Swedish Certification Body for IT Security

Certification Report NetIQ® Identity Manager 4.7

Issue: 1.0, 2020-Jun-15

Authorisation: Helén Svensson, Lead Certifier , CSEC

Table of Contents

1 Executive Summary

The TOE is NetIQ Identity Manager 4.7.

It is a software TOE consisting of the components listed below that can be setup on separate hardware platforms, see the [ST], or as a virtual appliances.

TOE Components:

- Identity Applications (RBPM) 4.7.3.0.1109
- Identity Manager Engine 4.7.3.0.AE
- Identity Reporting Module 6.5.0. F14508F
- Sentinel Log Management for Identity Governance and Administration 8.2.2.0_5415
- One SSO Provider (OSP) 6.3.3.0
- Self Service Password Reset (SSPR) 4.4.0.2 B366 r39762

The TOE is delivered as software with documentation and can be installed in a physical or virtual environment.

It is important to verify the integrity of the TOE for secure acceptance of the TOE in accordance with the preparative procedures of the guidance, i.e. verify the TLS connection, the CA certificate and the file hash. It is also important to update the TOE (including 3rd party software) and the operational environment of the TOE in accordance with the preparative procedures of the guidance to mitigate known vulnerabilities.

No conformance claims to any PP are made for the TOE.

The evaluation has been performed by Combitech AB in Växjö, Sweden and by EWA-Canada in Ottawa, Canada. Site Visit and parts of the testing was performed at the developer's site in Bangalore, India.

The evaluation was completed on 2020-06-02. The evaluation was conducted in accordance with the requirements of Common Criteria, version 3.1 R5.

Combitech AB is a licensed evaluation facility for Common Criteria under the Swedish Common Criteria Evaluation and Certification Scheme. Combitech AB is also accredited by the Swedish accreditation body SWEDAC according to ISO/IEC 17025 for Common Criteria evaluation. EWA-Canada Ltd. operates as a Foreign location for Combitech AB within 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 the Common Methodology for evaluation assurance level EAL3 augmented by ALC_FLR.2

As specified in the security target of this evaluation, the invocation of cryptographic primitives has been included in the TOE, while the implementation of these primitives has been located in TOE environment. Therefore the invocation of cryptographic primitives has been in the scope of this evaluation, while correctness of implementation of cryptographic primitives been excluded from the TOE. Correctness of implementation is done through third party certification Cryptographic Module Validation Program (CMVP) certificate number 1747 referred to in the Security Target.

Users of this product are advised to consider their acceptance of this third party affirmation regarding the correctness of implementation of the cryptographic primitives.

2 Identification

Certification Identification	
Certification ID	CSEC2018013
Name and version of the certified IT product	NetIQ® Identity Manager 4.7 TOE components: • Identity Applications (RBPM) 4.7.3.0.1109 • Identity Manager Engine 4.7.3.0.AE • Identity Reporting Module 6.5.0. F14508F • Sentinel Log Management for Identity Governance and Administration 8.2.2.0_5415 • One SSO Provider (OSP) 6.3.3.0 • Self Service Password Reset (SSPR) 4.4.0.2 B366 r39762
Security Target Identification	NetIQ Identity Manager 4.7 Security Target (ST), NetIQ Corporation , 2020-06-01, document version 2.6
EAL	EAL3 + ALC_FLR.2
Sponsor	NetIQ Corporation
Developer	NetIQ Corporation
ITSEF	Combitech AB and EWA-Canada
Common Criteria version	3.1 release 5
CEM version	3.1 release 5
QMS version	1.23.2
Scheme Notes Release	15.0
Recognition Scope	CCRA, SOGIS and EA/MLA
Certification date	2020-06-15

3 Security Policy

The security features performed by the TOE are as follows:

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

3.1 Security Management

The TOE maintains operator roles. The individual roles are categorized into two main roles: the Administrator and the User.

Administrator - A user who has rights to configure and manage all aspects of the TOE

User - The user's capabilities can be configured to:

- View hierarchical relationships between User objects
- View and edit user information (with appropriate rights).
- Search for users or resources using advanced search criteria (which can be saved for later reuse).
- Recover forgotten passwords.

Only an Administrator can determine the behavior of, disable, enable, and modify the behavior of the functions that implement the Discretionary Access Control SFP. The TPE ensures only secure values are accepted for the security attributes listed with Discretionary Access Control SFP.

