Certification Report

EAL 2+ Evaluation of Symantec™ Endpoint Protection Version 12.1.2

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-217-CR
Version: 1.0
Date: 20 May 2013
Pagination: i to iii, 1 to 11

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved evaluation facility – established under the Canadian Common Criteria Evaluation and Certification Scheme (CCS) – using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 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/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 EWA-Canada.

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 20 May 2013, and the security target identified in Section 4 of this report.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

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

- Symantec™ is a registered trademark of Symantec Corporation.

TABLE OF CONTENTS

Executive Summary

Symantec™ Endpoint Protection Version 12.1.2 (hereafter referred to as SEP v12.1.2), from Symantec Corporation, is the Target of Evaluation for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

SEP v12.1.2 is an antivirus application running on workstations (e.g., desktops and laptops), along with a management component running on a central server to control and monitor execution of the antivirus application.

SEP v12.1.2 combines Symantec Antivirus with advanced threat prevention to deliver a defense against malware for laptops, desktops, and servers. It provides protection against sophisticated attacks that evade traditional security measures, such as rootkits, zero-day attacks, and mutating spyware.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 5 March 2013 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 SEP v12.1.2, the security requirements, and the level of confidence (evaluation assurance level) to which it is asserted that the product satisfies its 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 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3.* The following augmentation is claimed: ALC_FLR.2 – Flaw reporting procedures.

SEP v12.1.2 is conformant to the U.S. Government Protection Profile Anti-Virus Applications for Workstations in Basic Robustness Environments, version 1.2, dated 25 July 2007.

[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 SEP v12.1.2 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) 2 augmented evaluation is Symantec™ Endpoint Protection Version 12.1.2 (hereafter referred to as SEP v12.1.2), from Symantec Corporation.

2 TOE Description

SEP v12.1.2 is an antivirus application running on workstations (e.g., desktops and laptops), along with a management component running on a central server to control and monitor execution of the antivirus application.

SEP v12.1.2 combines Symantec Antivirus with advanced threat prevention to deliver a defense against malware for laptops, desktops, and servers. It provides protection against sophisticated attacks that evade traditional security measures, such as rootkits, zero-day attacks, and mutating spyware.

A detailed description of the SEP v12.1.2 architecture is found in Section 1.7 of the Security Target (ST).

3 Evaluated Security Functionality

The complete list of evaluated security functionality for SEP v12.1.2 is identified in Section 6.1 of the ST.

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

Cryptographic Module	**Certificate #**
Windows XP Enhanced Cryptographic Provider (RSAENH) (Software Version: 5.1.2600.5507)	*#989*
Windows Server 2003 Enhanced Cryptographic Provider (RSAENH) (Software Version: 5.2.3790.4313)	*#1012*
Windows Server 2003 Enhanced Cryptographic Provider (RSAENH) (Software Version: 5.2.3790.3959)	*#868*
Windows Server 2003 Enhanced Cryptographic Provider (RSAENH) (Software Versions 5.2.3790.0 and 5.2.3790.1830 [Service Pack 1])	*#382*
Windows Server 2008 Enhanced Cryptographic Provider (RSAENH) (Software Versions: 6.0.6001.22202 and 6.0.6002.18005)	*#1010*

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in SEP v12.1.2:

Cryptographic Algorithm	**Standard**	**Certificate #**
Secure Hash Algorithm (SHA-1)	FIPS 180-2	176, 613, 753, 816, 1081

4 Security Target

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

Title: Security Target Symantec™ Endpoint Protection Version 12.1.2
Version: 0.8
Date: 13 February 2013

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3.*

SEP v12.1.2 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_(EXT).1 - Anti-Virus Actions
    - FAV_ALR_(EXT).1 - Anti-Virus Alerts
    - FAV_SCN_(EXT).1 - Anti-Virus Scanning
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 security assurance requirements in the EAL 2 package, as well as the following: ALC_FLR.2 – Flaw reporting procedures
d. SEP v12.1.2 is conformant with the U.S. Government Protection Profile Anti-Virus Applications for Workstations in Basic Robustness Environments, version 1.2, dated 25 July 2007.*5*.

6 Security Policy

SEP v12.1.2 implements a role-based access control policy to control user access to the system, detail of this security policy can be found in Section 7.1 of the ST.

In addition, SEP v12.1.2 implements other policies pertaining to security audit. Further details on these security policies may be found in Section 7.1 of the ST.

7 Assumptions and Clarification of Scope

Consumers of SEP v12.1.2 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:

- Administrators will back up audit files and monitor disk usage to ensure audit information is not lost.
- Administrators are non-hostile, appropriately trained, and follow all administrative guidance.
- 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 Environmental Assumptions are listed in the ST:

- The TOE receives alarms from the IT Environment to signal when audit logs are nearing capacity.
- The IT environment will provide a separate domain for the TOE's operation.
- The IT environment will ensure the TSF cannot be bypassed.
- The 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.
- The IT environment will provide a secure line of communications between distributed portions of the TOE and between the TOE and remote administrators.

