Certification Report

EAL 2+ Evaluation of Symantec™ Endpoint Protection

Version 11.0

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-84
Version: 1.0
Date: 25 June 2008
Pagination: i to iv, 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 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 EWA-Canada 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 25 June 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 http://www.commoncriteriaportal.es

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

- Symantec is a registered trademark of Symantec Corporation.
- Microsoft, Windows Vista, Windows Server 2003, Windows 2000 and Windows XP are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.

TABLE OF CONTENTS

Executive Summary

The Symantec™ Endpoint Protection version 11.0, from Symantec Corporation, is the Target of Evaluation for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

Symantec™ Endpoint Protection combines Symantec AntiVirus™ with advanced threat prevention to deliver defense against malware such as memory and file-based viruses, rootkits, zero-day attacks, and mutating spyware on laptops, desktops or servers.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 24 June 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 Symantec™ Endpoint Protection, 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 2 augmented 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*. The following augmentations are claimed:

a. ALC_FLR.2 – Flaw reporting procedures; and

b. AVA_MSU.1 – Examination of guidance.

The Security Target claims conformance to the security requirements, security objectives, and security environment statements for the defined TOE and its environment as they are stated in the U.S. Government Protection Profile for Anti-Virus Applications for Workstations in Basic Robustness Environments, Version 1.1, April 4, 2006.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the Symantec™ Endpoint Protection 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 Symantec™ Endpoint Protection version 11.0 from Symantec Corporation.

2 TOE Description

Symantec™ Endpoint Protection version 11.0 combines Symantec AntiVirus™ with advanced threat prevention to deliver defense against malware such as memory and file-based viruses, rootkits, zero-day attacks, and mutating spyware on laptops, desktops or servers.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for Symantec™ Endpoint Protection version 11.0 is identified in Section 5 of the Security Target (ST).

The TOE implements FIPS-approved cryptographic functionality. The following Government of Canada approved algorithm was evaluated for correct implementation in Symantec™ Endpoint Protection:

Algorithm: Secure Hash Algorithm (SHA-1)
Standard: FIPS 180-2
Certificate #: 248

4 Security Target

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

Title: Security Target: Symantec™ Endpoint Protection version 11.0
Version: 1.6
Date: 02 June 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 Symantec™ Endpoint Protection version 11.0 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:
    - FAV_ACT_EXP.1 – Antivirus Actions,
    - FAV_ALR_EXP.1 – Antivirus Alerts,

- FAV_SCN_EXP.1 – Antivirus Scanning,
- FPT_SEP_EXP.1- Partial TSF Domain Separation,
- FIA_PLA_EXP.1 – Performance and Log Alerts;

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 the security assurance requirements in the EAL 2 package, as well as the following: ALC_FLR.2 – Flaw Reporting Procedures and AVA_MSU.1 – Examination of Guidance.

Symantec™ Endpoint Protection version 11.0 conforms with the U.S. Government Protection Profile for Anti-Virus Applications for Workstations in Basic Robustness Environments, Version 1.1, April 4, 2006.

6 Security Policy

Symantec™ Endpoint Protection version 11.0 implements an anti-virus security policy. The TOE is designed to help prevent memory-based and file-based viruses. If a memory-based virus is detected on a host machine, the TOE will prevent the virus from further execution. The TOE also provides for administrator-defined actions upon the detection of a virus-infected file. The administrator can configure the TOE to clean the file, quarantine the file, delete the file, or take no action on the file.

In addition, Symantec™ Endpoint Protection implements security policies pertaining to security audit, cryptographic support, protection of the TOE Security Functions (TSF) and security management. Further details on these security policies may be found in Sections 5 and 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of Symantec™ Endpoint Protection version 11.0 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:

a) Administrators will back up the audit files and monitor disk usage to ensure audit information is not lost.

b) Administrators are non-hostile, appropriately trained, and follow all administrator guidance.

c) Administrators will implement secure mechanisms for receiving and validating updated signature files from the anti-virus vendors, and for distributing the updates to the central management systems.

7.2 Environmental Assumptions

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

a) It is assumed that appropriate physical security is provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.

b) The IT environment will provide a secure line of communications between distributed portions of the TOE and between the TOE and remote administrators.

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

7.3 Clarification of Scope

The TOE is assured to provide effective security measures in a co-operative non-hostile environment only if it is installed, managed, and used correctly. The operational environment must be managed in accordance with assurance requirements documentation for delivery, operation, and user/administrator guidance.

The Symantec™ Endpoint Protection version 11.0 relies on the environment to provide it physical and logical protection.

8 Architectural Information

The TOE architecture comprises the following three components:

- **Symantec™ Endpoint Protection Client**. The Symantec™ Endpoint Protection version 11.0 client software protects laptops, desktops and servers on an internal network. It performs the anti-virus scanning and file deletion/quarantine functionality of the TOE.

- **Symantec™ Endpoint Protection Manager**. The Symantec™ Endpoint Protection version 11.0 Manager component provides the core management functionality of the TOE including generating reports, managing policies, installing clients and configuring administrative accounts and actions.

