Certification Report

EAL 3 Evaluation of McAfee® Hercules® Policy Auditor v4.5 and McAfee® Hercules® Remediation Manager v4.5

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-88-CR
Version: 1.1
Date: 11 April 2008
Pagination: i to v, 1 to 15

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 2.3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 2.3*. 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 Standard 17025, General requirements for the accreditation of calibration and testing 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 Electronic Warfare Associates-Canada, Ltd. located in Ottawa, Ontario.

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 April 11, 2008, 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 at: http://www.cse-cst.gc.ca/services/common-criteria/trusted-products-e.html and on the official Common Criteria Program website at http://www.commoncriteriaportal.org.

This certification report makes reference to the following trademarked or registered trademarks:

- McAfee® and Hercules® are registered trademarks of McAfee Inc. in the United States and other countries.
- Microsoft, Windows, Windows NT, Windows Server, and SQL Server are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.
- CVE is a trademark of MITRE Corporation.
- HP-UX is a trademark of Hewlett Packard Company in the United States,
- Intel and Pentium are registered trademarks of Intel.
- Linux is a registered trademark of Linus Torvalds Inc.
- Mac OS X is a registered trademark of Apple Computer Inc.
- Red Hat is a registered trademark of Red Hat Inc.
- Solaris is a trademark of Sun Microsystems, Inc. in the United States and other countries.
- UNIX is a registered trademark in the United States and other countries, exclusively licensed through X/Open Company, Ltd.
- AIX is a registered trademark of International Business Machines Corporation.

TABLE OF CONTENTS

Executive Summary

The McAfee® Hercules® Policy Auditor v4.5 and McAfee® Hercules® Remediation Manager v4.5, from McAfee® Inc, hereafter referred to as McAfee® Hercules®, is the Target of Evaluation for this Evaluation Assurance Level (EAL) 3 evaluation.

The McAfee® Hercules® product is designed to facilitate the automatic vulnerability remediation of devices (servers and workstations) on a network as well as the enforcement of connection policy based on remediation status.These functions can be performed on standard TCP/IP networks consisting of Microsoft® Windows®, Solaris™, Red Hat® Linux®, HP-UX®, AIX®, Tru64®, and Mac OS®X clients. The product imports vulnerability information from a number of third-party commercial vulnerability scanner products and consolidates this information into a single view of the vulnerabilities of each device in the network. The product provides a sequence of automatically executable remediation steps which will correct each recognized vulnerability. Users of the product may download new signatures from the 'V-Flash' server operated by McAfee®. The McAfee® Hercules® product provides an interface which allows users to view the listed vulnerabilities of devices on the network. Logical groupings of devices may be defined. An automatic remediation schedule may be defined for a group. In addition, a specific list of vulnerabilities to be remediated may be defined for the group.

Electronic Warfare Associates-Canada, Ltd. is the CCEF that conducted the evaluation. This evaluation was completed in April 2008 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 the McAfee® Hercules®, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the 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 3 assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 2.3* (with applicable final interpretations), for conformance to the *Common Criteria for Information Technology Security Evaluation, version 2.3*.

[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.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the McAfee® Hercules® 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 Evaluation Assurance Level (EAL) 3 evaluation is the McAfee® Hercules® Policy Auditor v4.5 and McAfee® Hercules® Remediation Manager v4.5, hereafter referred to as McAfee® Hercules®.

This report pertains to the TOE, which is comprised of the following main systems:

a. McAfee® Hercules® Administrator;
b. McAfee® Hercules® Server; and
c. McAfee® Hercules® Client.

2 TOE Description

The McAfee® Hercules® product is designed to facilitate the automatic vulnerability remediation of devices (servers and workstations) on a network as well as the enforcement of connection policy based on remediation status. These functions can be performed on standard TCP/IP networks consisting of Microsoft® Windows®, Solaris™, Red Hat® Linux®, HP-UX®, AIX®, Tru64®, and Mac OS®X clients. The product imports vulnerability information from a number of third-party commercial vulnerability scanner products and consolidates this information into a single view of the vulnerabilities of each device in the network. The product provides a sequence of automatically executable remediation steps which will correct each recognized vulnerability. Users of the product may download new signatures from the 'V-Flash' server operated by McAfee®. The McAfee® Hercules® product provides an interface which allows users to view the listed vulnerabilities of devices on the network. Logical groupings of devices may be defined. An automatic remediation schedule may be defined for a group. In addition, a specific list of vulnerabilities to be remediated may be defined for the group.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the McAfee® Hercules® is identified in Section 5 of the Security Target (ST).

