Certification Report

NetIQ® Secure Configuration Manager™ 5.9.1

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-265-CR
Version: 1.0
Date: 28 November 2014
Pagination: i to iii, 1 to 10

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, applies 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, the evaluated security functionality, and the testing and analysis conducted by the CCEF.

This certification report is associated with the certificate of product evaluation dated 28 November 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:

- NetIQ® is a registered trademark of NetIQ Corporation
- Secure Configuration Manager ™ is a trademark of NetIQ Corporation

TABLE OF CONTENTS

Disclaimer ..... **i**

Foreword ..... **ii**

Executive Summary **1**

1 Identification of Target of Evaluation **2**

2 TOE Description **2**

3 Security Policy **3**

4 Security Target **3**

5 Common Criteria Conformance **3**

6 Assumptions and Clarification of Scope **4**

6.1 SECURE USAGE ASSUMPTIONS 4
6.2 ENVIRONMENTAL ASSUMPTIONS 4
6.3 CLARIFICATION OF SCOPE 4

7 Evaluated Configuration **5**

8 Documentation **5**

9 Evaluation Analysis Activities **6**

10 ITS Product Testing **7**

10.1 ASSESSMENT OF DEVELOPER TESTS 7
10.2 INDEPENDENT FUNCTIONAL TESTING 7
10.3 INDEPENDENT PENETRATION TESTING 8
10.4 CONDUCT OF TESTING 8
10.5 TESTING RESULTS 8

11 Results of the Evaluation **8**

12 Evaluator Comments, Observations and Recommendations **8**

13 Acronyms, Abbreviations and Initializations **9**

14 References **10**

Executive Summary

NetIQ® Secure Configuration Manager™ 5.9.1 (hereafter referred to as NetIQ SCM 5.9.1), from NetIQ Corporation, is the Target of Evaluation. The results of this evaluation demonstrate that NetIQ SCM 5.9.1 meets the requirements of Evaluation Assurance Level (EAL) 2 augmented for the evaluated security functionality.

NetIQ SCM 5.9.1 is a software application that enables organizations to determine organizational security policy compliance, to identify security vulnerabilities and potential threats, and to assist in correcting exposures in a timely manner to reduce the risk of security breaches, failed compliance audits or downtime. NetIQ SCM also provides reporting capabilities, risk scoring to assist with prioritizing the discovered potential threats and vulnerabilities, and an update service that integrates new expertise and security knowledge1 by providing new security checks for the latest vulnerabilities, updated policy templates, and current manufacturer-recommended patches.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 27 October 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 NetIQ SCM 5.9.1, and the security functional/assurance 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.

Communications Security Establishment, as the CCS Certification Body, declares that the NetIQ SCM 5.9.1 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).

