Certification Report

EAL 3+ Evaluation of

Symantec Risk Automation Suite 4.0.5

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Evaluation number:	383-4-144-CR
Version:	1.0
Date:	21 March 2011
Pagination:	i to iii, 1 to 9

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, 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 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 21 March 2011, 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;
- Microsoft, Windows, Windows Server, and SQL Server are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries; and
- Safari is a registered trademark of Apple Inc. in the U.S. and other countries.

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

TABLE OF CONTENTS

Executive Summary

Symantec Risk Automation Suite 4.0.5 (hereafter referred to as RAS 4.0.5), from Symantec Corporation, is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 3 augmented evaluation.

RAS 4.0.5 is a suite of technologies that provides a view of the technology and risks present in large IT networks by automating and integrating asset discovery, vulnerability detection, configuration scanning and reporting, and asset compliance with policies and standards into a single solution.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 7 March 2011 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 RAS 4.0.5, 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 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.1 - Basic Flaw Remediation.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the RAS 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) 3 augmented evaluation is Symantec Risk Automation Suite 4.0.5, (hereafter referred to as RAS 4.0.5), from Symantec.

2 TOE Description

RAS 4.0.5 is an integrated suite of software components that provides a view of the technology and risks present in large IT networks. RAS 4.0.5 comprises the main components:

RAS Portal that provides data analysis, reporting, scheduling, workflow, and management capabilities.

RAS Asset Discovery that discovers and inventories networks and network assets.

RAS Vulnerability Management that manages vulnerability scanners in vulnerability detection and reporting.

RAS Configuration Management that performs configuration scans and maintains an inventory of system configurations.

RAS Policy Management that evaluates system configurations and compliance with industry standards and corporate policies.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the RAS 4.0.5 is identified in Section 6 of the Security Target (ST).

4 Security Target

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

Title:	Security Target Symantec Risk Automation Suite 4.0.5
Version:	1.2
Date:	February 9, 2011

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*.

RAS 4.0.5 is:

a. *Common Criteria Part 2 extended,* with functional requirements based on functional components in Part 2, except for the following explicitly stated requirements defined in the ST:
   - SDC_ADR_EXT.1 – System data collection;
   - SDC_ADR_EXT.2 – System data analysis;
   - SDC_ADR_EXT.3 – System data display; and
   - SDC_ADR_EXT.4 – System data actions.

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

c. Common Criteria EAL 3 augmented, with all the security assurance requirements in the EAL 3, as well as the following: ALC_FLR.1 - Basic Flaw Remediation.

6 Security Policy

RAS 4.0.5 implements policies pertaining to Security Audit, Identification and Authentication, Scanning and Security Assessment, 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 RAS 4.0.5 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. The authorized administrators are not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by the TOE documentation, including the administrator guidance and to periodically check the audit record; however, they are capable of error; and

b. Personnel will be trained in the appropriate use of the TOE to ensure security.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

a. There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) on the TOE;

b. The TOE is interoperable with the IT Systems it monitors;

c. If email functionality is to be used, external email services will be available;

d. If external authentication is to be used, external authentication services will be available via Active Directory authentication credentials;

e. The TOE will be located within controlled access facilities, which will prevent unauthorized physical access such that the TOE can only be accessed by authorized users; and

f. The operational environment provides the TOE with reliable time stamps.

7.3 Clarification of Scope

RAS 4.0.5 is not intended to be placed or operated in a hostile environment, and should be protected by other products specifically designed to address sophisticated threats.

8 Evaluated Configuration

The evaluated configuration for RAS 4.0.5 comprises Symantec Risk Automation Suite v4.5.0.2506 running on Microsoft Windows 2003 Server or Microsoft Windows 2008 Server with Microsoft SQL Server 2005 or Microsoft SQL Server 2008, and browsers Internet Explorer, Firefox, or Safari.