4 Security Target

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

Title: Security Target, McAfee® Hercules® Policy Auditor and McAfee® Hercules® Remediation Manager (McAfee® Hercules®) Version 4.5
Version: 1.3
Date: 9 April 2008

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 2.3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, version 2.3*.

The McAfee® Hercules® 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 3 conformant, with all the assurance requirements in the EAL 3 package.

6 Security Policy

The McAfee® Hercules® implements role-based access control and information flow control policies to control user access to system resources and to control the flow of vulnerability and remediation data through the system. The TOE security functional policy details can be found in section 5.4 of the security target.

7 Assumptions and Clarification of Scope

Consumers of the McAfee® Hercules® product 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 are the assumptions about the environment of use of the TOE:

a. Personnel authorized to install, configure, and operate the McAfee® Hercules® possess appropriate training and will adhere to the procedures for secure usage of the product described in the ST.

b. Personnel authorized to install, configure, and operate McAfee® Hercules® will adhere to all organizational policies including standards regarding secure usage of computer resources including physical, network, and password security policies.

c. The organization operating McAfee® Hercules® has backup and recovery procedures in place such that McAfee® Hercules® may be recovered to a secure configuration if a hardware failure were to occur.

d. The TOE Administrator enforces all organizational password security policies when assigning user credentials to TOE users.

e. Organizational role-based access control policies are in place that determine which individuals are authorized as TOE users and a list of privileges that the user is permitted.

7.2 Environmental Assumptions

The following assumptions are made about the operating environment of the TOE:

a. The host machine upon which McAfee® Hercules® is installed resides in a physically secure location and only authorized individuals are granted physical access to the host.

b. The host machine upon which McAfee® Hercules® is installed resides in a secure networked environment.

c. The host operating system upon which the McAfee® Hercules® will reside has been installed, configured and security-hardened in accordance with the *McAfee® Hercules® Security Configuration Guide, Version 4.5, Revision 1.0*.

For more information about the TOE security environment, refer to Section 3 of the ST (TOE Security Environment).

7.3 Clarification of Scope

The McAfee® Hercules® offers protection against inadvertent or casual attempts to breach system security, by unsophisticated attackers possessing a low attack potential. It is not intended for situations which involve determined attempts by hostile or well-funded attackers using sophisticated attack techniques. The McAfee® Hercules® relies on the environment to provide it physical and logical protection.

8 Architectural Information

The McAfee® Hercules® is a software product comprising the following main components:

The McAfee® Hercules® Administrator Console. The McAfee® Hercules® Administrator Console provides the Human Machine Interface (HMI) for the product. It uses SSL-based communications with the McAfee® Hercules® Server(s), and has the ability to interact with Windows® user accounts, domain privileges and NTFS privileges. It authenticates (using Windows® integrated authentication) to Internet Information Server on the McAfee® Hercules® server. The McAfee® Hercules® Administrator Console is designed to be installed and used on a trusted and appropriately configured and controlled Windows® machine that is used for network administration. Users of the McAfee® Hercules® Administrator Console require full administrative privileges on the machine running the console as well as the McAfee® Hercules® Server and all client machines. The McAfee® Hercules® Administrator

Console provides the HMI for the product and includes the display and input devices through which the user interacts with the McAfee® Hercules® application. Information that can be gathered from this HMI includes connected client systems, client status, list of vulnerabilities that will be remediated on a particular client or group of clients, remediation status, remediation signatures, scanner data, and vulnerabilities found on clients.

