Certification Report

NetIQ Access Manager 4.5

Sponsor and developer: ***NetIQ / Micro Focus Corporation***
Suite 1200, 515 South Post Oak Blvd
Houston, Texas 77027
USA

Evaluation facility: ***Brightsight***
Brassersplein 2
2612 CT Delft
The Netherlands

Report number: **NSCIB-CC-0006151-CR**

Report version: **1**

Project number: **0006151**

Author(s): **Kjartan Jæger Kvassnes**

Date: **7 November 2019**

Number of pages: **13**

Number of appendices: **0**

Headoffice:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Dutch Chamber of Commerce under number 27288788

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

Certificate

Standard	Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 5 (ISO/IEC 15408)
Certificate number	**CC-19-0006151**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer	**NetIQ Inc.** **Suite 1200, 515 South Post Oak Blvd, Houston, Texas 77027, USA**
Product and assurance level	**NetIQ Access Manager 4.5** Assurance Package: EAL3 augmented with ALC_FLR.1
Project number	**0006151**
Evaluation facility	**Brightsight BV located in Delft, the Netherlands** Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 5 (ISO/IEC 18045)

Common Criteria Recognition Arrangement for components up to EAL2

SOGIS Mutual Recognition Agreement for components up to EAL4

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation version 3.1 Revision 5 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 5. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report. The evaluation has been conducted in accordance with the provisions of the Netherlands scheme for certification in the area of IT security [NSCIB] and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by TÜV Rheinland Nederland B.V. or by other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Rheinland Nederland B.V. or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Validity	Date of 1st issue : **07-11-2019** Certificate expiry : **07-11-2024**

PRODUCTS
RvA C 078
Accredited by the Dutch Council for Accreditation

C.C.M. van Houten, LSM Systems
TÜV Rheinland Nederland B.V.
Westervoortsedijk 73, 6827 AV Arnhem
P.O. Box 2220, NL-6802 CE Arnhem
The Netherlands

TÜVRheinland®
Precisely Right.

CONTENTS:

TÜVRheinland®
Precisely Right.

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TÜV Rheinland Nederland B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TÜV Rheinland Nederland B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TÜV Rheinland Nederland B.V. to perform Common Criteria evaluations; a significant requirement for such a license is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TÜV Rheinland Nederland B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, 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 or site satisfies the security requirements stated in the (site) security target.

Recognition of the certificate

Presence of the Common Criteria Recognition Arrangement and SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement and will be recognised by the participating nations

International recognition

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC. Starting September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

European recognition

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA) version 3 effective from April 2010 provides mutual recognition of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (resp. E3-basic) is provided for products related to specific technical domains. This agreement was initially signed by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOGIS-MRA in December 2010. The current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies can be found on: http://www.sogisportal.eu.eIDAS-Regulation

TÜV Rheinland Nederland BV, operating the Netherlands Scheme for Certification in the Area of IT Security (NSCIB), has been notified as a Designated Certification Body from The Netherlands under Article 30(2) and 39(2) of Regulation 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the NetIQ Access Manager 4.5. The developer of the NetIQ Access Manager 4.5 is NetIQ / Micro Focus Corporation located in Houston, Texas, USA and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The TOE, NetIQ Access Manager 4.5 provides Single Sign-on (via SAML, OAuth/OIDC, Liberty, WS-Fed) to the enterprise web application. The TOE provides authorized users with secure access to intranet and cloud applications based on the context and information of who they are, where they are located and what devices they are using and where they are located.

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 11 October 2019 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the NetIQ Access Manager 4.5, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the NetIQ Access Manager 4.5 are advised to verify that their own environment is consistent with 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 provides sufficient evidence that the TOE meets the EAL3 augmented (EAL3+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_FLR.1.2 (Basic Flaw Remediation).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 5 *[CC]*.

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. It should be noted that the certification results only apply to the specific version of the product as evaluated.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the NetIQ Access Manager 4.5 from NetIQ / Micro Focus Corporation located in Houston Texas, USA.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Software	NetIQ Access Manager	4.5.0.0.191

To ensure secure usage a set of guidance documents is provided together with the NetIQ Access Manager 4.5. Details can be found in section “Documentation” of this report.

2.2 Security Policy

The TOE, NetIQ Access Manager 4.5 provides Single Sign-on (via SAML, OAuth/OIDC, Liberty, WS-Fed) to the enterprise web application. The TOE provides authorized users with secure access to intranet and cloud applications based on the context and information of who they are, where they are located and what devices they are using and where they are located.

The TOE supports various types of authentication including multi-factor authentication and one can configure a type authentication for a resource.

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. Detailed information on these security objectives that must be fulfilled by the TOE environment can be found in section 3.4 of the *[ST]*.

