



COMMON CRITERIA CERTIFICATION REPORT

McAfee Data Loss Prevention 11.0 with ePolicy Orchestrator 5.9.0

4 January 2018

383-4-429

Version 1.0





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.

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 Architecture	3
----------	------------------------	---

LIST OF TABLES

Table 1	TOE Identification	2
Table 2	Cryptographic Module(s).....	4



EXECUTIVE SUMMARY

McAfee Data Loss Prevention 11.0 with ePolicy Orchestrator 5.9.0 (hereafter referred to as the Target of Evaluation, or TOE), from McAfee, LLC., was the subject of this Common Criteria evaluation. A description of the TOE can be found in Section 1.2. The results of this evaluation demonstrate that TOE meets the requirements of the conformance claim listed in Table 1 for the evaluated security functionality.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed 4 January 2018 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 Canadian 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 Data Loss Prevention 11.0 with ePolicy Orchestrator 5.9.0
Developer	McAfee, LLC.
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

Data loss can occur when confidential or private information leaves an enterprise as a result of unauthorized communication through channels such as applications, physical devices, or network protocols. McAfee® Data Loss Prevention (DLP) is a suite of products that identify and protect data within the network. It provides an understanding of the types of data on a network, how the data is accessed and transmitted, and if the data contains sensitive or confidential information. DLP is used to build and implement effective protection policies, while reducing the need for extensive trial and error. DLP includes extensions for ePolicy Orchestrator (ePO) that add management features and reports to its capabilities.

1.3 TOE ARCHITECTURE

A diagram of the TOE architecture is as follows:

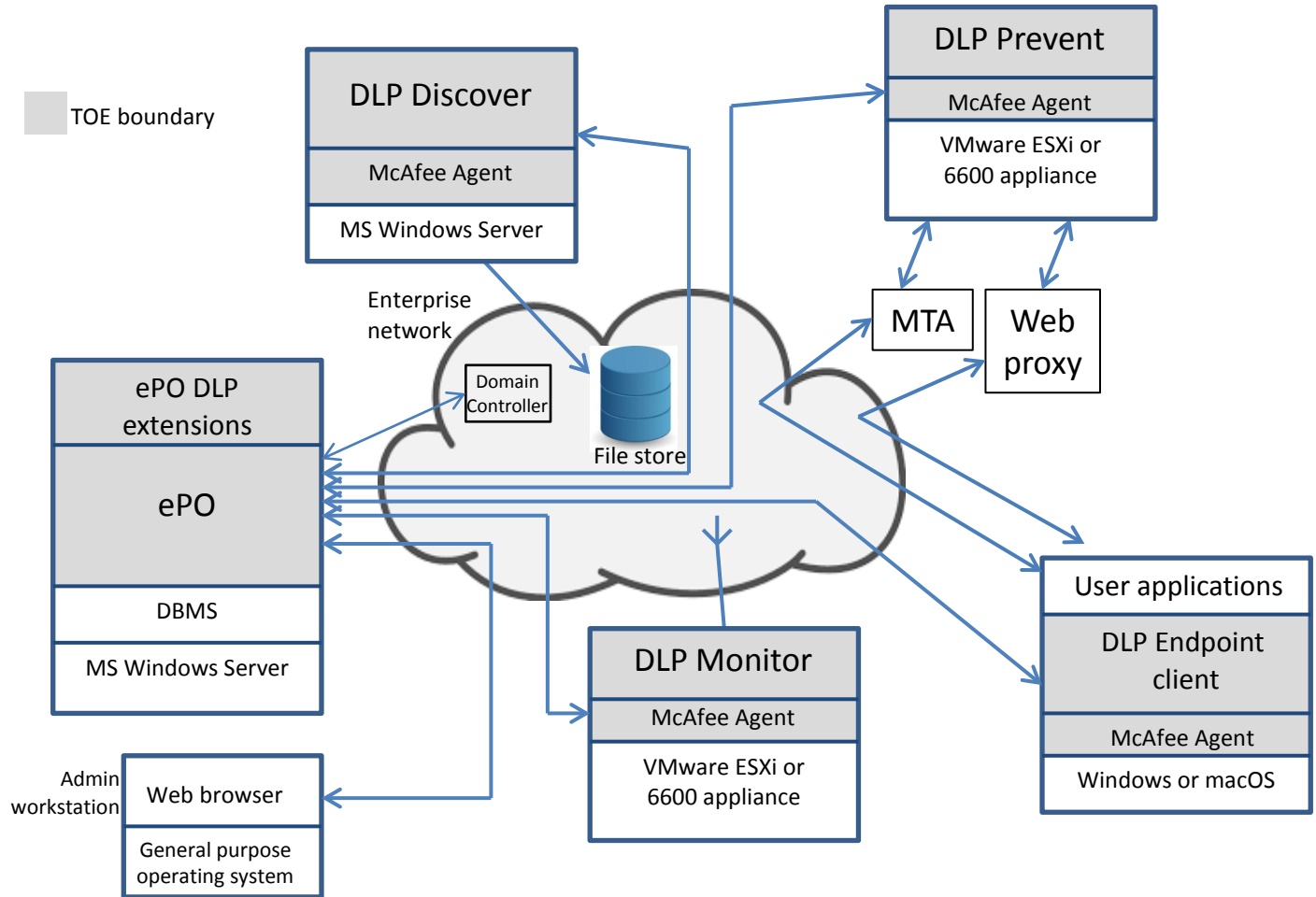


Figure 1 TOE Architecture



2 SECURITY POLICY

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

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management
- Cryptographic Support
- Protection of the TSF

