Certification Report

EAL 3+ Evaluation of Symantec™ Control Compliance Suite v10.5.1

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number:	383-4-178-CR
Version:	1.0
Date:	16 September 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, 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 16 September 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 registered trademark:

- *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

Disclaimer i

Foreword ii

Executive Summary 1

1 Identification of Target of Evaluation 2

2 TOE Description 2

3 Evaluated Security Functionality 2

4 Security Target 2

5 Common Criteria Conformance 3

6 Security Policy 3

7 Assumptions and Clarification of Scope 3

7.1 SECURE USAGE ASSUMPTIONS 4
7.2 ENVIRONMENTAL ASSUMPTIONS 4
7.3 CLARIFICATION OF SCOPE 4

8 Evaluated Configuration 4

9 Documentation 5

10 Evaluation Analysis Activities 5

11 ITS Product Testing 6

11.1 ASSESSMENT OF DEVELOPER TESTS 6
11.2 INDEPENDENT FUNCTIONAL TESTING 7
11.3 INDEPENDENT PENETRATION TESTING 7
11.4 CONDUCT OF TESTING 8
11.5 TESTING RESULTS 8

12 Results of the Evaluation 8

13 Evaluator Comments, Observations and Recommendations 8

14 Acronyms, Abbreviations and Initializations 8

15 References 9

Executive Summary

The Symantec™ Control Compliance Suite v10.5.1 (hereafter referred to as the Symantec CCS v10.5.1), from Symantec, is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 3 augmented evaluation.

Symantec™ CCS v10.5.1 is a software only IT risk and compliance management solution which allows administrators to link administrator defined policies to specific technical and procedural standards, and which automates the tracking of compliance to those policies across the organization. It provides an agent-less or agent-based capability to audit and scan managed devices and identify problems with system configurations and internal controls.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 9 September 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 the Symantec CCS v10.5.1, 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.2 - Flaw Reporting Procedures.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the Symantec™ CCS v10.5.1 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 may not be 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™ Control Compliance Suite v10.5.1 (hereafter referred to as Symantec CCS v10.5.1), from Symantec.

2 TOE Description

Symantec™ CCS v10.5.1 is a software only IT risk and compliance management solution which allows administrators to link administrator defined policies to specific technical and procedural standards, and which automates the tracking of compliance to those policies across the organization. It provides an agent-less or agent-based capability to audit and scan managed devices and identify problems with system configurations and internal controls.

A description of the Symantec™ CCS v10.5.1 architecture and functionality is found in Sections 1.4.1 and 1.5.1 of the Security Target (ST).

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the Symantec™ CCS v10.5.1 is identified in Section 6 of the Security Target (ST).

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

Cryptographic Modules	**Certificate #**
Windows Server 2008 R2 Enhanced Cryptographic Provider (RSAENH) Software Version: 6.1.7600.16385	1337
OpenSSL FIPS Runtime Module Software Version 1.2	1111

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation:

Cryptographic Algorithm	**Standard**	**Certificate #**
Advanced Encryption Standard (AES)	FIPS 197	1168
Secure Hash Algorithm (SHA-1)	FIPS 180-3	723
Rivest Shamir Adleman (RSA)	ANSI X9.31 PKCS #1 v1.5 RSASSA-PSS	323

4 Security Target

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

Title: Symantec™ Control Compliance Suite v10.5.1 Security Target
Version: 0.19
Date: 25 August, 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*.

The Symantec CCS v10.5.1 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:
   - EXT_CCS_SDC.1 – System Data Collection;
   - EXT_CCS_ANL.1 – Analysis;
   - EXT_CCS_ARP.1 – Security Alarms; and
   - EXT_CCS_RDR.1 – Restricted Data Review.

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 package, as well as the following: ALC_FLR.2 – Flaw Reporting Procedures.

6 Security Policy

The Symantec CCS v10.5.1 implements Control Compliance System policies to collect information from managed devices, analyze the data for compliance and send alerts based on programmable alarms. Further details on these security policies may be found in Sections 5 and 6.2.6 of the ST.

In addition, Symantec CCS v10.5.1 implements policies pertaining to Security Audit, Cryptographic Support, Security Management, Protection of the TOE Security Functionality, and Trusted Path/Channel. Further details on these security policies may be found in Section 6.2 of the ST.

7 Assumptions and Clarification of Scope

Consumers of the Symantec CCS v10.5.1 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

The following Secure Usage Assumptions are listed in the ST:

a. The administrator of the TOE is competent, non-hostile, appropriately trained and follows all guidance; and

b. Components of the TOE critical to the security policy enforcement must be located within controlled access facilities.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

a. The IT environment provides the TOE with reliable time stamps; and

b. The IT environment provides the TOE with identification and authentication of TOE users.