2.3.2 Clarification of scope

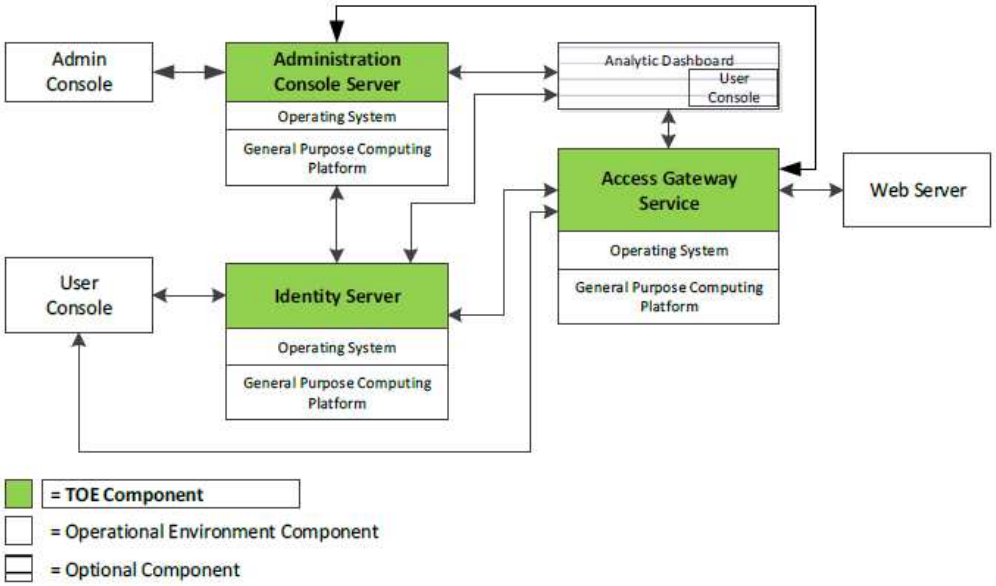
The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

2.4 Architectural Information

The TOE includes of the following components:

- Administration Console Server: Allows you to configure and manage each component, and allows you to centrally manage resources, such as policies, hardware, and certificates, which are used by multiple components.
- Identity Server: Responsible for authenticating users and distributing role information to facilitate authorization decisions.
- Access Gateway Service: Provides secure access to existing HTTP-based Web servers. It provides the typical security services (authorization, single sign-on, and data encryption), and is integrated with the identity and policy services of Access Manager.

The logical architecture of the TOE can be depicted as follows:



2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Identifier	Version
NetIQ Access Manager 4.5 Operational Guidance and Installation Procedures	v2.0, 11/10/2019
Access Manager 4.5 Administration Guide	April 2019
Access Manager 4.5 Best Practices Guide	April 2019
Access Manager 4.5 Installation and Upgrade Guide	April 2019
Access Manager 4.5 Security Guide	April 2019

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

The test environment is based on the developer's test plan. The test strategy took into account the dependencies of the test cases of the developer and the evaluator chose to repeat all the test cases as the test cases are related to each other which make it difficult to sample.

The evaluator have reproduced all of the developer tests, and additionally 10 test cases designed by the evaluator.

2.6.2 Independent Penetration Testing

To identify potential vulnerabilities the evaluator performed the following activities:

- SFR design analysis: Based on the information obtained in the evaluation evidence, the SFR implementation details were examined. The aspects described in CEM annex B were considered. During this examination several potential vulnerabilities were identified.
- Additional security analysis: When the implementation of the SFR was understood, a coverage check was performed on the relevant aspects of all SFRs. This expanded the list of potential vulnerabilities.

- Public vulnerability search: The evaluator performed public domain vulnerability search based on the TOE name, TOE type, and identified 3rd party security relevant libraries and/or services. Several additional potential vulnerabilities were identified during a search in the public domain.
- The potential vulnerabilities identified were analysed, and some of the potential vulnerabilities were concluded not exploit within in the Basic attack potential, or covered by guidance. For remaining potential vulnerabilities, penetration tests were devised.

The evaluator focused on the following for devising penetration tests:

- Remote accessible interfaces/protocols.
- Trying to misuse (including brute force) the Web GUI interface
- Performing generic web fuzzing
- Trying to disrupt audit record generations.

2.6.3 Test Configuration

The developer tested the TOE (version 4.5.0.0.191).

2.6.4 Testing Results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

2.7 Evaluated Configuration

The TOE is defined uniquely by its name and version number NetIQ Access Manager 4.5.

2.8 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*[2] and which references an ASE Intermediate Report and other evaluator documents.

The verdict of each claimed assurance requirement is "**Pass**".

Based on the above evaluation results the evaluation lab concluded the NetIQ Access Manager 4.5, to be **CC Part 2 conformant, CC Part 3 conformant**, and to meet the requirements of **EAL 3 augmented with ALC_FLR.1**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

2.9 Comments/Recommendations

The user guidance as outlined in section 2.5 contains necessary information about the usage of the TOE.

In addition all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

[2] The Evaluation Technical Report contains information proprietary to the developer and the evaluator and is not releasable for public review

3 Security Target

The NetIQ Access Manager 4.5 Security Target, v2.0, 11/10/2019 *[ST]* is included here by reference.

4 Definitions

IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT security
PP	Protection Profile
TOE	Target of Evaluation

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report:

[CC] Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017.

[CEM] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.

[ETR] Evaluation Technical Report NetIQ Access Manager 4.5, 19-RPT-734 ETR v1.0 15 October 2019.

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019.

[NSP#6] NSCIB Scheme Procedure 6 Alternative Evaluator Reporting, v1.3 draft, 20 October 2016

[NSI#00] NSI_00_International_Supporting_Documents, version 1.4

[NSI#7] NSCIB Scheme Instruction 07 Side Audits, v4.1, 1 June 2018

[NSI#9] NSCIB Scheme Instruction 09 Clarification of the TSFI concept, v1.1, 1 October 2017

[ST] NetIQ Access Manager 4.5 Security Target, v2.0, 11/10/2019.

(This is the end of this report).