Certification Report

NetScout nGeniusONE™ Unified Performance Management Platform V5.2.1 and nGenius® InfiniStream® V5.2.1

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

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) provide 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 CSC Security Testing/Certification Laboratories.

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 06 March 2015, 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:

- nGeniusONE™ is a trademark of NetScout Systems, Inc.
- nGenius® is a registered trademark of NetScout Systems, Inc.

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   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   INDEPENDENT FUNCTIONAL TESTING 7
    10.2   INDEPENDENT PENETRATION TESTING... 7
    10.3   CONDUCT OF TESTING 7
    10.4   TESTING RESULTS 7

11   Results of the Evaluation.. 7

12   Acronyms, Abbreviations and Initializations... 8

13   References 9

Executive Summary

NetScout nGeniusONE™ Unified Performance Management Platform V5.2.1 and nGenius® InfiniStream® V5.2.1 (hereafter referred to as NetScout nGenius® V5.2.1), from NetScout Systems, Inc., is the Target of Evaluation. The results of this evaluation demonstrate that nGenius® V5.2.1 is conformant with the Protection Profile for Network Devices, v1.1, June 8, 2012 (hereafter referred to as the NDPP).

NetScout nGenius® V5.2.1 consists of multiple software components that together address the following performance management disciplines:

• application and network monitoring

• network capacity planning, network troubleshooting

• fault detection

• service level management

The nGenius InfiniStream appliance passively and non-intrusively captures all network traffic and generates metrics to provide an operational understanding of application and network performance in live production environments.

The nGeniusONE™ Unified Performance Management platform unifies application and network performance management providing a top-down view into IP-based services, including voice, video and data.

CSC Security Testing/Certification Laboratories is the CCEF that conducted the evaluation. This evaluation was completed on 06 March 2015 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 NetScout nGenius® V5.2.1, 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 nGenius® V5.2.1 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

NetScout nGeniusONE™ Unified Performance Management Platform V5.2.1 and nGenius®
InfiniStream® V5.2.1 (hereafter referred to as NetScout nGenius® V5.2.1), from NetScout
Systems, Inc., is the Target of Evaluation. The nGenius® V5.2.1 is conformant with the
Protection Profile for Network Devices, v1.1, June 8, 2012 (hereafter referred to as the
NDPP).

2   TOE Description

NetScout nGenius® V5.2.1 consists of multiple software components that together address
the following performance management disciplines:

•   application and network monitoring;

•   network capacity planning, network troubleshooting;

•   fault detection;

•   service level management.

The nGenius® InfiniStream® appliance is an intelligent deep packet capture and analysis
appliance that delivers dedicated monitoring and continuous capture capabilities for real-time
and back-in-time analysis. The appliance can be used with the nGeniusONE™ Unified
Performance Management platform to analyze all packets traversing the network for problem
isolation and service delivery assurance.

The nGeniusONE™ server provides centralized management functionality to control and
monitor nGenius InfiniStream appliances and manage configuration parameters within the
nGeniusONE platform.

A diagram of the NetScout nGenius® V5.2.1 architecture is as follows:
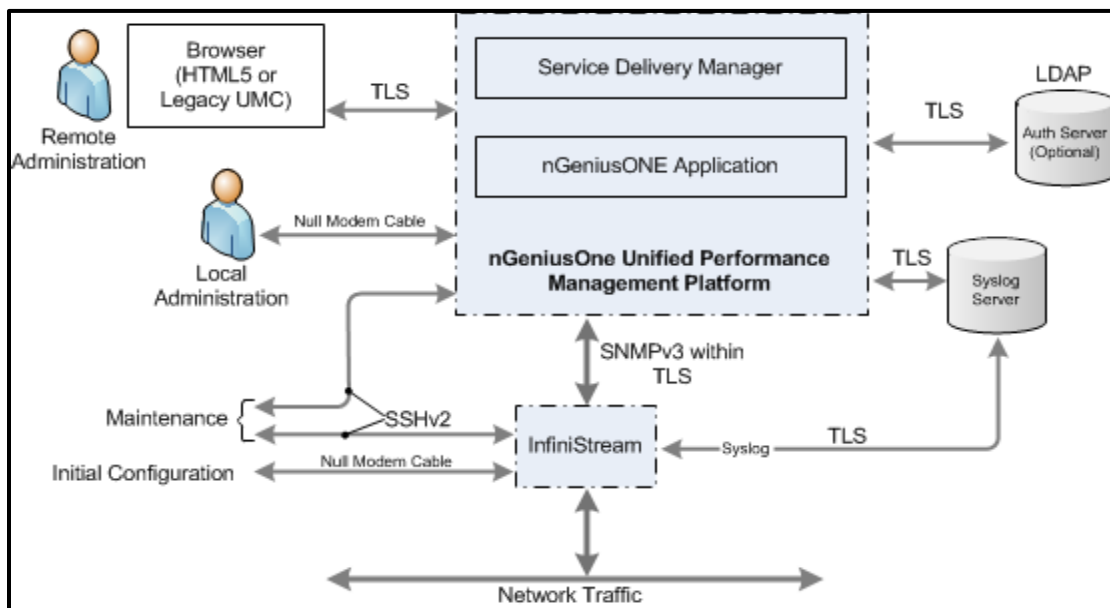
3   Security Policy

NetScout nGenius® V5.2.1 implements a role-based access control policy to control administrative access to the system. In addition, NetScout nGenius® V5.2.1 implements policies pertaining to the following security functional classes:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TOE Security Functionality (TSF)
- TOE Access
- Trusted Path/Channels

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

Cryptographic Module	Certificate #
OpenSSL FIPS Object Module	1747
NSS Cryptographic Module	1837

4   Security Target

The ST associated with this Certification Report is identified below:

NetScout Systems, Inc. nGeniusONE™ Unified Performance Management Platform (V5.2.1) and nGenius® InfiniStream® (V5.2.1) Security Target, Version 1.0, 06 March 2015.