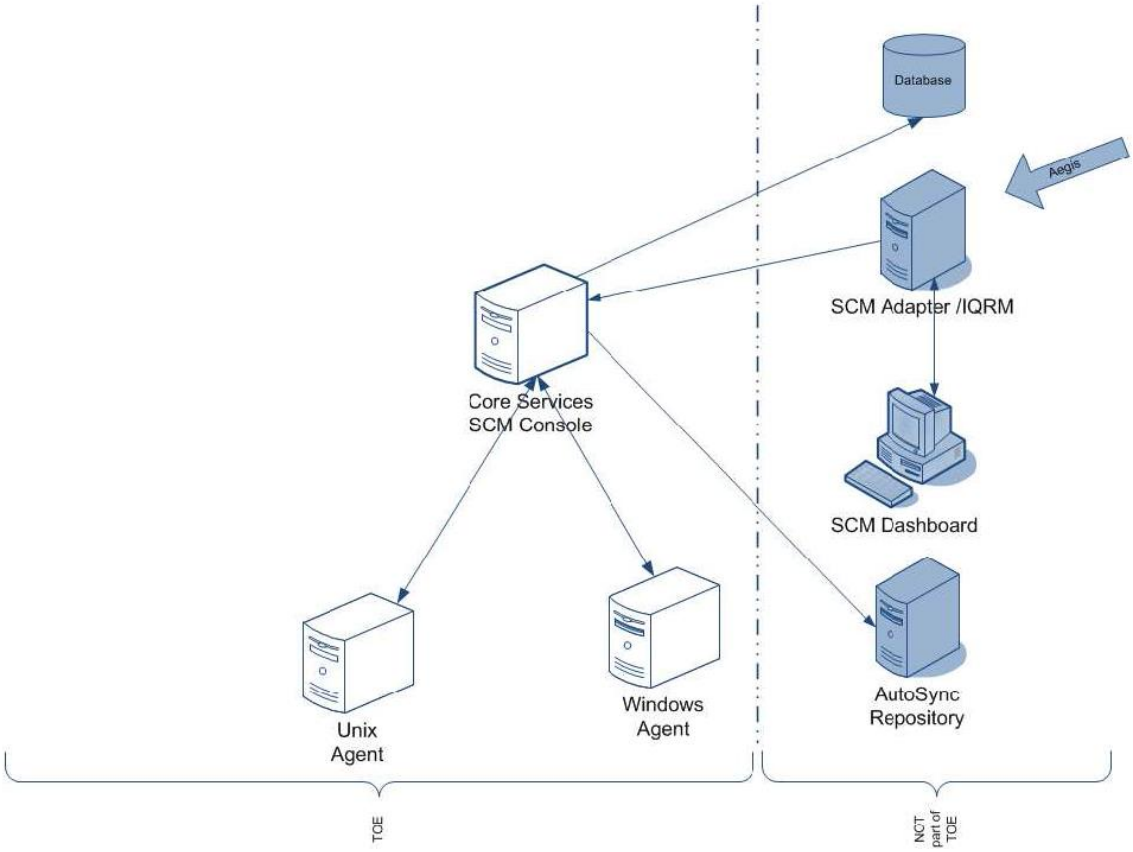
1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this EAL 2+ evaluation is NetIQ® Secure Configuration Manager™ 5.9.1 (hereafter referred to as NetIQ SCM 5.9.1), from NetIQ Corporation.

2 TOE Description

NetIQ SCM 5.9.1 is a software application that enables organizations to determine organizational security policy compliance, to identify security vulnerabilities and potential threats, and to assist in correcting exposures in a timely manner to reduce the risk of security breaches, failed compliance audits or downtime. NetIQ SCM 5.9.1 also provides reporting capabilities, risk scoring to assist with prioritizing the discovered potential threats and vulnerabilities, and an update service that integrates new expertise and security knowledge by providing new security checks for the latest vulnerabilities, updated policy templates, and current manufacturer-recommended patches.

A diagram of the NetIQ SCM 5.9.1 architecture is as follows:



3 Security Policy

NetIQ SCM 5.9.1 implements a role-based access control policy to control administrative access to the system. In addition, NetIQ SCM 5.9.1 implements policies pertaining to the following security functional classes:

- Security Audit
- Cryptographic Operations
- User Data Protection
- Identification and Authentication
- Protection of the TOE
- Security Management
- Secure Communications

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

Cryptographic Module	**Certificate**
OpenSSL FIPS Object Module v1.2	*#1051*
Network Security Services (NSS) Cryptographic Module (Extend ECC) v3.12.4	*#1279*
Network Security Services (NSS) v3.12.4	*#1475*

4 Security Target

The ST associated with this Certification Report is identified below:

NetIQ® Secure Configuration Manager™ 5.9.1 Security Target v3.0, August 27,2014

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.*

NetIQ SCM 5.9.1 is:

a. EAL 2 augmented, containing all security assurance requirements listed, as well as the following:
   - ALC_FLR.1 – Basic flaw remediation

b. *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:*
   - FPT_SEP_EXT.1 – Partial TSF domain separation

c. *Common Criteria Part 3 conformant,* with security assurance requirements based only upon assurance components in Part 3.