The McAfee® Hercules® Server. The McAfee® Hercules® Server using a basic configuration comprises the McAfee® Hercules® Server, the McAfee® Hercules® Download Server, and the McAfee® Hercules® Channel Server Windows® service(s) that communicates with the McAfee® Hercules® Client to distribute remediation profiles and gather remediation progress data. Multiple McAfee® Hercules® Servers may be deployed within a network and administered from a single McAfee® Hercules® Administrator Console. The McAfee® Hercules® Server is designed to be installed and used on a trusted and appropriately configured and controlled Windows® server. This component also generates audit events in the log, including start, stop, successful actions and failed actions. The McAfee® Hercules® Server supports the export of user data for backup and transfer purposes as well as the import of remediation data, scanner data and device identifiers. Support for importing data in third-party vulnerability scanner data is also supported. Remediation data, remediation profiles and roles can be managed through this component. Remediation profiles can be approved and then the profile data, along with remediation data, can be pushed out to client systems. The Server receives remediation status back from the client. Remediation activities can be scheduled to be performed on a single client, or a group of clients.

The McAfee® Hercules® Windows®, Unix®, and Mac® Clients. The McAfee® Hercules® Windows®, Unix®, and Mac® clients are services that perform remediation activities on network devices such as workstations and servers. The clients establish HTTPS/SSL-based communication to the McAfee® Hercules® Server.

9 Evaluated Configuration

The McAfee® Hercules® includes two evaluated configurations: Standalone; and Distributed. The two configurations comprise the same functional components and differ only in packaging. To operate the TOE in the evaluated configuration, the various server components must be configured to use Secure Socket Layer (SSL) certificates as described in the McAfee® Hercules® Security Configuration Guide. The two configurations are described in detail in the ST Sections 2.1.2 and 2.1.3 respectively.

9.1 Stand Alone

McAfee® Hercules® Administrator Console. The McAfee® Hercules® Administrator Console executing on an Intel® Pentium compatible based PC running one of the following operating systems:

- Windows® 2000 Server with Service Pack 4,

- Windows® 2000 Advanced Server with Service Pack 4,
- Windows 2000 Professional with Service Pack 4,
- Windows® XP Professional with Service Pack 2,
- Windows® Server 2003 Standard Edition with Service Pack 1,
- Windows® Server 2003 Enterprise Edition with Service Pack 1, and
- Windows Vista Business or Windows Vista Enterprise.

The following software is also required for all configurations:

- Internet Explorer 5.5 or above,
- Microsoft .NET Framework v1.1 Service Pack 2, and Adobe Acrobat Reader™ 7.0 or higher are also required, and
- If the McAfee® Hercules® Administrator Console is running on Windows® 2000, the Windows® 2000 High Encryption Pack is required.

The minimum hardware requirements for the McAfee® Hercules® Administrator Console are specified in the McAfee® Hercules® Installation Guide. The required setup of the McAfee® Hercules® Administrator Console is described in the McAfee® Hercules® Security Configuration Guide.

McAfee® Hercules® Server. One or more McAfee® Hercules® Server(s) executing on an Intel® Pentium compatible based PC running one of the following operating systems:

- Windows® Server 2003 Standard Edition with Service Pack 1, and
- Windows® Server 2003 Enterprise Edition with Service Pack 1.

The following software is also required for all configurations:

- IIS 6.0
- Internet Explorer 6.0 and
- Microsoft SQL Server 2005,
- Microsoft Reporting Services,
- Microsoft .NET Framework v1.1 Service Pack 2, and
- Microsoft ASP.Net.

The minimum hardware requirements for a McAfee® Hercules® Server are specified in the McAfee® Hercules® Installation Guide. The required setup of a McAfee® Hercules® Server is described in the McAfee® Hercules® Security Configuration Guide.

McAfee® Hercules® Windows®, Unix®, and Mac® Clients. One or more network devices with McAfee® Hercules® Client Version 4.5 installed on either a supported Windows®, Unix®, and Mac® operating system.