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 used by the TOE:

Table 2 Cryptographic Module(s)

Cryptographic Module	Certificate Number
OpenSSL v1.0.2l	2398
RSA BSAFECrypto-C Micro Edition v4.0.1	2097



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:

- The TOE has appropriate access to the systems it is intended to manage;
- The MTA is configured to route email traffic via DLP Prevent, and to act on the header strings that DLP Prevent adds to the email messages;
- Access to the database used by the TOE via mechanisms outside the TOE boundary is restricted to authorized users;
- The authorized administrators 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; and
- The hardware, operating system, and other software on which the TOE depends, operate correctly.

3.2 CLARIFICATION OF SCOPE

Refer to the ST for the full functionality of the McAfee Agent, DLP Endpoint and Device Control as the components running on Apple software have limited capabilities as compared to Windows.



4 EVALUATED CONFIGURATION

The evaluated configuration for the TOE comprises:

- The TOE, McAfee Data Loss Prevention 11.0 with ePolicy Orchestrator 5.9.0, consists of the following software components:
 - ePO 5.9.0.732 with hotfix 1205305 management system residing on a compatible hardware platform running Windows Server 2012 R2 with Microsoft Internet Explorer 11.0.
 - DLP Discover 11.0.0.103 requires a Microsoft Windows 2008 R2 or 2012 R2 operating system and compatible hardware platform.
 - DLP Prevent 11.0.0.137 requires VMware vSphere ESXi 5.5 update 2 or 6.0 and compatible hardware platform, or a Model 6600 appliance hardware platform.
 - DLP Monitor 11.0.0.137 requires VMware vSphere ESXi 5.5 update 2 or 6.0 and compatible hardware platform, or a Model 6600 appliance hardware platform.
 - McAfee Agent 5.0.5.658.
 - DLP Endpoint and Device Control 11.0.2.32 (for Windows) and DLP Endpoint and Device Control 11.0.0.85 (for Mac) execute on one or more systems that are to be monitored. The client platforms within the scope of the evaluation are:
 - Windows 10 version 1607
 - Windows 2012 R2 Server
 - Apple macOS 10.12

4.1 DOCUMENTATION

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

- a. Product Guide: McAfee Data Loss Prevention 11.0.0 for use with McAfee ePolicy Orchestrator;
- b. Installation Guide McAfee ePolicy Orchestrator 5.9.0 Software;
- c. Product Guide for McAfee ePolicy Orchestrator 5.9.0 Software;
- d. Product Guide McAfee Agent 5.0.3;
- e. McAfee Data Loss Prevention 11.0 with ePolicy Orchestrator 5.9.0 Common Criteria Evaluated Configuration Guide;
- f. Release Notes for McAfee Data Loss Prevention 11.0;
- g. Release Notes for McAfee Agent 5.0.5; and
- h. Release Notes for McAfee ePolicy Orchestrator 5.9.0.



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 documentation provided by the vendor; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces and how the TSF implements the security functional requirements (SFRs). The evaluators determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained.

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 the developer for the TOE. 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 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. Security Management: The objective of this test goal is to confirm that a deleted user cannot access any of the management functions;
- c. Cryptographic Operations: The objective of this test goal is to confirm that communication between the ePO and the following TOE components is encrypted:
 - a. DLP Prevent;
 - b. DLP Monitor;
 - c. DLP Server; and
 - d. Discover Server.
- d. USB Block Rule: The objective of this test goal is to confirm that the TOE can block access to USB devices on managed endpoints;
- e. Email Rules: The objective of this test goal is to confirm that files can be blocked based on file names. Via the email protection rules functionality; and
- f. Classification of files: The objective of this test goal is to confirm that files can be classified based in different file types and conditions.



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; and
- b. Information Leakage Verification: The objective of this test goal is to monitor for data leakage during user login;
- c. Concurrent User Login: The objective of this test goal is to demonstrate that ePO can handle multiple concurrent logins; and
- d. Security Bypass: The objective of this test goal is to attempt to have the endpoint workstation attempt to uninstall the programs and stop running services in order to bypass the TOE restrictions.

6.4.1 PENETRATION TEST RESULTS

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



7 RESULTS OF THE EVALUATION

This evaluation has provided the basis for the conformance claim documented in Table 1. The overall verdict for this 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 RECOMMENDATIONS/COMMENTS

It is recommended that all guidance outlined in Section 4.1 be followed to configure the TOE in the evaluated configuration.



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
DLP	Data Loss Prevention
EAL	Evaluation Assurance Level
ePO	ePolicy Orchestrator
ETR	Evaluation Technical Report
GC	Government of Canada
IT	Information Technology
ITS	Information Technology Security
MTA	Message Transfer Agent (Server)
PP	Protection Profile
SFR	Security Functional Requirement
ST	Security Target
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.
McAfee Data Loss prevention 11.0 with ePolicy Orchestrator 5.9.0 Security Target, version 1.0, December 11, 2017.
Evaluation Technical Report for McAfee Data Loss prevention 11.0 with ePolicy Orchestrator 5.9.0, version 3.0. January 4, 2018.