Swedish Certification Body for IT Security

Certification Report NetIQ Access Manager 4.0

Issue: 1.0, 2014-sep-17

Authorisation: Jerry Johansson, , CSEC

Table of Contents

1 Executive Summary

The Target of Evaluation, TOE, is the three software parts of a single sign-on solution for enterprise web applications, NetIQ Access Manager 4.0. The operating systems are not included in the TOE.

The TOE provides configurable user identification and authentication mechanisms, and the capability to secure the communications between the user, the TOE, and the enterprise web applications. The TOE also provides configurable identity federations and identity translations between the users and the web application domains, as well as configurable user access control for the web applications. The system is modular and scalable. The cryptographic implementations are included in the scope of the TOE.

The certified version of the TOE is "NetIQ Access Manager 4.0.1-88 + HF 1-93".

The ST does not claim conformance to any Protection Profiles (PPs).

There are seven assumptions made in the ST regarding the secure usage and environment of the NetIQ Access Manager 4.0. The TOE relies on these being met to counter the three threats in the ST. The assumptions and the threats are described in chapter 4 Assumptions and Clarifications of Scope.

The evaluation has been performed by Combitech AB in Växjö and Sundbyberg, Sweden, partly with the assistance of Electronic Warfare Associates-Canada Ltd. in Ottawa, Canada. Site-visit and parts of the testing were performed on-site in the developers premises in Bangalore, India.

The evaluation was completed in 2014-08-20. The evaluation was conducted in accordance with the requirements of Common Criteria (CC), version 3.1, release 4 and the Common Methodology (CEM) version 3.1, release 4. The evaluation was performed at the evaluation assurance level EAL 3, augmented by ALC_FLR.1 Basic flaw remediation.

Combitech AB is a licensed evaluation facility for Common Criteria under the Swedish Common Criteria Evaluation and Certification Scheme. Combitech AB are also accredited by the Swedish accreditation body SWEDAC according to ISO/IEC 17025 for Common Criteria.

Electronic Warfare Associates-Canada Ltd. operates as a Foreign Location for Combitech AB within the scope of the Swedish Common Criteria Evaluation and Certification Scheme.

The certifier monitored the activities of the evaluator by reviewing all successive versions of the evaluation reports, and by observing site-visit and testing. The certifier determined that the evaluation results confirm the security claims in the Security Target (ST), and have been achieved in agreement with the requirements of the Common Criteria and the Common Methodology for evaluation assurance level EAL 3 augmented by ALC_FLR.1.

The technical information in this report is based on the Security Target [ST] and the Final evaluation report produced by Combitech AB.

2 Identification

Certification Identification

Certification ID	CSEC2013005
Name and version of the certified IT product and the TOE	NetIQ Access Manager 4.0.1-88+HF1-93 NetIQ is a registered trademark of NetIQ Corporation Access Manager is a trademark of NetIQ Corporation
Security Target	Security Target: NetIQ Access Manager 4.0, NetIQ Corporation, 2014-08-07, document version 1.13
Assurance level	EAL 3 + ALC_FLR.1
Sponsor	NetIQ Corporation
Developer	NetIQ Corporation
ITSEF	Combitech AB and EWA-Canada Ltd.
Common Criteria version CEM version	3.1 release 4 3.1 release 4
QMS version	1.16.2
Certification date	2014-09-17

3 Security Policy

The TOE provides the following security services:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Trusted Channels.

3.1 Security Audit

The TOE generates audit records interactions between the User Console and the Access Gateway Service, and between the Access Gateway Service and the backend web servers. Each audit record contains date and time, type of action, and the outcome of the action.

3.2 Cryptographic Support

The TOE has the capability to use HTTPS with TLS when communicating with the User Console and backend web servers. TLS is always used between the system parts. In the evaluated configuration, the TOE uses the following algorithms:

- AES-128 in CBC mode for encryption and decryption
- RSA for user authentication (2048 bit, RSASSA-PKCS1-v1_5)
- HMAC SHA-1 for message authentication.

3.3 User Data Protection

The TOE provides protection against unauthorized access to the backend web servers.

Required user authentication method and permitted access is configured on an individual basis by the administrator.

3.4 Identification and Authentication

The TOE requires that users successfully identify and authenticate prior to gaining access to TOE functions and data.

3.5 Security Management

The TOE allows only Administrators to access the TOE functions to query, create, modify, and delete the following security attributes:

- Access Gateway Conditions
- Identity Injection Actions
- Form Fill Options.