7.3 Clarification of Scope

SEP v12.1.2 offers protection against inadvertent or casual attempts to breach system security by unsophisticated attackers possessing basic attack potential. SEP v12.1.2 is not intended for situations which involve determined attempts by hostile or well-funded attackers using sophisticated attack techniques.

8 Evaluated Configuration

The evaluated configuration for SEP v12.1.2 comprises:

Management system	• Windows XP (32-bit, SP-3, 64-bit, all SPs), • Windows Server 2003 (32-bit, 64-bit, R2, SP1), • Windows Server 2008 (32-bit, 64-bit)
	• 1 GB of RAM • Hard disk: 4 GB or more free space • Java Runtime Environment 1.6.0.u24 • Apache Tomcat 6.0.32 • Apache HTTP Server 2.2.16
Client systems	• Windows XP (32-bit, SP-3, 64-bit, all SPs), • Windows XP Embedded (SP-3), • Windows Vista (32-bit, 64-bit), • Windows 7 (32-bit, 64-bit), • Windows 7 Embedded, Windows Server 2003 (32-bit, 64-bit, R2, SP-2), • Windows Server 2008 (32-bit, 64-bit), • Windows Small Business Server 2011 (64-bit), or • Windows Essential Business Server 2008 (64-bit), • Mac OS X 10.5 or 10.6 (32-bit, 64-bit only), • Mac OS X Server 10.5 or 10.6 (32-bit, 64-bit)

The publication entitled Operational and User Guidance and Preparative Procedures Supplement Symantec Endpoint Protection Version 12.1, Document Version 1.4, February 11, 2013 describes the procedures necessary to install and operate SEP v12.1.2 in its evaluated configuration.

9 Documentation

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

a. Symantec™ Endpoint Protection and Symantec Network Access Control Implementation Guide, Document Version 12.01.00.00.00, 2011; and

b. Operational and User Guidance and Preparative Procedures Supplement Symantec Endpoint Protection Version 12.1, Document Version 1.4, February 11, 2013

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of SEP v12.1.2, including the following areas:

Development: The evaluators analyzed the SEP v12.1.2 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 SEP v12.1.2 security architectural description and determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the SEP v12.1.2 preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance, and determined that they are complete and sufficiently detailed to result in a secure configuration.

Life-cycle support: An analysis of the SEP v12.1.2 configuration management system and associated documentation was performed. The evaluators found that the SEP v12.1.2 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.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of SEP v12.1.2 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for SEP v12.1.2. 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 evaluators conducted an independent vulnerability analysis of SEP v12.1.2. Additionally, the evaluators conducted a search of public domain vulnerability databases to identify SEP v12.1.2 potential vulnerabilities. The evaluators identified potential vulnerabilities for testing applicable to SEP v12.1.2 in its operational environment.

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

11 ITS Product Testing

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

11.1 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].

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.

[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.

11.2 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 is 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. Account creation/deletion: The objective of this test goal is to confirm the creation and deletion of administrator accounts;

c. Audit: The objective of this test goal is to confirm that audit records are created for the various events detected by the TOE and that they can be reviewed; and

d. Antivirus: The objective of this test goal is to confirm that the TOE can scan e-mail messages and that the TOE reacts accordingly.

11.3 Independent Penetration Testing

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

a. Port Scan: The objective of this test goal is to scan the TOE using a port scanner to identify open ports for potential issues;

b. Vulnerability Identification: Tool Scanning: The objective of this test goal is to scan the TOE for vulnerabilities using automated tools;

c. Information Leakage Verification: The objective of this test goal is to monitor the TOE for leakage during start-up, shutdown, login, and other scenarios using a packet sniffer; and

d. SQL Injection: The objective of this test goal is to determine if the TOE is vulnerable to SQL injection attacks.

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

11.4 Conduct of Testing

SEP v12.1.2 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.

11.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that SEP v12.1.2 behaves as specified in its ST and functional specification.

12 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.

13 Acronyms, Abbreviations and Initializations

Include acronyms, abbreviations, initializations used in the CR, e.g.

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
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories - Canada
ST	Security Target
TOE	Target of Evaluation

14 References

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

a. CCS Publication #4, Technical Oversight, Version 1.8, October 2010.

b. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 3, July 2009.

d. US Government Protection Profile: Anti-Virus Applications for Workstations in Basic Robustness Environments, 1.2, 25-JUL-2007

e. Security Target Symantec™ Endpoint Protection Version 12.1.2, 0.8, 13 February 2013.

f. Evaluation Technical Report for EAL 2+ Common Criteria Evaluation of Symantec Corporation Symantec™ Endpoint Protection Version 12.1.2, Version 1.0, 5 March 2013.