Certification Report

Symantec™ Network Access Control Version 12.1.2

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-216-CR
Version: 1.0
Date: 17 June 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 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 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.

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 17 June 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).

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

- Symantec™ is a trademark of Symantec Corporation.

TABLE OF CONTENTS

Executive Summary

Symantec™ Network Access Control Version 12.1.2 (hereafter referred to as Symantec NAC v12.1.2), from Symantec Corporation, is the Target of Evaluation for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

Symantec NAC v12.1.2 is a network access control solution running on clients (e.g., desktops and laptops), an Enforcer to grant the endpoint network access, block network access, or remediate non-compliant computers, and a management component running on a central server to control and monitor execution of the network access control client application.

The primary purpose of Symantec NAC v12.1.2 is to ensure that the clients that run the software are compliant with an organization's security policies. Security policy compliance is enabled by using the Host Integrity policies created in the Symantec Endpoint Protection Manager component. Together, Host Integrity policies and hardware enforcement keep non-compliant computers off of the network.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 10 May 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 Symantec NAC v12.1.2, 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.

[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.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the Symantec NAC v12.1.2 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™ Network Access Control Version 12.1.2 (hereafter referred to as Symantec NAC v12.1.2), from Symantec Corporation.

2 TOE Description

Symantec NAC v12.1.2 is a network access control solution running on clients (e.g., desktops and laptops), an Enforcer to grant the endpoint network access, block network access, or remediate non-compliant computers, and a management component running on a central server to control and monitor execution of the network access control client application.

The primary purpose of Symantec NAC v12.1.2 is to ensure that the clients that run the software are compliant with an organization's security policies. Security policy compliance is enabled by using the Host Integrity policies created in the Symantec Endpoint Protection Manager component. Together, Host Integrity policies and hardware enforcement keep non-compliant computers off of the network.

A detailed description of the Symantec NAC v12.1.2 architecture is found in Section 1.7 of the Security Target (ST).

3 Evaluated Security Functionality

The complete list of evaluated security functionality for Symantec NAC v12.1.2 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™ Network Access Control Version 12.1.2
Version: 0.12
Date: 14 February 2013

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.*

Symantec NAC v12.1.2 is:

a. *Common Criteria Part 2 conformant*, with security functional requirements based only upon functional components in Part 2; and

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.

6 Security Policy

Symantec NAC v12.1.2 implements a role-based access control policy to control user access to the system, as well as an information flow control policy to control information entering the system; details of these security policies can be found in Section 7.1 of the ST.

In addition, Symantec NAC v12.1.2 implements policies pertaining to security audit and security management. Further details on these security policies may be found in Section 7.1 of the ST.

7 Assumptions and Clarification of Scope

Consumers of Symantec NAC v12.1.2 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 will back up the audit files and monitor disk usage to ensure audit information is not lost.
- Administrators are non-hostile, appropriately trained, and follow all administrator guidance.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) nor storage repository capabilities on the system on which SEPM executes.
- Appropriate physical security is provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.
- The IT environment will provide a secure line of communications between distributed portions of the TOE and between the TOE and remote administrators.

8 Evaluated Configuration

The evaluated configuration for Symantec NAC v12.1.2 comprises:

- The TOE running on a GPC with the following minimum requirements;
    - Windows 7 (32-bit and 64-bit SP1), Windows XP (32-bit and 64-bit, SP-3), Windows Server 2003 (32-bit, 64-bit, R2, SP-2), Windows Server 2008 (32-bit, 64-bit SP2), Windows Small Business Server 2008 (64-bit), Windows Small Business Server 2011 (64-bit), or Windows Essential Business Server 2008 (64-bit)
    - 1 Ghz intel P3 or 2 Ghz P4 with x86-64 support
    - 1 GB of RAM
    - JRE v1.6.0 and Apache Tomcat v6.0.32
- Symantec Network Access Control Enforcer 6100 Series Appliance

The publication entitled Operational User Guidance and Preparative Procedures Supplement: Symantec Network Access Control Version 12.1, 1.2, May 22, 2012 describes the procedures necessary to install and operate Symantec NAC v12.1.2 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: Symantec Network Access Control Version 12.1, 1.2, May 22, 2012;

b. Symantec™ Endpoint Protection and Symantec Network Access Control Client Guide, 12.01.00.00.00, © 2011 Symantec Corporation;

c. Symantec™ Network Access Control Enforcer Implementation Guide, Documentation Version 11.00.03.00.00, © 2008 Symantec Corporation;

d. Symantec™ Network Access Control Enforcer Installation and Administration Guide Release 5.1, Documentation Build 5.1.0.7003, December 19, 2005;

e. Symantec™ Network Access Control Getting Started Guide, 12.01.00.00, © 2011 Symantec Corporation; and

f. Symantec™ Endpoint Protection and Symantec Network Access Control Implementation Guide, 12.01.00.00.00, © 2011 Symantec Corporation.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Symantec NAC v12.1.2, including the following areas:

Development: The evaluators analyzed the Symantec NAC v12.1.2 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 NAC v12.1.2 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 Symantec NAC v12.1.2 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 NAC v12.1.2 configuration management system and associated documentation was performed. The evaluators found that the Symantec NAC v12.1.2 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 Symantec NAC v12.1.2 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the Symantec NAC v12.1.2. 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 Symantec NAC v12.1.2. Additionally, the evaluators conducted a search of public domain vulnerability databases to identify Symantec NAC v12.1.2 potential vulnerabilities. The evaluators identified potential vulnerabilities for testing applicable to Symantec NAC v12.1.2 in its operational environment.

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

b. Concurrent logins: The objective of this test goal is to confirm that there is no privilege escalation with concurrent logins;

c. User Deletion: The objective of this test goal is to confirm that a deleted user cannot login; and

d. IDS functions: The objective of this test goal is exercise the IDS functionality of the TOE.

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; and

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.

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

11.4 Conduct of Testing

Symantec NAC v12.1.2 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 Symantec NAC v12.1.2 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 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
ST	Security Target
TOE	Target of Evaluation

14 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, July 2009.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, July 2009.

d. Security Target: Symantec™ Network Access Control Version 12.1.2, 0.12, 14 February 2013.

e. Evaluation Technical Report for EAL 2+ Common Criteria Evaluation of Symantec Corporation Symantec™ Network Access Control Version 12.1.2, Version 1.1, 10 May 2013.