Windows® Operating System

The supported Windows® operating systems are:

- Windows® NT 4.0 Workstation with Service Pack 6,
- Windows® NT 4.0 Standard Server with Service Pack 6,
- Windows® NT 4.0 Terminal Server with Service Pack 6,
- Windows® 2000 Professional,
- Windows® 2000 Server,
- Windows® 2000 Advanced Server,
- Windows® XP Professional,
- Windows® Server 2003 Standard Edition,
- Windows® Server 2003 Enterprise Edition,
- Windows® Vista Home Basic,
- Windows® Vista Home Premium,
- Windows® Vista Business,
- Windows® Vista Enterprise and
- Windows® Vista Ultimate.

For Windows® NT 4.0 platforms, Internet Explorer 5.5 with Service Pack 2 or above is also required. The minimum system requirements for Windows® clients are specified in the McAfee® Hercules® Enterprise Installation Guide.

Unix® operating system

The supported Unix® operating systems are:

- Solaris™ 2.6, 7, 8, 9, 10,
- Red Hat® Desktop 7.3, 8, 9,
- Red Hat® Enterprise Linux (AS, EW, WS) 2.1, 3.0, 4.0,
- AIX® 5.1, 5.2, 5.3,
- HPUX® 11.0, 11iv1, and
- Tru64® 5.1B.

The following software is required for all configurations:

- OpenSSH v3.5p1 or higher,
- SSL/HTTPS enabled with OpenSSL 0.96 or higher, and
- Sudo v1.6.7 or later.

The minimum system requirements for Unix® clients are specified in the McAfee® Hercules® Installation Guide.

Mac® operating system

The supported Mac® operating systems are Mac OS X 10.2, 10.3, and 10.4. The following software is required for all configurations:

- OpenSSH v3.5p1 or higher,

- SSL/HTTPS enabled with OpenSSL 0.96 or higher, and
- Sudo v1.6.7 or later.

The minimum system requirements for Mac® clients are specified in the McAfee® Hercules® Installation Guide.

9.2 Distributed Configuration

In this configuration, the McAfee® Hercules® Channel Server and the McAfee® Hercules® Download Server may be installed separately from the McAfee® Hercules® Server. The McAfee® Hercules® Channel Server and the McAfee® Hercules® Download Server have the same operating system support requirements as the McAfee® Hercules® Server. The configuration of the TOE is described in detail in the McAfee® Hercules® Installation Guide.

10 Documentation

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

a. McAfee® Hercules® Installation Guide;

b. McAfee® Hercules® QuickStart Guide;

c. McAfee® Hercules® Remedy Actions Reference;

d. McAfee® Hercules® Reporting Schema;

e. McAfee® Hercules® Security Configuration Guide;

f. McAfee® Hercules® Product Guide;

g. McAfee® Hercules® Vulnerability Assessment and Remediation Overview;

h. Creating Network Install Package for Microsoft Internet Explorer 6.0; and

i. Using Hercules and Administrative Network Installation Points to Remediate Microsoft® Office 2000.

These documents are provided in Adobe PDF format on the shipped CD.

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the McAfee® Hercules®, including the following areas:

Configuration management: An analysis of the McAfee® Hercules® development environment and associated documentation was performed. The evaluators found that the

McAfee® Hercules® configuration items were clearly marked, and could be modified and controlled. The developer's configuration management system was observed during a site visit, and it was found to be mature and well developed.

Secure delivery and operation: The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of the McAfee® Hercules® during distribution to the consumer. The evaluators examined and tested the installation, generation and start-up procedures, and determined that they were complete and sufficiently detailed to result in a secure configuration.

Design documentation: The evaluators analysed the McAfee® Hercules® functional specification and high-level design; they determined that the documents were internally consistent, and completely and accurately instantiated all interfaces and security functions. The evaluators also independently verified that the correspondence mappings between the design documents were correct.

Guidance documents: The evaluators examined the McAfee® Hercules® user and administrator guidance documentation and determined that it sufficiently and unambiguously described how to securely use and administer the product, and that it was consistent with the other documents supplied for evaluation.

Life-cycle support: The evaluators assessed the development security procedures during a site visit and determined that they detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the McAfee® Hercules® design and implementation.