3.6 Trusted Channels

The TOE implements secure communications between the User Console and Identity Server and Access Gateway Service using HTTPS with TLS. The TOE also implements HTTPS with TLS between the Access Gateway Service and the back-end web servers.

4 Assumptions and Clarifications of Scope

4.1 Usage Assumptions

The Security Target [ST] makes three assumptions on the usage of the TOE.

A.MANAGE - Administrators of the TOE are assumed to be properly trained and able to install, configure and maintain the TOE in a secure and trusted manner.

A.NOEVIL - Administrators of the TOE, and users on the local network, are assumed not to be careless, wilfully negligent, nor hostile, and to follow the instructions in the TOE documentation.

A.CONFIG - It is assumed that passwords, certificates, and other necessary data used for user identification and authentication will be transferred to the TOE and kept up-to -date.

4.2 Environmental Assumptions

The Security Target [ST] makes four assumptions on the operational environment of the TOE.

A.LOCATE - The processing platforms on which TOE resides are assumed to be located within a facility that provides controlled access.

A.TIMESOURCE - It is assumed that the TOE has access to a trusted source for system time.

A.WEB_PROTECT - It is assumed that the operational environment protects corporate web servers from external access, except through the TOE.

A.HTTPS - It is assumed that the web browsers used to access the TOE support HTTPS using TLS, and that the web servers in the intranet support HTTPS using TLS.

4.3 Clarification of Scope

The Security Target contains three threats, which have been considered during the evaluation.

T.NO_AUTH An unauthorized user may gain access to the TOE and alter the user access policies and gain unauthorized access to corporate web servers.

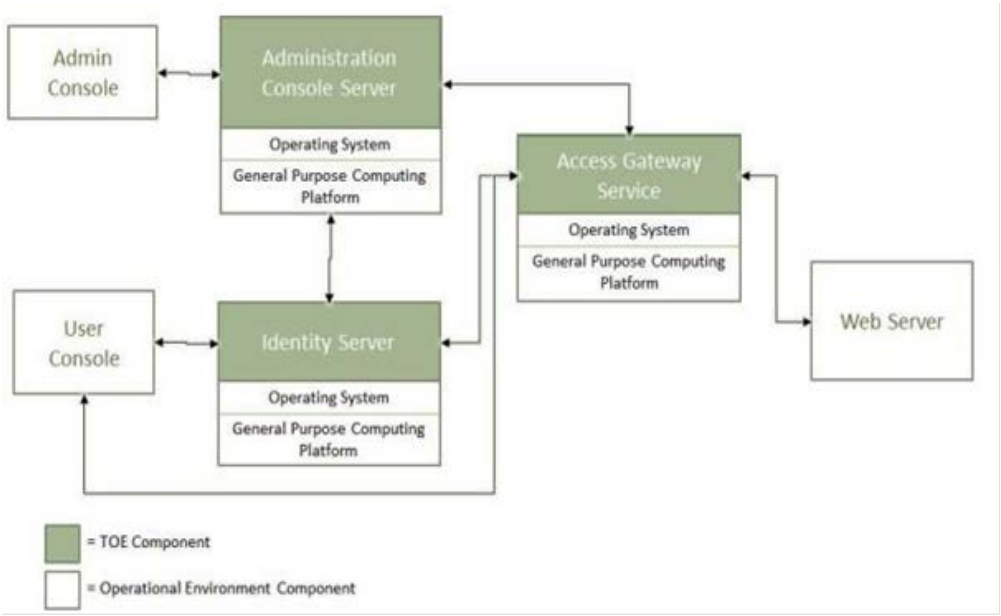
T.NO_PRIV An authorized user of the TOE exceeds his/her assigned security privileges resulting in unauthorized modification of the TOE configuration and/or data including user access policies.

T.USER_ACTION_DENY Users may be able to access user authentication data and user access policies and deny their access to it later.

5 Architectural Information

The TOE consists of software only and is divided in the following subsystems:

- Administration Console Server
- Identity Console Server
- Access Gateway Server.



The Administration Console Server is the central configuration and management tool for the product. It can be used only to manage the Access Manager components. It contains a Dashboard option, which allows you to assess the health of all Access Manager components.

The Administration Console also 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.

The Identity Server is the central authentication and identity access point for all other services. It is responsible for authenticating users and distributing role information to facilitate authorization decisions. It also provides the Liberty Alliance Web Service Framework to distribute identity information.