3.2 Security Audit

The TOE generates the following audit data:

- Start-up and shutdown of the audit functions (instantiated by startup of the TOE)
- User login/logout
- Login failures

The TOE provides the Administrator with the capability to read all audit data generated within the TOE via the console. The GUI provides a suitable means for an Administrator to interpret the information from the audit log.

The A.TIMESOURCE is added to the assumptions on operational environment, and OE.TIME is added to the operational environment security objectives. The time and date provided by the operational environment are used to form the timestamps. The TOE ensures that the audit trail data is stamped when recorded with a dependable date and time received from the OE (operating system). In this manner, accurate time and date is maintained on the TOE.

3.3 Identification and Authentication

The IDM console application provides user interfaces that administrators may use to manage TOE functions. The operating system and the database in the TOE Environment are queried to individually authenticate administrators or users. The TOE maintains authorization information that determines which TOE functions an authenticated administrators or users (of a given role) may perform.

The TOE maintains the following list of security attributes belonging to individual users:

- User Identity (i.e., user name)
- Authentication Status (whether the IT Environment validated the username/password)
- Privilege Level (Administrator or User)

3.4 User Data Protection

The TOE implements a discretionary access control policy to define what roles can access particular functions of the TOE. All access and actions for system reports, component audit logs, TOE configuration, operator account attributes (defined in FIA_ATD.1) are protected via access control list. When a user requests to perform an action on an object, the TOE verifies the role associated with the user name. Access is granted if the user (or group of users) has the specific rights required for the type of operation requested on the object.

Identity Manager can enforce password policies on incoming passwords from connected systems and on passwords set or changed through the User Application password self-service. If the new password does not comply, you can specify that Identity Manager not accept the password. This also means that passwords that don't comply with your policies are not distributed to other connected systems.

In addition, can enforce password policies on connected systems. If the password being published to the Identity Vault does not comply with rules in a policy, you can specify that Identity Manager not only does not accept the password for distribution, but actually resets the noncompliant password on the connected system by using the current Distribution password in the Identity Vault.

3.5 Trusted Path / Channel

The TOE provides a trusted channel between the TOE and external web servers.

The TOE provides a trusted path for TOE administrators and TOE users to communicate with the TOE. The trusted path is implemented using HTTPS. The TOE’s implementation of TLS is described in the previous section (Trusted Channel).

3.6 Cryptographic Support

Cryptographic protection of data in transit between the TOE and remote users, and between the TOE and external web servers is provided by the OpenSSL FIPS Object Module software version 2.0.10 (Cryptographic Module Validation Program (CMVP) certificate number 1747) libraries.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

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

A.MANAGE - Administrators of the TOE are assumed to be appropriately trained to undertake the installation, configuration and management of the TOE in a secure and trusted manner.

A.NOEVIL - Administrators of the TOE and users on the local area network are not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the TOE documentation

4.2 Environmental Assumptions

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

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

A.CONFIG - The TOE is configured to receive all passwords and associated data from network-attached systems.

A.TIMESOURCE - The TOE has a trusted source for system time via NTP server

4.3 Clarification of Scope

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

T.NO_AUTH - An unauthorized user may gain access to the TOE and alter the TOE configuration.

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.

T.USER_ACCESS_DENY - An authorized user may be able to change user authentication data and or user access policies and deny their access to it later.

T.PASSWD_COMPROMISE - An unauthorized user may be able to obtain and use user passwords.

T.PROT_TRANS - An unauthorized user may be able to gather information from communications between components.

The Security Target contains one Organisational Security Policies (OSPs), which have been considered during the evaluation.

P.REMOTE_DATA - Passwords and account information from network-attached systems shall be monitored and managed.

5 Architectural Information

The TOE consists of the following components:

- Administration Workstation (Console)2
- Identity Applications (RBPM)
  - Designer aka Identity Manager Designer
  - Analyzer aka Identity Manager Analyzer
- Identity Manager
- Identity Manager Engine
  - Identity Vault
  - iManager
- Reporting Server
  - Identity Reporting Module
- Log Manager
  - Sentinel Log Management for Identity Governance and Administration
- SSO Provider
  - One SSO Provider (OSP)
- Self Service Password Reset
  - Self Service Password Reset (SSPR)

