Certification Report

EAL 2+ Evaluation of Symantec Altiris IT Management Suite 7.1 SP2

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number:	383-4-225-CR
Version:	1.0
Date:	25 April 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 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 3 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).

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 ... **3**

2 TOE Description ... **3**

3 Evaluated Security Functionality ... **3**

4 Security Target ... **4**

5 Common Criteria Conformance ... **4**

6 Security Policy ... **4**

7 Assumptions and Clarification of Scope ... **4**

7.1 SECURE USAGE ASSUMPTIONS ... 4
7.2 ENVIRONMENTAL ASSUMPTIONS ... 5
7.3 CLARIFICATION OF SCOPE ... 5

8 Evaluated Configuration ... **6**

9 Documentation ... **6**

10 Evaluation Analysis Activities ... **6**

11 ITS Product Testing ... **7**

11.1 ASSESSMENT OF DEVELOPER TESTS ... 8
11.2 INDEPENDENT FUNCTIONAL TESTING ... 8
11.3 INDEPENDENT PENETRATION TESTING ... 8
11.4 CONDUCT OF TESTING ... 9
11.5 TESTING RESULTS ... 9

12 Results of the Evaluation ... **9**

13 Evaluator Comments, Observations and Recommendations ... **10**

14 Acronyms, Abbreviations and Initializations ... **10**

15 References ... **11**

Executive Summary

Symantec Altiris IT Management Suite 7.1 SP2 (hereafter referred to as ITMS), from Symantec Corporation, is the Target of Evaluation for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

ITMS is a collection of solutions that run on the Symantec Management Platform. The platform and solutions of ITMS provide the following key features:

- Central Web-based management console
- Role-and-scope-based security
- Zero-touch OS deployment and migration
- Integrated hardware and software inventory with Web-based reporting
- Policy-based software management
- Automated patch management
- Software license compliance and harvesting
- Centralized management of mixed hardware and OS environments

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 6 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 ITMS, 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

[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.

conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision.* The following augmentation is claimed: ALC_FLR.2 – Flaw Reporting Procedures

Communications Security Establishment Canada, as the CCS Certification Body, declares that the ITMS 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 Altiris IT Management Suite 7.1 SP2 (hereafter referred to as ITMS), from Symantec Corporation.

2 TOE Description

ITMS is a collection of solutions that run on the Symantec Management Platform. The platform and solutions of ITMS provide the following key features:

- Central Web-based management console
- Role-and-scope-based security
- Zero-touch OS deployment and migration
- Integrated hardware and software inventory with Web-based reporting
- Policy-based software management
- Automated patch management
- Software license compliance and harvesting
- Centralized management of mixed hardware and OS environments

A detailed description of the ITMS architecture is found in Section 1.6 of the Security Target (ST).

3 Evaluated Security Functionality

The complete list of evaluated security functionality for ITMS is identified in Section 1.6 of the ST.

4 Security Target

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

Title: Security Target: Symantec Altiris IT Management Suite 7.1 SP2
Version: 1.2
Date: 6 March 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.*

ITMS 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:
   - FMS_SCN_(EXT).1 - Target 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

6 Security Policy

ITMS implements a role-based access control policy to control user access to the system; details of this security policy can be found in Section 7 of the ST.

In addition, ITMS implements insert other policies pertaining to security audit, managed systems, identification and authentication, and security management. Further details on these security policies may be found in Section 7 of the ST.

7 Assumptions and Clarification of Scope

Consumers of ITMS 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:

- One or more authorized administrators are assigned who are competent to manage the TOE and the security of the information it contains, and who can be trusted not to deliberately abuse their privileges.

- The TOE is delivered, installed, managed, and operated in a manner that maintains the TOE security objectives.

- Users of the TOE possess the necessary privileges to access the information managed by the TOE.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE is located in a physically secure environment and protected from unauthorized physical access.

- The Operational Environment will provide a means to review audit logs.

7.3 Clarification of Scope

ITMS offers protection against inadvertent or casual attempts to breach system security by unsophisticated attackers possessing basic attack potential. ITMS 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 ITMS comprises:

Hardware requirements for all Servers and Agents	General purpose workstation with 8-core 2.4GHz processor, 8GB DDR2 RAM, 6MB L2 cache, Gigabit network, 10GB disk space on 10,000 RPM SCSI or better with RAID 5 or 1+0
Software requirements for systems running the Management System	• NET Framework 3.5 SP1 • Internet Explorer 7.0 • SQL Server 2005 or SQL Server 2008 • Windows Server 2008 R2 x64
Software requirements for systems running the Windows Agents	• Windows XP SP3 x64/x86 • Windows Vista SP1 x64/x86 • Windows 7 x64/x86 • Windows Server 2003 SP2 • Windows Server 2008 GA x64/x86

The publication entitled Operational User Guidance and Preparative Procedures Supplement: Symantec Altiris IT Management Suite 7.1 SP2 from Symantec describes the procedures necessary to install and operate ITMS in its evaluated configuration.

9 Documentation

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

a. Operational User Guidance and Preparative Procedures Supplement: Altiris IT Management Suite Version 7.1 SP2 from Symantec, Document Version 1.3, March 6, 2013;

b. Symantec Management Platform 7.1 SP2 User Guide, 2011;

c. Symantec Management Platform 7.1 SP2 Installation Guide, 2011;

d. Altiris IT Management Suite Version 7.1 SP2 from Symantec Planning and Implementation Guide, 7.1 SP2, 2011; and

e. Symantec File Connect User Guide, 10/19/2006, 10/19/2006.

10 Evaluation Analysis Activities

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

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

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

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

11 ITS Product Testing

Testing at EAL 2 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. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests;

b. Audit creation: The objective of this test goal was to confirm that audit records were created for authentication failure and use of the TSFIs;

c. Limits of platform administrator: The objective of this test goal is to confirm that platform administrators are unable to login to the TOE unless authorized;

d. Software discovery: The objective of this test goal is to exercise the software discovery scan functions of the TOE with the relation to scheduling scans and use of scanning polices; and

e. Management of security settings: The objective of this test goal is to exercise the management of the TOE's security settings.

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:

[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. 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.

d. Concurrent Logins: The objective of this test goal is to test the effects of concurrent logins on TOE.

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

11.4 Conduct of Testing

ITMS 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 ITMS 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

Although the complete suite includes many features, only those functions detailed in the ST were tested. It is recommended that potential users of the TOE review the ST to ensure an accurate understanding of the evaluated security functionality. It is also recommended that users of the TOE consult the Guidance Supplement to ensure implementation of the TOE in its evaluated configuration

14 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
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation

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 Altiris IT Management Suite 7.1 SP2, 1.2, 6 March 2013.

e. ETR for EAL 2+ CC Evaluation of Altiris IT Management Suite Version 7.1 SP2 from Symantec, v1.1, 6 March 2013.