An Identity Server always operates as an identity provider and can optionally be configured to run as an identity consumer (also known as a service provider), using Liberty, SAML 1.1, or SAML 2.0 protocols. As an identity provider, the Identity Server validates authentications against the supported identity user store, and is the heart of the user's identity federations or account linkage information.

In an Access Manager configuration, the Identity Server is responsible for managing:

- Authentication
- Identity Stores
- Identity Federation
- Account Provisioning
- Custom Attribute Mapping

- SAML Assertions
- Single Sign.on and Logout
- Identity Integration
- Clustering.

An 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) previously provided by Novell iChain, and is integrated with the new identity and policy services of Access Manager.

The Access Gateway Service is designed to work with the Identity Server to enable single sign-on to protected Web services. The following features facilitate single sign-on to Web servers that are configured to enforce authentication or authorization policies:

- Access Gateway
- Identity Injection
- Form Fill.

6 Documentation

The following documents are included in the scope of the TOE:

Operational User Guidance and Preparative Procedures Supplement [SUP]

Access Manager 4.0 Readme [Readme]

Installation Guide [Install]

Setup Guide [Setup]

Access Gateway Guide [AGG]

Administration Console Guide [ACG]

Identity Server Guide [ISG]

Policy Guide [PG]

SSL VPN Server Guide [VPN]

Best Practises Guide [BPG]

Access Manager 4.0 Service Pack 1 Hotfix 1 Readme [SP1 Readme]

Installation Guide, Access Manager 4.0 SP1 [Install SP1].

7 IT Product Testing

7.1 Developer Tests

The developer's testing covers the security functional behaviour of all TSFIs and interactions of all subsystems. The relevance, coverage and depth of the developer tests has been examined and verified by the evaluators during the evaluation.

7.2 Independent Evaluator Tests

The evaluator repeated all the developer's tests.

The evaluator conducted and executed seven additional test cases to cover more of the TOE security functionality behaviour, including manual penetration testing. The functionality testing covered:

- Installation and configuration
- Access control
- Cryptographic functionality (source code and configuration review)
- SSL/TLS version handling

The TSFI was exercised via consoles used for administration. User traffic and the TOE behavior was observed at the consoles and using a packet sniffer (Wireshark). All evaluator test cases were run on the evaluated configuration in a virtual environment (VMware/VirtualBox).

The developer's tests were repeated using TOE version NetIQ Access Manager 4.0.0-110 at the developer's site under oversight by the certifier. The developer's tests were later repeated using the TOE version NetIQ Access Manager 4.0.0-143 at the evaluator's site where also the evaluator's additional testing took place using the latter TOE version.

7.3 Penetration Tests

Three types of penetration tests were executed:

- Port scanning
- Fuzzing
- Vulnerability scanning

The User Console and the Web Server interface, facing WAN and LAN networks, were scanned for open ports and available services. The tool NMAP (www.nmap.org) was used configured for TCP Connect, TCP SYN, and IP scanning.

To verify the stability of the User Console interface, the HTTPS identification and authentication methods were fuzzed using various different inputs. The tool WebScarab (www.owasp.org) was used.

To reveal possible vulnerabilities, the User Console interface, facing an unprotected WAN network at the Identity Server and the Access Gateway Service, was scanned using the Nessus (www.tenable.com) vulnerability scanner.

In addition some manual penetration tests were performed as variations of the functional testing.

8 Evaluated Configuration

The TOE sub systems shall run on PC hardware fulfilling the following minimum requirements:

- 100 GB of disk space
- 4 GB RAM
- X86-64 bit Dual or Core 2 Duo processors, 3.0 GHz, or comparable chip

The TOE sub systems shall run on the following operating system:

- SUSE Linux Enterprise System 11 SP1, 64 bit.

The TOE shall be installed and configured in accordance with the TOE guidance listed in chapter 6 of this document.

9 Results of the Evaluation

The evaluators applied each work unit of the Common Methodology [CEM] within the scope of the evaluation, and concluded that the TOE meets the security objectives stated in the Security Target [ST] for a *Basic* attack potential.

The certifier reviewed the work of the evaluator and determined that the evaluation was conducted in accordance with the Common Criteria [CC].

The evaluators overall verdict is PASS.