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.*

NetScout nGenius® V5.2.1 is:

a. Conformant to the Protection Profile for Network Devices, v1.1, June 8, 2012,
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:*

- FAU_STG_EXT.1 - External audit trail storage
- FCS_CKM_EXT.4 - Cryptographic key zeroization
- FCS_RBG_EXT.1 - Cryptographic operation: random bit generation
- FCS_HTTPS_EXT.1 - HTTPS
- FCS_TLS_EXT.1 - TLS

- FIA_PMG_EXT.1 - Password management
- FIA_UIA_EXT.1 - User identification and authentication
- FIA_UAU_EXT.2 - Password-based authentication mechanism
- FPT_SKP_EXT.1 - Protection of TSF data
- FPT_APW_EXT.1 - Protection of administrator passwords
- FPT_TUD_EXT.1 - Trusted update
- FPT_TST_EXT.1 - TSF testing
- FTA_SSL_EXT.1 - TSF-initiated session locking

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 NetScout nGenius® V5.2.1 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:

- There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE; and
- TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

6.2   Environmental Assumptions

The following Environmental Assumption is listed in the ST:

- Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.

6.3   Clarification of Scope

The NetScout nGenius® V5.2.1network monitoring functionality was not included within the scope of this evaluation.

7   Evaluated Configuration

The evaluated configuration for NetScout nGenius® V5.2.1 comprises:

One or more instances of an InfiniStream appliance which may be any of the following:

- *nGenius InfiniStream 7900 Series;*
- *nGenius InfiniStream 6900 Series;*
- *nGenius InfiniStream 4500 Series;*
- *nGenius InfiniStream 2900 Series; and*

One instance of nGeniusONE Unified Performance Management Platform appliance that includes a licensed nGenius Service Delivery Manager application.

The publication entitled Common Criteria Supplemental Guidance for nGeniusONE™ Unified Performance Management Platform (V5.2.1) and nGenius® InfiniStream® (V5.2.1) (Part Number 733-0504 Rev A) describes the procedures necessary to install and operate nGenius® V5.2.1 in its evaluated configuration.

8   Documentation

The NetScout Systems, Inc. documents provided to the consumer are as follows:

a.   nGenius InfiniStream Administrator Guide (Part Number 733-0549 Rev. A),

b.   nGeniusONE™ Administrator Guide (Part Number 733-0547 Rev. A),

c.   nGeniusONE™ online help version 5.2, nGenius® Agent Administrator Guide for CDM v5.2.1 (Part Number 733-0528 Rev. A), and

d.   Common Criteria Supplemental Guidance for nGeniusONE™ Unified Performance Management Platform V5.2.1 and nGenius® InfiniStream® (V5.2.1) (Part Number 733-0504 Rev A).

9 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of NetScout nGenius® V5.2.1, including the following areas:

Development: The evaluators analyzed the NetScout nGenius® V5.2.1 functional specification and determined that the functional specification describes the purpose and method of use for each TSF interface and that the NetScout nGenius® V5.2.1 functional specification is an accurate and complete instantiation of the SFRs.

Guidance Documents: The evaluators examined the NetScout nGenius® V5.2.1 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 NetScout nGenius® V5.2.1 configuration management system and associated documentation was performed. The evaluators found that the NetScout nGenius® V5.2.1 configuration items were clearly marked.

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 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. NDPP required assurance activities: The objective of this test goal is to perform the assurance activities mandated by the NDPP to which the TOE is claiming conformance.

10.2 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. NDPP required assurance activities. The evaluator performed the assurance activities mandated by the protection profile to which the TOE is claiming conformance; and
b. Use of automated vulnerability scanning tools to discover potential network, platform and application layer vulnerabilities.

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

10.3 Conduct of Testing

NetScout nGenius® V5.2.1 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.

10.4 Testing Results

The independent tests yielded the expected results, providing assurance that NetScout nGenius® V5.2.1 behaves as specified in its ST and functional specification.

11 Results of the Evaluation

This evaluation has provided the basis for a NDPP conformance claim as claimed in Section 5. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

12 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
NDPP	Protection Profile for Network Devices
PALCAN	Program for the Accreditation of Laboratories - Canada
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

13 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.   Protection Profile for Network Devices, v1.1, June 8, 2012.

e.   NetScout Systems, Inc. nGeniusONE™ Unified Performance Management Platform (V5.2.1) and nGenius® InfiniStream® (V5.2.1) Security Target, Version 1.0, 06 March 2015.

f.   Evaluation Technical Report NetScout Systems, Inc. nGeniusONE™ Unified Performance Management Platform and nGenius® InfiniStream® V5.2.1, Version: 1.1, 06 March 2015.