6 Assumptions and Clarification of Scope

Consumers of NetIQ SCM 5.9.1 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.

6.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- *All networks will allow for communications between the components;*
- *The TOE has access to all the IT System data it needs to perform its functions;*
- *The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors;*
- *The TOE component for Core Services must be connected to the Internet, behind appropriate boundary protection mechanisms, in order to receive updated content information from the NetIQ servers;*
- *Administrators will implement procedures for reviewing and validating updated content files from NetIQ, and for applying the updates; and*
- *The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.*

6.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- *The TOE will be able to rely on the IT environment to determine the identity of users;*
- *The server components of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access; and*
- *The TOE will be able to rely on the IT environment to obtain a reliable time stamp.*

6.3 Clarification of Scope

The FIPS validation is vendor affirmed and the cryptographic modules have been ported in accordance with FIPS IG G.5.

7 Evaluated Configuration

The evaluated configuration for NetIQ SCM 5.9.1 comprises:

- *The SCM Console v5.9.1 and the SCM Core Services v5.9.1 components installed on a GPC running Windows Server 2012 R2;*
- *A security Agent installed on a monitored system running either Sun Solaris 5.1.1 or Windows Server 2012*

The publication entitled NetIQ Secure Configuration Manager 5.9.1 Operation User Guidance and Preparative Procedures v1.0 describes the procedures necessary to install and operate NetIQ SCM 5.9.1 in its evaluated configuration.

8 Documentation

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

a. NetIQ Secure Configuration Manager 5.9.1 Operation User Guidance and Preparative Procedures, v1.0, 27 October 2014

b. NetIQ Secure Configuration Manager Installation Guide, July 2013

c. NetIQ Secure Configuration Manager Windows Agent Installation and Configuration Guide, July 2013; and

d. *NetIQ Secure Configuration Manager User Guide, July 2013.*

9 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of NetIQ SCM 5.9.1, including the following areas:

Development: The evaluators analyzed the NetIQ SCM 5.9.1 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 NetIQ SCM 5.9.1 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 NetIQ SCM 5.9.1 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 NetIQ SCM 5.9.1 configuration management system and associated documentation was performed. The evaluators found that the NetIQ SCM 5.9.1 configuration items were clearly marked.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of NetIQ SCM 5.9.1 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the NetIQ SCM 5.9.1. 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

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

10 ITS Product Testing

Testing consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

10.1 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[1].

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.

10.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation.

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 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. Agent Push: The objective of this test goal is to confirm that the TOE can push an agent installation out to a PC;

c. Agent Uninstall: The objective of this test goal is to confirm that the TOE can uninstall an agent from a PC;

d. Group Policy Pull: The objective of this test goal is to confirm that the TOE can pull group policy settings from Windows 2012 servers;

e. Security Check: The objective of this test goal is to have the TOE perform a security check on a monitored system; and

f. Software Inventory: The objective of this test goal is to confirm that the TOE can determine what software a monitored system has installed.

[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.

10.3 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. Use of automated vulnerability scanning tools to discover potential network, platform and application layer vulnerabilities.

b. 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; and

c. Agent Restart: The objective of this test goal is to attempt to disable the agent on a monitored system.

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

10.4 Conduct of Testing

NetIQ SCM 5.9.1 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 Test Facility. 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.

10.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, providing assurance that NetIQ SCM 5.9.1 behaves as specified in its ST and functional specification.

11 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.

12 Evaluator Comments, Observations and Recommendations

The evaluator recommends reading and understanding about potential Windows domain requirements before deployment of this product.

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
GPC	General Purpose Computer
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
TSF	TOE Security Function

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, September 2012.

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

d. NetIQ® Secure Configuration Manager™ 5.9.1 Security Target v3.0, August 27,2014

e. Evaluation Technical Report for EAL 2+ Common Criteria Evaluation of NetIQ Corporation NetIQ® Secure Configuration Manager™ 5.9.1 Document No. 1824-000-D002 Version 1.2, 27 October 2014.