9 Documentation

The Symantec documents provided to the consumer are as follows:

a. Operational User Guidance and Preparative Procedures Supplement: Symantec Risk Automation Suite Version 4.05;

b. Symantec Risk Automation Suite (SRAS) Quick Start Guide For Risk Automation Suite v4.0 – Enterprise Edition;

c. Operational User Guidance and Preparative Procedures Supplement: Symantec Risk Automation Suite Version 4.05;

d. Symantec Risk Automation Suite (SRAS) Off-Line Scanning Guide For Risk Automation Suite v4.0 – Enterprise Edition;

e. Symantec Risk Automation Suite (SRAS) Policies & Controls - A Guide to Managing Policies and Controls in the SRAS Portal For Risk Automation Suite v4.0 - Enterprise Edition;

f. Symantec Risk Automation Suite (SRAS) A Guide to Reporting For Risk Automation Suite v4.0 – Enterprise Edition;

g. Symantec Risk Automation Suite (SRAS) Portal A Guide to Managing Scans For Risk Automation Suite v4.0 – Enterprise Edition;

h. Symantec Risk Automation Suite (SRAS) Secure Content Automation Protocol (SCAP) User Guide Supplement For Risk Automation Suite v4.0 – Enterprise Edition;

i. Symantec Risk Automation Suite (SRAS) Guide for RAS/SMP Integration For Risk Automation Suite v4.0 – Enterprise Edition, and

j. Symantec Risk Automation Suite User Guide.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of RAS 4.0.5, including the following areas:

Development: The evaluators analyzed the RAS 4.0.5 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 RAS 4.0.5 security architectural description and determined that the initialization process is secure and that the security functions are protected against tamper and bypass. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the RAS 4.0.5 preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously described 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 were complete and sufficiently detailed to result in a secure configuration.

Life-Cycle Support: An analysis of the RAS 4.0.5 configuration management system and associated documentation was performed. The evaluators found that the RAS 4.0.5 configuration items were clearly marked and that the access control measures as described in the configuration management documentation are effective in preventing unauthorized access to the configuration items. The developer's configuration management system was also observed during the site visit, and it was found to be mature and well developed.

During the site visit the evaluators examined the development security procedures and determined that they detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the RAS 4.0.5 design and implementation. The evaluators confirmed that the developer used a documented model of the TOE life-cycle and that the life-cycle model provides for the necessary control over the development and maintenance of the TOE.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of RAS 4.0.5 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used for RAS 4.0.5. During a site visit, the evaluators 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 RAS 4.0.5. Additionally, the evaluators conducted a review of public domain vulnerability databases, and a search of all evaluation deliverables. The evaluators identified potential vulnerabilities for testing applicable to the RAS 4.0.5 in its operational environment.

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

11 ITS Product Testing

Testing at EAL 3 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 and depth analysis and found them to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the functional specification and TOE design 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 was the following list of EWA-Canada test goals:

[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.

a. Initialization: The objective of this test goal is to confirm that the TOE can be installed and configured into the evaluated configuration, as identified in the TOE Description of the Security Target, by following all instructions in the developer's Installation and Administrative guidance;

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

c. Identification and Authentication: The objective of this test goal is to augment testing of concurrent logins, user lockout, and password strength;

d. Audit: The objective of this test goal is to augment testing of audit generation, audit review, and audit security;

e. Roles: The objective of this test goal is to augment testing of role restrictions; and

f. Basic Functionality: The objective of this test goal is to augment testing of data collection, data analysis, data display and data actions.

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 port scanning, banner grabbing, leakage verification, and misuse testing.

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

11.4 Conduct of Testing

RAS 4.0.5 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 Testing (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 RAS 4.0.5 behaves as specified in its ST, functional specification, TOE design, and security architecture description.

12 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.

13 Evaluator Comments, Observations and Recommendations

The complete documentation for the RAS includes a comprehensive installation guide, and security guides and a user's guide.

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 RAS 4.0.5.

14 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
API	Application Program Interface
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
OS	Operating System
PALCAN	Program for the Accreditation of Laboratories Canada
QA	Quality Assurance
RAS	Risk Automation Suite
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 3, July 2009.

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

d. Security Target Symantec Risk Automation Suite 4.0.5, Revision No. 1.2, February 9, 2011.

e. Evaluation Technical Report (ETR) Risk Automation Suite, EAL 3+ Evaluation, Common Criteria Evaluation Number: 383-4-144, Document No. 1650-000-D002, Version 1.1, 07 March 2011.