Certification Report

Symantec® Security Information Manager 4.8.1

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number:	383-4-235-CR
Version:	1.0
Date:	24 March 2014
Pagination:	i to iii, 1 to 7

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 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4*. 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, or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the Communications Security Establishment, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

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.

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 24 March 2014, 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 in the United States and other countries*

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

TABLE OF CONTENTS

Executive Summary

Symantec® Security Information Manager 4.8.1 (hereafter referred to as SSIM), from Symantec Corporation, is the Target of Evaluation for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

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

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 26 February 2014 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 SSIM, 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 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4.* The following augmentation is claimed: ALC_FLR.2 – Flaw Reporting Procedures.

Communications Security Establishment, 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) 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® Security Information Manager 4.8.1 (hereafter referred to as SSIM), from Symantec Corporation.

2 TOE Description

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

3 Evaluated Security Functionality

The complete list of evaluated security functionality for SSIM is identified in Section 6 of the ST.

4 Security Target

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

Title: Security Target Symantec® Security Information Manager Version 4.8.1
Version: 1.7
Date: 30 January 2014

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4.*

SSIM 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:
   - SIM_ANL.1 – Event Analysis; and
   - 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 augmented*, containing all security assurance requirements in the EAL 2 package, as well as the following: e.g. ALC_FLR.2 – Flaw Reprting Procedures.

6 Security Policy

SSIM implements an Administrative Access Control policy to control user access to the system; details of this security policy can be found in Section 6 of the ST.

In addition, SSIM implements insert other policies pertaining to security audit, identification and authentication, and security management. Further details on these security policies may be found in Section 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of SSIM 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 of the TOE are appropriately trained to undertake the installation, configuration and management of the TOE in a secure and trusted manner; and
- Administrators of the TOE and users on the local area network are not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the TOE documentation.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The processing platforms on which the TOE resides are located within a facility that provides controlled access; and
- The processing platforms on which the TOE resides and the TOE software critical to security policy enforcement will be protected from unauthorized physical modification.

8 Evaluated Configuration

The evaluated configuration for SSIM is software only and comprises:

- SSIM Server running on RedHat Enterprise Linux 6.4 x86 64-bit OS; and
- Management Console running on one of the following Operating Systems:
  - Windows-XP 32-bit SP3 and 64-bit SP2;
  - Windows Server 2003 32-bit and 64-bit SP2;
  - Windows Server 2008 32-bit and 64-bit SP2;
  - Windows Vista 32-bit and 64-bit SP2; and
  - Windows 7 32-bit and 64-bit.

The following publications describe the procedures necessary to install and operate SSIM in its evaluated configuration:

a. Symantec™ Security Information Manager 4.8.1 Installation Guide;
b. Symantec™ Security Information Manager 4.8.1 Administrator Guide; and
c. Symantec™ Security Information Manager 4.8.1 User Guide.

9 Documentation

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

a. Symantec™ Security Information Manager 4.8.1 Installation Guide;
b. Symantec™ Security Information Manager 4.8.1 Administrator Guide;
c. Symantec™ Security Information Manager 4.8.1 User Guide; and
d. Symantec™ Security Information Manager 4.8.1 Release Notes.

10 Evaluation Analysis Activities

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

Development: The evaluators analyzed the SSIM 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 SSIM 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 SSIM 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 SSIM configuration management system and associated documentation was performed. The evaluators found that the SSIM 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 SSIM during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for SSIM. 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 SSIM. Additionally, the evaluators conducted a search of public domain vulnerability databases to identify SSIM potential vulnerabilities. The evaluators identified potential vulnerabilities; subsequent to follow-on penetration testing (ref: section 11.3) it was verified that none of the potential vulnerabilities were exploitable in the operational environment for SSIM.

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.

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. Initialization: The goal of this test case is to verify that the Administrator can install and configure the TOE following the guidance provided with the product, and duplicate the settings and environment as detailed in the Security Target;

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

c. Security Management: The objective of this test goal is to verify that the SSIM Server can integrate with an Active Directory Server;

[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.

d. Incident Management: The purpose of this test goal is to verify that incidents are audited and tracked; and

e. Schedule and Distribute Reports: The purpose of this test goal is to verify that authorized users can create and distribute standard reports and queries.

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 purpose of this test case is to identify any suspicious open ports on the TOE system;
b. Monitor, Information leakage: The purpose of this test goal is to monitor for data leakage during login, logout and other scenarios; and
c. Bypass, Session Management: The objective of this test goal is to verify the secure management of the SSIM Web Interface session.

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

11.4 Conduct of Testing

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 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, providing assurance that SSIM 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 Evaluator Comments, Observations and Recommendations

The TOE must be operated in accordance with the Installation and Administration Guides and must be installed within a non-hostile and well-managed operating environment. The evaluator recommends that the users read the ST and make sure all the assumptions made regarding the environment are true in the intended environment of the TOE. The evaluator strongly recommends users of the TOE consult the Guidance Supplement for references on relevant user guidance in order to configure the TOE in its evaluated configuration. An unintentional misconfiguration due to a poorly trained administrator can easily lead to security threats not being countered as expected. The evaluator noted throughout the testing and vulnerability assessment portions of the evaluation that there are a great deal of configuration options available on the TOE and the Operational Environment.

14 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
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories - Canada
SFR	Security Functional Requirement
SIM	Security Information Manager
ST	Security Target
TOE	Target of Evaluation
TSF	Toe Security Functionality

15 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 4, September 2012.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012.

d. Symantec® Security Information Manager Version 4.8.1 , 1.7, 30 January 2014.

e. Evaluation Technical Report, Symantec® Security Information Manager v8.4.1, v1.1, 26 February 2014.