Vulnerability assessment: The McAfee® Hercules® ST's strength of function claims were validated through independent evaluator analysis. The evaluators examined the developer's vulnerability analysis for the McAfee® Hercules® and found that it sufficiently described each of the potential vulnerabilities along with a sound rationale as to why it was not exploitable in the intended environment. Additionally, the evaluators conducted an independent review of public domain vulnerability databases, and all evaluation deliverables to provide assurance that the developer has considered all potential vulnerabilities. Penetration testing was conducted by evaluators, which did not expose any residual vulnerabilities that would be exploitable in the intended operating environment for the TOE.

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

12 ITS Product Testing

Testing consists of the following three areas: coverage, functional tests, independent testing. The evaluators examined the developer's testing activities and verified that the developer has met their testing responsibilities.

12.1 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].

McAfee® employs a rigorous testing process that tests the changes and fixes in each release of the McAfee® Hercules®. Comprehensive regression testing is conducted for all releases.

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.

12.2 Independent Functional Testing

During this evaluation, the evaluators 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 was the following list of Electronic Warfare Associates-Canada, Ltd. test goals:

a. Initialization: The objective of this test goal is to provide the procedures for determining the system configuration in order to ensure that the TOE that is tested is correct;

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

c. Identification and Authentication: The objective of this test goal is to ensure that the identification and authentication requirements have been met;

d. Audit: The objective of this test goal is to ensure that the audit data is recorded and can be viewed;

e. Users and Roles: The objective of this test goal is to ensure the users and roles functionality is correct;

f. User Data Protection: The objective of this test goal is to determine the TOE's ability to protect user data; and

[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.

g. Basic Product Functionality: The objective of this test goal is to exercise the TOE's functionality to ensure that the security claims may not be inadvertently compromised.

12.3 Independent Penetration Testing

Subsequent to the examination of the developer's vulnerability analysis, limited independent evaluator penetration testing was conducted. The penetration tests focused on the following:

- Generic vulnerabilities,
- Port scanning,
- Monitoring network traffic,
- Misuse testing by the TOE user (network injection and SQL injection), and
- Misuse testing by an outsider (buffer overflow attacks and password capture).

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

12.4 Conduct of Testing

The McAfee® Hercules® was subjected to a comprehensive suite of formally documented independent functional tests. The testing took place at the Information Technology Security Evaluation and Test (ITSET) Facility at Electronic Warfare Associates-Canada, Ltd. 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.

12.5 Testing Results

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

13 Results of the Evaluation

This evaluation has provided the basis for an **EAL 3** level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

14 Evaluator Comments, Observations and Recommendations

The complete documentation for the McAfee® Hercules® includes a comprehensive Installation Guide, Security Configuration Guide and Product Guide.

The McAfee® Hercules® is straightforward to configure, use and integrate into a corporate network.

McAfee® Inc.'s Configuration Management (CM) and Quality Assurance (QA) provide the requisite controls for managing all CM/QA activities.

15 Acronyms, Abbreviations and Initializations

This section expands any acronyms, abbreviations and initializations used in this report.

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
CVE	Common Vulnerabilities and Exposures
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
HMI	Human Machine Interface
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
NTFS	NT File System
OS	Operating System
PALCAN	Program for the Accreditation of Laboratories Canada
QA	Quality Assurance
SFP	Security Function Policy
SQL	Structured Query Language
SSL	Secure Socket Layer
ST	Security Target
TOE	Target of Evaluation

16 References

This section lists all documentation used as source material for this report:

a. Canadian Common Criteria Evaluation and Certification Scheme (CCS) Publication #4, Technical Oversight, Version 1.0.

b. Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 2.3, August 2005.

d. McAfee® Hercules® Policy Auditor and McAfee® Hercules® Remediation Manager (McAfee® Hercules®) Version 4.5 Security Target, Version No. 1.3, 9 April 2008.

e. Evaluation Technical Report (ETR) McAfee® Hercules® Policy Auditor v4.5 and McAfee® Hercules® Remediation Manager v4.5, EAL 3 Evaluation, Common Criteria Evaluation Number: 383-4-88, Document No. 1566-000-D002, Version 1.1, 10 April 2008.