Certification Report

EAL 2 Evaluation of

Symantec™ Security Information Manager Version 4.5

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

© 2007 Government of Canada, Communications Security Establishment

Document number:	383-4-71-CR
Version:	0.8
Date:	12 September 2007
Pagination:	i to iv, 1 to 09

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 (CSE), 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 CSE, 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 (CSE).

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 10 September 2007, 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 Common Criteria Portal list of evaluated products at: http://www.commoncriteriaportal.org/

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

- Symantec is a registered trademark of Symantec Corporation
- Linux is a registered trademark of Linus Torvalds. Inc.
- Red Hat is a registered trademark of Red Hat, Inc.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

TABLE OF CONTENTS

Executive Summary

The Symantec™ Security Information Manager Version 4.5, from Symantec Corporation (hereafter referred to as SSIM), is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 evaluation.

The SSIM provides the ability to analyze historical security events and generate reports on security metrics in support of satisfying security policy compliance needs. The SSIM provides real-time event correlation and data archiving to protect against security threats and to preserve critical security data. The SSIM collects, analyzes, and archives information from security devices, critical applications, and services.

Electronic Warfare Associates-Canada, Ltd. is the CCEF that conducted the evaluation. This evaluation was completed on 29 August 2007 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 SSIM, 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 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*.

CSE, as the CCS Certification Body, declares that the SSIM 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) at http://www.cse-cst.gc.ca/services/common-criteria/trusted-products-e.html and on the official International Common Criteria Program website at http://www.commoncriteriaportal.org.

[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 evaluation is the Symantec™ Security Information Manager Version 4.5 (hereafter referred to as SSIM), from Symantec Corporation.

2 TOE Description

The SSIM provides the ability to analyze historical security events and generate reports on security metrics in support of satisfying security policy compliance needs. The SSIM provides real-time event correlation and data archiving to protect against security threats and to preserve critical security data. The SSIM collects, analyzes, and archives information from security devices, critical applications, and services.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the SSIM 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 for Common Criteria Evaluation: Symantec™ Security Information Manager Version 4.5
Version: Version 1.7
Date: 24 August 2007

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 SSIM is:

a. Common Criteria Part 2 extended, with security functional requirements based upon functional components in Part 2, as well as the following:
    - SIM_ANL.1 Event Analysis
    - SIM_RES.1 Incident Resolution

b. Common Criteria Part 3 conformant, with security assurance requirements based only upon assurance components in Part 3; and

c. Common Criteria EAL 2 conformant, containing all security assurance requirements from EAL 2.

6 Security Policy

The TOE implements the Administrative Access Control SFP. This SFP determines and enforces the privileges associated with operator roles. An authorized administrator can define specific services available to administrators and users via the Management Console.

In addition, the SSIM implements policies pertaining to security audit, user data protection, identification and authentication, and security management. Further details on these security policies may be found in Section 5 of the ST.

7 Assumptions and Clarification of Scope

Consumers of the SSIM 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

Personnel authorized to install, configure, and operate the SSIM possess appropriate training, are not hostile, and will adhere to the procedures for secure usage of the product.

7.2 Environmental Assumptions

The SSIM resides within controlled access facilities, which will prevent unauthorized physical access.

7.3 Clarification of Scope

The SSIM relies on the environment to provide it physical and logical protection. The SSIM provides a level of protection that is appropriate for low robustness environments handling sensitive data. It offers protection against inadvertent or casual attempts to breach system security. It is not intended for situations in which hostile and well-funded attackers use sophisticated attacks from within the physical zone.

8 Architectural Information

The SSIM is composed of the following component subsystems:

- ***Agent*** - Facilitates communicating configuration information and event data between the Event Service and the Event Collector;
- ***Configuration Service*** - Responsible for configuration of the TOE;

- ***Correlation Engine*** - Provides filters rules to generate correlations in multiple events and creates incidents when a rule is fired. This component also provides all incident management functions;

- ***Database*** - Stores configuration information, event logs, and reports in addition to events, correlated events, conclusions, and incidents;

- ***Event Collector*** - Receives inbound events from sensors and forwards to the Agent for processing;

- ***Event Service*** - Communicates with Agent to push updated configurations and to receive events for processing and forwarding to the Correlation Engine;

- ***Management Console*** - Allows configuration as well as review of configuration settings and reports. There are two console management interfaces: one is web-based and the other is Java-based. The web-based console is used to configure local items specific to the appliance (such as network settings, date/time, etc.). The Java-based console is used to view incidents, tickets, events and is also used in user & role administration. This application is part of the Information Manager software and downloaded to a workstation via a Web-browser; and

- ***Sensor*** - Receives events from point products attached to the network and forwards to the Event Collector for aggregation.

9 Evaluated Configuration

The evaluated configuration for the SSIM comprises:

- SSIM 9650 running on SSIM Version 4.5.0.113 with Linux-based Operating System, Red Hat version 4.0 running with Linux Kernel v2.6; and

- A PC Computer running on Windows 2000 Pro SP4, Windows XP SP2, Windows 2003 Server SP1 or Windows 2000 Advanced Server SP4, with any number of User Interactive Programs and Third-party Applications installed and running.

10 Documentation

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

a. Symantec™ Security Information Manager 4.5 Installation Guide, 2006;

b. Symantec™ Security Information Manager 4.5 Administrator's Guide;

c. Symantec™ Security Information Manager 4.5 User's Guide;

d. Symantec™ Security Information Manager 4.5 Release Notes; and

e. Administrative Guidance and Installation, Generation and Startup Procedures: Symantec™ Security Information Manager 4.5.

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the SSIM, including the following areas:

Configuration management: An analysis of the SSIM CM system and associated documentation was performed. The evaluators found that the SSIM 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 SSIM 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 SSIM 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 SSIM 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.

Vulnerability assessment: The SSIM ST's strength of function claims were validated through independent evaluator analysis. The evaluators examined the developer's vulnerability analysis for the SSIM 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.

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

12 ITS Product Testing

Testing at EAL 2 consists of the following three steps: assessing developers 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 the SSIM. 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. The following areas were tested:

a. Product Initialization;

b. Identification and Authentication;

c. Audit;

d. Users and Roles;

e. User Data Protection; and

f. Basic Product Functionality.

[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 SSIM. The only ports found to be open were ones that would be expected to be. The evaluator used a publicly available tool to scan the SSIM for weaknesses, and none were found. The evaluator also used a publicly available packet capture tool to examine output from the SSIM 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 SSIM 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 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 SSIM 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 SSIM includes a comprehensive Installation and Security Guide, an Administrator’s Guide and an User’s Guide.

The SSIM is straightforward to configure, use and integrate into a corporate network.

Symantec is strongly committed to secure practices, the CC effort and effective configuration management and delivery processes as evidenced by the high-quality of the CC evaluation evidence and its practical application for the SSIM project.

Though life-cycle support development security is not part of this evaluation, the evaluator observed that Symantec is particularly conscious of security. The physical, procedural, and personnel security measures meet the assurance requirements of higher-level CC evaluations.

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
CSE	Communications Security Establishment
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
SFP	Security Function Policy
SSIM	Symantec Security Information Manager
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

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 for Common Criteria Evaluation: Symantec Security Information Manager Version 4.5, Version 1.7, 24 August 2007.

e. Evaluation Technical Report (ETR) Symantec™ Security Information Manager Version 4.5, EAL 2 Evaluation, Common Criteria Evaluation Number: 383-4-71, Document No. 1555-000-D002, Version 1.1, 29 August 2007.