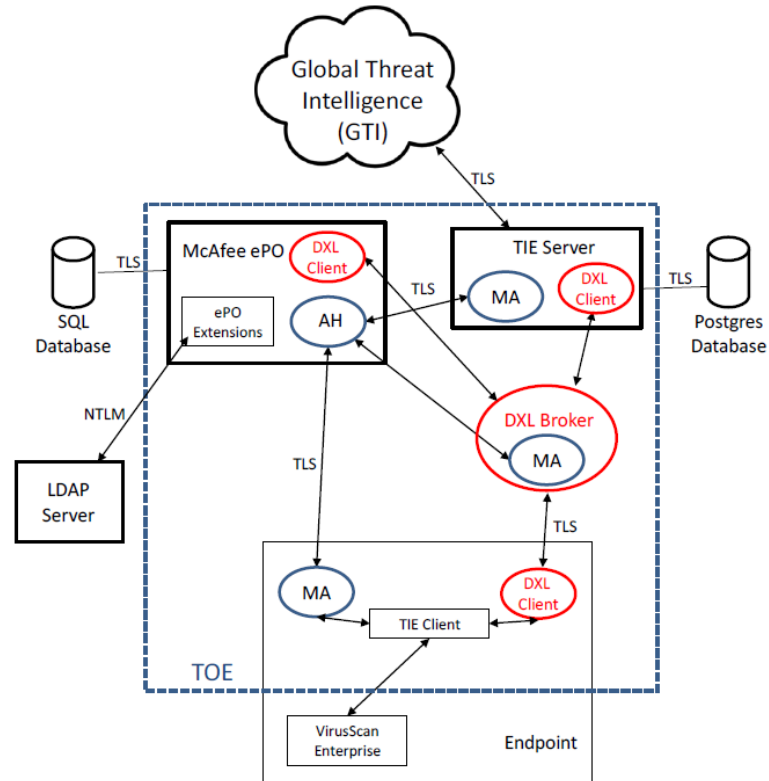


Figure 1 TOE Architecture



2 SECURITY POLICY

The TOE implements policies pertaining to the following security functional classes:

- Policy Enforcement
- Identification & Authentication
- Management
- Audit
- System Information Import
- TSF Data Protection

Complete details of the security functional requirements (SFRs) can be found in the Security Target (ST) referenced in section 8.2.

2.1 CRYPTOGRAPHIC FUNCTIONALITY

The following cryptographic modules were evaluated by the CMVP and implemented in the TOE:

Table 2 Cryptographic Module(s)

Cryptographic Module	Certificate Number
OpenSSL FIPS Object Module SE (Software Version: 2.0.12)	# 2398
RSA BSAFE® Crypto-C Micro Edition (Software Version: 4.0.1)	# 2097
RSA BSAFE® Crypto-J JSAFE and JCE Software Module (Software Version: 6.2)	# 2468



3 ASSUMPTIONS AND CLARIFICATIONS OF SCOPE

Consumers of the TOE 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.

3.1 USAGE AND ENVIRONMENTAL ASSUMPTIONS

The following assumptions are made regarding the use and deployment of the TOE:

- McAfee GTI provides reliable and appropriate file reputation information when requested.
- 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 use by authorized users.
- The administrators assigned to manage the TOE are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
- The hardware on which the TOE and the IT environment software are installed will be protected from unauthorized physical modification.
- The hardware, operating system, and other software on which the TOE depends, operate correctly.

3.2 CLARIFICATION OF SCOPE

The following features that are not part of the evaluated configuration for the TOE:

- Distributed Repositories - placed throughout a managed environment to provide managed systems access to receive signatures, product updates, and product installations with minimal bandwidth impact.
- Remote Agent Handlers - servers installed in various network locations to help manage McAfee Agent communication, load balancing, and product updates.
- The TOE can interact with Advanced Threat Defense to receive information on suspected threats, but its use is not part of the evaluated configuration.
- Reputation data may also be accepted from McAfee Web Gateway (MWG), but its use is not part of the evaluated configuration.
- Use of the TOE Server command line interface is disabled in the evaluated configuration.



4 EVALUATED CONFIGURATION

The evaluated configuration for the TOE comprises:

- Threat Intelligence Exchange (TIE) Server v2.0.0 Build 645
 - Installed on VMware vSphere 5.1.0 With ESXi 5.1, 5.5 or 6.0
- DXL 3.0.0 Build 285
 - Installed on VMware vSphere 5.1.0 With ESXi 5.1, 5.5 or 6.0
- ePolicy Orchestrator 5.3.2 build 156
 - Installed on A Windows Server 2012 R2 Platform
- McAfee Agent 5.0.4 build 283 for Windows managed systems
 - Installed on Windows 10 or Windows 2012 R2 Server

With support from the environment:

- Microsoft SQL Server 2008 R2
- Active Directory Server

4.1 DOCUMENTATION

The following documents are provided to the consumer to assist in the configuration and installation of the TOE:

- a. McAfee Threat Intelligence Exchange 2.0.0 and Data Exchange Layer 3.0.0 with ePolicy Orchestrator 5.3.2 Common Criteria Evaluated Configuration Guide, version 1.4
- b. Product Guide: McAfee ePolicy Orchestrator 5.3.0 Software
- c. User Guide: McAfee ePolicy Orchestrator 5.3.0 Software FIPS Mode
- d. Installation Guide: McAfee ePolicy Orchestrator 5.3.0 Software
- e. Product Guide: McAfee Agent 5.0.3 for use with McAfee ePolicy Orchestrator
- f. Product Guide: McAfee Threat Intelligence Exchange 2.0.0 for use with McAfee ePolicy Orchestrator
- g. Product Guide: McAfee Data Exchange Layer 3.0.0 for use with McAfee ePolicy Orchestrator
- h. Product Guide: McAfee VirusScan Enterprise 8.8 software Installation Guide: McAfee VirusScan Enterprise 8.8 software



5 EVALUATION ANALYSIS ACTIVITIES

The evaluation analysis activities involved a structured evaluation of the TOE. Documentation and process dealing with Development, Guidance Documents, and Life-Cycle Support were evaluated.

5.1 DEVELOPMENT

The evaluators analyzed the TOE 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 TOE 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.

5.2 GUIDANCE DOCUMENTS

The evaluators examined the TOE 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.

Section 4.1 provides details on the guidance documents.

5.3 LIFE-CYCLE SUPPORT

An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the TOE 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 the TOE during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the TOE. 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 TOE.



6 TESTING ACTIVITIES

Testing consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

6.1 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.

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.

6.2 CONDUCT OF TESTING

The TOE 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.

6.3 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. The following testing activities were performed:

- a. Repeat of Developer's Tests: The evaluator repeated a subset of the developers tests;
- b. Protection of data transfer between DXL Brokers: The evaluator confirmed that TSF data transferred between DXL brokers is protected.

6.3.1 FUNCTIONAL TEST RESULTS

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



6.4 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, FREAK, POODLE, and GHOST;
- b. Password Guessing: The evaluator attempted to compromise the security of the TOE by using weak password and then multiple attempts to login to the TOE; and
- c. Session Management: The evaluator attempted to compromise the security of the TOE by logging of the web interface and then attempting to load cached sessions and directly going to an admin webpage.

6.4.1 PENETRATION TEST RESULTS

The independent penetration testing did not uncover any exploitable vulnerabilities in the intended operating environment, provided all guidance is followed regarding the use of strong passwords as the TOE itself does not enforce a strong password policy or have a lockout setting.



7 RESULTS OF THE EVALUATION

This evaluation has provided the basis for the conformance claim documented in Table 1. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

The IT product identified in this report has been evaluated at an approved evaluation facility established under the Canadian Common Criteria Scheme using the Common Methodology for IT Security Evaluation, Version 3.1 Revision 4, for conformance to the Common Criteria for IT Security Evaluation, Version 3.1 Revision 4. These evaluation results apply only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report.

The evaluation has been conducted in accordance with the provisions of the Canadian Common Criteria Scheme and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This is not an endorsement of the IT product by CSE or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by CSE or by any other organization that recognizes or gives effect to this certificate, is expressed or implied.

7.1 EVALUATOR RECOMMENDATIONS/COMMENTS

It is recommended that all guidance outlined in Section 4.1 be followed to configure the TOE in the evaluated configuration, such as the guidance regarding strong passwords in Section 3.1.2 of the McAfee Threat Intelligence Exchange 2.0.0 and Data Exchange Layer 3.0.0 with ePolicy Orchestrator 5.3.2 Common Criteria Evaluated Configuration Guide, version 1.4 .



8 SUPPORTING CONTENT

8.1 LIST OF ABBREVIATIONS

Term	Definition
CAVP	Cryptographic Algorithm Validation Program
CCEF	Common Criteria Evaluation Facility
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
DXL	Data Exchange Layer
EAL	Evaluation Assurance Level
ePO	ePolicy Orchestrator
ETR	Evaluation Technical Report
GC	Government of Canada
IT	Information Technology
ITS	Information Technology Security
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories – Canada
PP	Protection Profile
SFR	Security Functional Requirement
ST	Security Target
TIE	Threat Intelligence Exchange
TOE	Target of Evaluation
TSF	TOE Security Function



8.2 REFERENCES

Reference
Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012.
Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012.
Security Target: McAfee Threat Intelligence Exchange 2.0.0 and Data Exchange Layer 3.0.0 with ePolicy Orchestrator 5.3.2, version 1.0, 23 November 2016
Evaluation Technical Report for McAfee Threat Intelligence Exchange 2.0.0 and Data Exchange Layer 3.0.0 with ePolicy Orchestrator 5.3.2, v1.0, 30 November 2016