The verdicts for the respective assurance classes and components are summarised in the following table:

Assurance Class/Family	*Short name*	*Verdict*
Development	ADV	PASS
Security Architecture	ADV_ARC.1	PASS
Functional Specification	ADV_FSP.3	PASS
TOE Design	ADV_TDS.2	PASS
Guidance Documents	AGD	PASS
Operational User Guidance	AGD_OPE.1	PASS
Preparative Procedures	AGD_PRE.1	PASS
Life-cycle Support	ALC	PASS
CM Capabilities	ALC_CMC.3	PASS
CM Scope	ALC_CMS.3	PASS
Delivery	ALC_DEL.1	PASS
Development Security	ALC_DVS.1	PASS
Flaw Remediation	ALC_FLR.1	PASS
Life-cycle Definition	ALC_LCD.1	PASS
Security Target Evaluation	ASE	PASS
ST Introduction	ASE_INT.1	PASS
Conformance Claims	ASE_CCL.1	PASS
Security Problem Definition	ASE_SPD.1	PASS
Security Objectives	ASE_OBJ.2	PASS
Extended Components Definition	ASE_ECD.1	PASS
Security Requirements	ASE_REQ.2	PASS
TOE Summary Specification	ASE_TSS.1	PASS
Tests	ATE	PASS
Coverage	ATE_COV.2	PASS
Depth	ATE_DPT.1	PASS
Functional Tests	ATE_FUN.1	PASS
Independent Testing	ATE_IND.2	PASS
Vulnerability Assessment	AVA	PASS
Vulnerability Analysis	AVA_VAN.2	PASS

10 Evaluator Comments and Recommendations

None.

11 Acronyms

AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
HMAC	Hashed Message Authentication Code
HTML	Hypertext Markup Language
HTTPS	Hyper Text Transport Protocol Secure
IP	Internet Protocol
NTP	Network Time Protocol
SAML	Secure Assertion Markup Language
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SLES	SUSE Linux Enterprise Server
TLS	Transport Layer Security
TOE	Target of Evaluation

12 Bibliography

ST	Security Target NetIQ Access manager 4.0, NetIQ Corporation, 2014-08-07, document version 1.13
SUP	Operational User Guidance and Preparative Procedures Supplement: NetIQ Access manager 4.0, NetIQ Corporation, 2014-06-23, document version 1.4
Readme	Access Manager 4.0 Readme, NetIQ Corporation, Nov 2013
Install	Installation Guide Access manager 4.0, NetIQ Corporation, November 2013
Setup	Setup Guide Access manager 4.0, NetIQ Corporation, November 2013
AGG	Access Gateway Guide Access manager 4.0, NetIQ Corporation, November 2013
ACG	Administration Console Guide Access manager 4.0, NetIQ Corporation, November 2013
ISG	Identity Server Guide Access manager 4.0, NetIQ Corporation, November 2013
PG	Policy Guide Access manager 4.0, NetIQ Corporation, November 2013
VPN	SSL VPN Server Guide Access manager 4.0, NetIQ Corporation, November 2013
BPG	Best Practises Guide Access manager 4.0, NetIQ Corporation, November 2013
SP1 Readme	Access Manager 4.0 Service Pack 1 Hotfix 1 Readme, NetIQ Corporation, June 2014
Install SP1	Installation Guide, Access Manager 4.0 SP1, NetIQ Corporation, May 2014

CCpart1	Common Criteria for Information Technology Security Evaluation, Part 1, version 3.1 revision 4, CCMB-2012-09-001
CCpart2	Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1 revision 4, CCMB-2012-09-002
CCpart3	Common Criteria for Information Technology Security Evaluation, Part 3, version 3.1 revision 4, CCMB-2012-09-003
CC	CCpart1 + CCpart2 + CCpart3
CEM	Common Methodology for Information Technology Security Evaluation, version 3.1 revision 4, CCMB-2012-09-004
SP-002	SP-002 Evaluation and Certification, CSEC, 2013-09-30, document version 20.0
SP-188	SP-188 Scheme Crypto Policy, CSEC, 2013-06-18, document version 4.0

Appendix A - QMS Consistency

During the certification project, the following versions of the quality management system (QMS) have been applicable since the certification application was received 2013-11-15:

QMS 1.15 valid from 2013-10-23

QMS 1.16 valid from 2014-02-13

QMS 1.16.1 valid from 2014-02-27

QMS 1.16.2 valid from 2014-10-23

In order to ensure consistency in the outcome of the certification, the certifier has examined the changes introduced in each update of the quality management system.

The changes between consecutive versions are outlined in “Ändringslista QMS 1.16.2”.

The certifier concluded that, from QMS 1.15 to the current QMS 1.16.2, there are no changes with impact on the result of the certification.