7.3 Clarification of Scope

The Symantec CCS v10.5.1 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 Symantec CCS v10.5.1 comprises:

a. Control Compliance Suite Reporting and Analytic v10.5.1 10.50.530.20000;

b. Risk Management Server v10.5.1, 10.50.194.20000;

c. Response Assessment Manager v10.5, 10.50.166.10000;

d. bv-control Windows v10.5.1;

e. bv-control SQL Server v10.5.1;

f. bv-control Oracle Subsystem v10.5.1;

g. bv-control NDS/Netware v10.5.1; and

h. FIPS Validated cryptographic modules: Windows Server 2008 R2 Enhanced Cryptographic Provider (RSAENH) Software Version: 6.1.7600.16385 (Certificate # 1337) and OpenSSL FIPS Runtime Module Software Version 1.2 (Certificate # 1111).

The third party software that the TOE relies upon is identified in Table 3 of the ST.

The publications entitled *Symantec™ Control Compliance Suite Installation Guide and Symantec™ Response Assessment Module Installation Guide* describe the procedures necessary to install Symantec CCS v10.5.1 in its evaluated configuration.

9 Documentation

The Symantec documents provided to the consumer are as follows:

a. Symantec Corporation Control Compliance Suite 10.5.1 Guidance Documentation Supplement;
b. Symantec™ Control Compliance Suite Installation Guide, Version 10.5;
c. Symantec™ Response Assessment Module 10.5 Installation Guide;
d. Symantec™ RMS Console and Information Server Getting Started Guide, Version 10.5;
e. Symantec™ Control Compliance Suite User Guide, Version 10.5;
f. Symantec™ Control Compliance Suite Planning and Deployment Guide, Version 10.5;
g. Symantec™ Response Assessment Module User Guide, Version 10.5;
h. Symantec™ bv-Control® for Microsoft® SQL Server Getting Started Guide, Version 10.5;
i. Symantec™ bv-Control® for Microsoft® NDS eDirectory Getting Started Guide, Version 10.5;
j. Symantec™ bv-Control® for Netware® Server Getting Started Guide, Version 10.5;
k. Symantec™ bv-Control® for Oracle® Getting Started Guide, Version 10.5; and
l. Symantec™ bv-Control® for Windows® Getting Started Guide, Version 10.5.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the Symantec CCS v10.5.1, including the following areas:

Development: The evaluators analyzed the Symantec CCS v10.5.1 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 Symantec CCS v10.5.1 security architectural description and determined that the initialization process is secure and 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 Symantec CCS v10.5.1 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 Symantec CCS v10.5.1 configuration management system and associated documentation was performed. The evaluators found that the

Symantec CCS v10.5.1 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 Symantec CCS v10.5.1 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 Symantec CCS v10.5.1 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by Symantec for Symantec CCS v10.5.1. 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 Symantec CCS v10.5.1. 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 Symantec CCS v10.5.1 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 the test evidence, and reviewing the test results, as documented in the ETR[2].

[2] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and may not be releasable for public review.

The evaluators analyzed the developer's test coverage and depth analyses 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's 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. 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; and

c. Security Management: The objective of this test goal is to ensure that role based access control requirements have been met and that functionality pertaining to the creation, access, review and approval of administrator defined CCS policies operate as specified.

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. Bypass: The objective of this test was to verify that browser sessions were successfully destroyed;

b. Monitoring: The objective of this test was to verify that the TOE does not leak sensitive information and to scan for unnecessary open ports; and

c. Misuse: The objective of this test is to verify that the TOE continues to operate when a communication failure occurs.

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

11.4 Conduct of Testing

Symantec™ CCS v10.5.1 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 the Symantec CCS v10.5.1 behaves as specified in its ST and functional specification and TOE design.

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 Symantec CCS v10.5.1 includes a comprehensive Installation and Security Guide and a User's Guide.

14 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
AES	Advanced Encryption Standard (AES)
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CCS	Control Compliance Suite
CCSRA	Control Compliance Suite Reporting and Analytics
CPL	Certified Products list
EAL	Evaluation Assurance Level
ESM	Enterprise Security Manager
ETR	Evaluation Technical Report
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing

Acronym/Abbreviation/ Initialization	Description
PALCAN	Program for the Accreditation of Laboratories Canada
RAM	Response Assessment Manager
RMS	Risk Management Server
RSA	Rivest Shamir Adleman
RSAENH	Windows Server 2008 R2 Enhanced Cryptographic Provider
SHA-1	Secure Hash Algorithm
SFR	Security Functional Requirement
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. Symantec™ Control Compliance Suite v10.5.1 Security Target, Revision No. 0.19, 25 August, 2011.

e. Evaluation Technical Report (ETR) Symantec™ Control Compliance Suite v10.5.1, EAL 3+ Evaluation, Common Criteria Evaluation Number: 383-4-178, Document No. 1693-000-D002, Version 1.1, 09 September 2011.