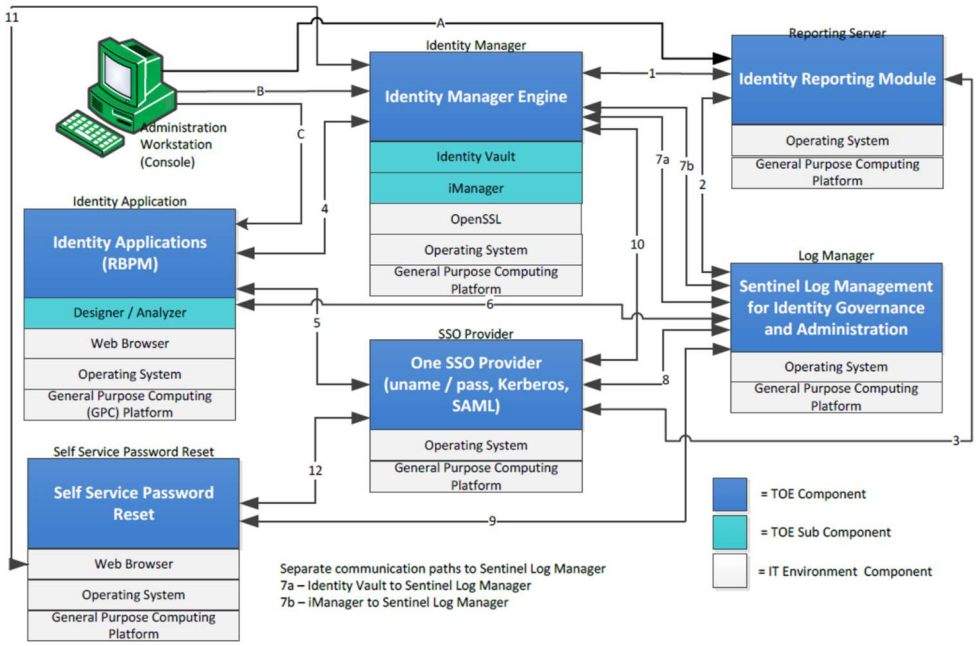

Figure 1, TOE Deployment with subsystems

The TOE provides the following functions: data synchronization, role management, auditing/reporting, and management.

- Data synchronization, including password synchronization, is provided by the base components of the Identity Manager solution: the Identity Vault, Identity Manager engine, drivers, Remote Loader, and connected applications
- Role management is provided by the User Application
- Auditing and reporting are provided by the Identity Reporting Module

6 Documentation

The TOE includes the following guidance documentation:

- Quick Start Guide for Installing NetIQ Identity Manager 4.7 February 2018 [QSIM]
- NetIQ Identity Manager Setup Guide for Linux February 2018 [SUL]
- NetIQ Identity Manager 4.7, Operational User Guidance and Preparative Procedures Supplement (AGD-IGS), version 0.6, is supplied for those customers that need guidance on how to set the TOE in the evaluated configuration. [AGD]

7 IT Product Testing

7.1 Developer Testing

There are 30 test cases covering all SFRs with at least one test per SFR. All tests were successful with a pass verdict.

7.2 Evaluator Testing

Since all SFRs and security function requirements were tested by the developer the evaluator focused on repetition of the developer's test cases and penetration testing.

7.3 Penetration Testing

Port and vulnerability scan were performed on Identity manager engine, Identity applications (RBPM), and Identity reporting module.

No unforeseen ports or vulnerabilities were found.

8 Evaluated Configuration

The TOE consists of a set of software applications run on one or multiple distributed systems. The TOE requires the following software components as part of the evaluated configuration:

Component	Requirements
Administration Workstation	Mozilla Firefox 65
Identity Applications (RBPM)	SUSE Linux Enterprise Server 12 SP4
Designer / Analyzer)	
Identity Manager (Identity Manager Engine)	SUSE Linux Enterprise Server 12 SP4
Reporting Server (Identity Reporting Module)	SUSE Linux Enterprise Server 12 SP4
Log Manager (Sentinel Log Management for Identity Governance and Administration)	SUSE Linux Enterprise Server 12 SP4
SSO Provider (OneSSO Provider)	SUSE Linux Enterprise Server 12 SP4
Self Service Password Reset	SUSE Linux Enterprise Server 12 SP4

In addition to the platform requirements mentioned above, the following hardware resources are needed in order to install and configure Identity Manager on each platform:

- A minimum of 8 GB RAM
- 15 GB available disk space to install all the components.
- Additional disk space to configure and populate data. This might vary depending on your connected systems and number of objects in the Identity Vault.