- **Symantec™ Endpoint Protection Management Console**. The Symantec™ Endpoint Protection version 11.0 Management console provides the Graphical User Interface (GUI) which allows the TOE operator to configure and administer the Symantec™ Endpoint Protection Manager.

9 Evaluated Configuration

The evaluated configuration for Symantec™ Endpoint Protection version 11.0 comprises:

- Symantec Endpoint Protection Client Version 11.0776.942 running on Microsoft Windows® Vista, Microsoft Windows® Server 2003 Service Pack 1, Microsoft Windows® XP Service Pack 2 or Microsoft Windows® 2000 Service Pack 3 and higher; and

- Symantec™ Endpoint Protection Manager Version 11.0.780.1109 running on Microsoft Windows® Server 2003 SP1, Microsoft Windows® XP Service Pack 2 or Microsoft Windows® 2000 Service Pack 3 and higher.

10 Documentation

The Symantec documents provided to the consumer are as follows:

a. Symantec™ Endpoint Protection Getting Started Guide, PN: 12167130;

b. Installation Guide for Symantec™ Endpoint Protection and Symantec™ Network Access Control, Documentation version 11.00.00.00.00;

c. Administration Guide for Symantec™ Endpoint Protection and Symantec™ Network Access Control, Documentation version 11.00.00.00.03;

d. Client Guide for Symantec™ Endpoint Protection and Symantec™ Network Access Control, Documentation version 11.00.00.00.02;

e. Symantec™ Endpoint Protection readme.txt, September 2007; and

f. Administrative Guidance and Installation, Generation, and Startup Procedures: Symantec™ Endpoint Protection Version 11.0.

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the Symantec™ Endpoint Protection version 11.0, including the following areas:

Configuration management: An analysis of Symantec™ Endpoint Protection version 11.0 configuration management system and associated documentation was performed. The evaluators found that Symantec™ Endpoint Protection version 11.0 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.

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

Symantec™ Endpoint Protection version 11.0 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 Symantec™ Endpoint Protection version 11.0 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 Symantec™ Endpoint Protection version 11.0 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 reviewed the flaw remediation procedures used by Symantec for the Symantec™ Endpoint Protection version 11.0. 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 Symantec™ Endpoint Protection version 11.0 ST's strength of function claims were validated through independent evaluator analysis. The evaluators examined the developer's vulnerability analysis for the Symantec™ Endpoint Protection version 11.0 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. The evaluators also examined the guidance and other evaluation evidence to determine that the guidance identifies all possible modes of operation of the TOE, their consequences and implications for maintaining secure operation.

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

12 ITS Product Testing

Testing at EAL 2 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

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].

Symantec employs a rigorous testing process that tests the changes and fixes in each release of Symantec™ Endpoint Protection version 11.0. 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 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 was 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 provide the procedures for determining the system configuration in order to ensure that the TOE that is tested is correct;

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

d. Users and Roles: The objective of this test goal is to ensure the users and roles functionality (account creation, account deletion and role assignment) performed by the TOE is correct; and

e. Antivirus: The objective of this test goal is to test the antivirus functionality. Test cases focused on antivirus actions and scanning performed by the TOE and antivirus alerts generated by the TOE.

[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.

12.3 Independent Penetration Testing

Subsequent to the examination of the developer's vulnerability analysis and the independent review of public domain vulnerability databases and all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on:

- Generic vulnerabilities;
- Bypassing;
- Tampering; and
- Direct attacks

The evaluator conducted a port scan of the Symantec™ Endpoint Protection version 11.0. The only ports found to be open were ones that would be expected to be. The evaluator used a publicly available tool to scan Symantec™ Endpoint Protection version 11.0 for weaknesses, and none were found. The evaluator also used a publicly available packet capture tool to examine output from Symantec™ Endpoint Protection version 11.0 during startup, shutdown and normal operations. The evaluator searched the captured results in an attempt to extract information which might be useful to a potential attacker; no useful information was uncovered.

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

12.4 Conduct of Testing

The Symantec™ Endpoint Protection version 11.0 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.

12.5 Testing Results

The developer’s tests and the independent functional tests yielded the expected results, giving assurance that the Symantec™ Endpoint Protection behaves as specified in its ST and functional specification.

13 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.

14 Evaluator Comments, Observations and Recommendations

The complete documentation for the Symantec™ Endpoint Protection version 11.0 includes a comprehensive Installation and Security Guide and a User's Guide.

The Symantec™ Endpoint Protection version 11.0 is straightforward to configure, use and integrate into a corporate network.

15 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
GUI	Graphical User Interface
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories Canada
SHA-1	Secure Hash Algorithm
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

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. Security Target: Symantec™ Endpoint Protection version 11.0, Version 1.6, 02 June 2008.

e. Evaluation Technical Report (ETR) Symantec™ Endpoint Protection, EAL 2+ Evaluation, Common Criteria Evaluation Number: 383-4-84, Document No. 1569-000-D002, Version 1.5, 24 June 2008.