For server-based components, it is recommended that the platform have a minimum of 2 CPUs or cores.

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 an attack potential of Basic.

The certifier reviewed the work of the evaluators 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 description	ADV_ARC.1	PASS
Functional specification with complete summary	ADV_FSP.3	PASS
Architectural 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
Authorisation controls	ALC_CMC.3	PASS
Implementation representation CM coverage	ALC_CMS.3	PASS
Delivery procedures	ALC_DEL.1	PASS
Identification of security measures	ALC_DVS.1	PASS
Developer defined life-cycle model	ALC_LCD.1	PASS
Flaw reporting procedures	ALC_FLR.2	PASS
Security Target evaluation	ASE:	PASS
Conformance claims	ASE_CCL.1	PASS
Extended components definition	ASE_ECD.1	PASS
ST introduction	ASE_INT.1	PASS
Security objectives	ASE_OBJ.2	PASS
Derived security requirements	ASE_REQ.2	PASS
Security problem definition	ASE_SPD.1	PASS
TOE summary specification	ASE_TSS.1	PASS
Tests	ATE:	PASS
Analysis of coverage	ATE_COV.2	PASS
Testing: basic design	ATE_DPT.1	PASS
Functional testing	ATE_FUN.1	PASS
Independent testing - sample	ATE_IND.2	PASS
Vulnerability assessment	AVA:	PASS
Vulnerability analysis	AVA_VAN.2	PASS

10 Evaluator Comments and Recommendations

None.

11 Glossary

CC	Common Criteria version 3.1
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
IDM	Identity Manager
ITSEF	IT Security Evaluation Facility, test laboratory licensed to operate within a evaluation and certification scheme
NTP	Network Time Protocol
OSP	Organizational Security Policy
OSP	One SSO Provider
SSO	Single Sign On
SFP	Security Function Policy
SFR	Security Functional Requirement
SSPR	Self Service Password Reset
ST	Security Target
TOE	Target of Evaluation

12 Bibliography

ST	NetIQ Identity Manager 4.7 Security Target (ST), NetIQ Corporation, 2020-06-01, document version 2.6
QSIM	Quick Start Guide for Installing NetIQ Identity Manager 4.7 February 2018
SUL	NetIQ Identity Manager Setup Guide for Linux February 2018
AGD	NetIQ Identity Manager 4.7, Operational User Guidance and Preparative Procedures Supplement (AGD-IGS), version 0.6
CCpart1	Common Criteria for Information Technology Security Evaluation, Part 1, version 3.1 revision 5, CCMB-2017-04-001
CCpart2	Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1 revision 5, CCMB-2017-04-002
CCpart3	Common Criteria for Information Technology Security Evaluation,Part 3, version 3.1 revision 5, CCMB-2017-04-003
CC	CCpart1 + CCpart2 + CCpart3
CEM	Common Methodology for Information Technology Security Evaluation, version 3.1 revision 5, CCMB-2017-04-004
SP-002	SP-002 Evaluation and Certification, CSEC, 2019-09-24, document version 31.0

Appendix A Scheme Versions

During the certification the following versions of the Swedish Common Criteria Evaluation and Certification scheme have been used.

A.1 Scheme/Quality Management System

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

QMS 1.21.5 valid from 2018-11-19

QMS 1.22 valid from 2019-02-01

QMS 1.22.1 valid from 2019-03-08

QMS 1.22.2 valid from 2019-05-02

QMS 1.22.3 valid from 2019-05-20

QMS 1.23 valid from 2019-10-14

QMS 1.23.1 valid from 2020-03-06

QMS 1.23.2 valid from 2020-05-11

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 CSEC QMS 1.23.1". The certifier concluded that, from QMS 1.21.5 to the current QMS 1.23.2, there are no changes with impact on the result of the certification.

Note that the SP-188 Scheme Crypto Policy version 9.0 was introduced in QMS 1.23. The certification application was submitted before the SP-188 Scheme Crypto Policy version 9.0 was introduced and therefore version 8.0 was used.

A.2 Scheme Notes

The following Scheme interpretations have been considered during the certification.

- Scheme Note 15 - Demonstration of test Coverage
- Scheme Note 18 - Highlighted Requirements on the Security Target
- Scheme Note 22 - Vulnerability assessment
- Scheme Note 28 - Updated procedures for application, evaluation and certification