Swedish Certification Body for IT Security

Certification Report NetIQ Identity Manager 4.9.0

Issue: 1.0, 2025-jun-19

Authorisation: Jerry Johansson, Lead certifier , CSEC

Table of Contents

1 Executive Summary

The TOE is the software parts of the NetIQ Identity Manager 4.9.0.0000:

Identity Manager (engine) 4.9.0.0000

- Identity Vault 4.9.0.0000
- ID Console 1.7.2.0000

Identity Applications (RBPM) 4.9.0.0000

- Identity Manager Designer 4.9.0.0000
- Identity Manager Analyzer 4.9.0.0000

Identity Reporting Module

- NetIQ Identity Reporting 7.2.0000

Log Manager

- Sentinel Log Management for Identity Governance and Administration 8.6.1.0000

SSO Provider

- One SSO Provider (OSP) 6.7.0.0000

Self Service Password Reset

- Self Service Password Reset (SSPR) 4.7.0.2

excluding the operating systems which are considered part of the environment.

The implementation of the crypto module OpenSSL is considered part of the operating environment, but the invocation and usage of cryptographic functionality by the TOE is part of the evaluation.

The TOE type is an Identity Manager. The TOE facilitates managing of identity data between multiple systems.

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

There are six assumptions made in the ST regarding the secure usage and environment of the NetIQ Identity Manager 4.9.0. The TOE relies on these being met to counter the four threats and one organisational security policy 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 their premises in Bromma, Sweden. Site-visit and testing oversight at the developer's site in Bangalore, India, was performed virtually via Teams.

The evaluation was completed in 2025-06-04. The evaluation was conducted in accordance with the requirements of Common Criteria (CC), version 3.1, release 5 and the Common Methodology (CEM) version 3.1, release 5. The evaluation was performed at the evaluation assurance level EAL 3, augmented by ALC_FLR.3.

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.

The certifier monitored the activities of the evaluator by reviewing all successive versions of the evaluation reports. 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.3.

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

The certification results only apply to the version of the product indicated in the certificate, and on the condition that all the stipulations in the Security Target are met. This certificate is not an endorsement of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate is either expressed or implied.

2 Identification

Certification Identification	
Certification ID	CSEC2023005
Name and version of the certified IT product	NetIQ Identity Manager v.4.9.0.0000
Security Target Identification	NetIQ Identity Manager 4.9.0 Security Target
EAL	EAL 3 + ALC_FLR.3
Sponsor	OpenText Corporation
Developer	OpenText Corporation
ITSEF	Combitech AB
Common Criteria version	3.1 release 5
CEM version	3.1 release 5
QMS version	2.6
Scheme Notes Release	22.0
Recognition Scope	CCRA, SOGIS, EA/MLA
Certification date	2025–06–19

3 Security Policy

The TOE provides the following security services:

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

3.1 Security Management

The TOE restricts the ability to enable, modify and disable security policy rules and user roles to an authorized Administrator. The TOE also provides the functions necessary for effective management of the TOE security functions. Administrators configure the TOE with the Management Console via Web-based connection.

3.2 Security Audit

The TOE supports the provision of log data from each system component, such as user login/logout and incident/ticket management actions. It also records security events such as failed login attempts, etc. Audit trails can be stored for later review and analysis.

3.3 Cryptographic Support

The TOE trusted channels and inter-TOE communications are protected by HTTPS/TLS v1.2.

3.4 Identification and Authentication

The TOE enforces individual I&A. Operators must successfully authenticate using a unique identifier and password prior to performing any actions on the TOE.

3.5 Protection of the TSF

Inter-TSF basic TSF data consistency requires that passwords are protected.

3.6 User Data Protection

The TOE enforces discretionary access rules using an access control list with user attributes.

3.7 Trusted Channel/Path

The TOE utilizes HTTPS/TLS to provide trusted paths and inter-TSF trusted channels.

4 Assumptions and Clarification of Scope

4.1 Assumptions

The Security Target [ST] makes six assumptions on the usage and the operational environment 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 or hostile.

A.LOCATE

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

A.TIMESOURCE

The environment provides the TOE with a reliable timestamp.

A.ENV_PROT

The environment provides security domains for TOE execution.

A.CRYPTO

The environment provides cryptography used by the TOE.

4.2 Clarification of Scope

The Security Target contains four 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.PROT_TRANS

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

The Security Target contains one Organisational Security Policy (OSP).

P.REMOTE_DATA

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

5 Architectural Information

The TOE is software only, the hardware and operating systems the TOE run on are part of the operational environment. The TOE in its evaluated configuration consists of the following components:

Identity Manager (engine) v4.9.0.0000

- Identity Vault v4.9.0.0000
- ID Console v1.7.2.0000

Identity Applications (RBPM) v4.9.0.0000

- Identity Manager Designer v4.9.0.0000
- Identity Manager Analyzer v4.9.0.0000

Identity Reporting Module

- NetIQ Identity Reporting v7.2.0000

Log Manager

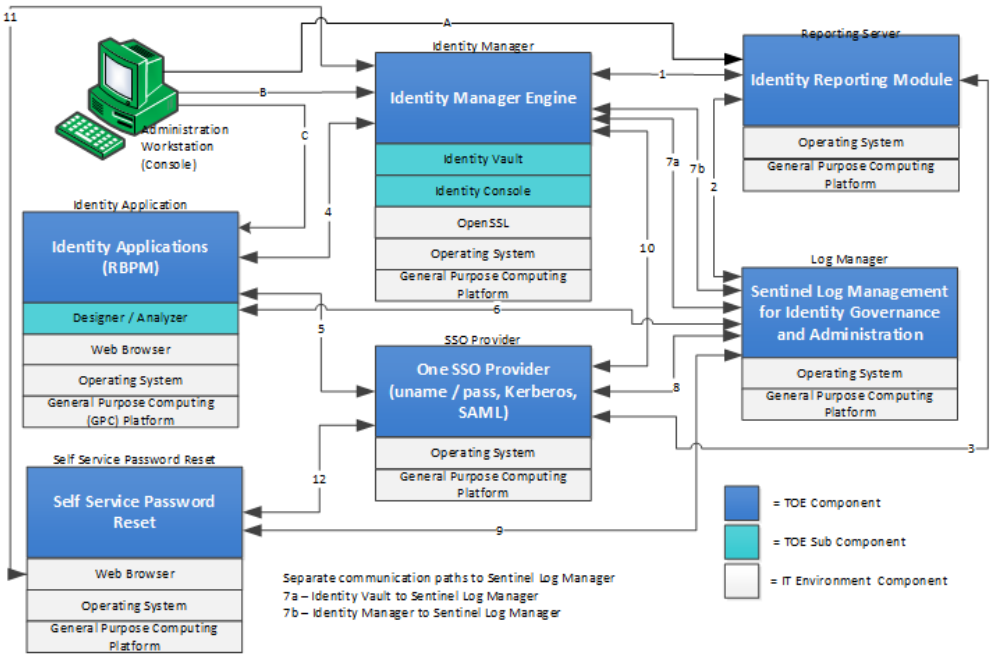
- Sentinel Log Management for Identity Governance and Administration v8.6.1.0000

SSO Provider

- One SSO Provider (OSP) v6.7.0.0000

Self Service Password Reset

- Self Service Password Reset (SSPR) v4.7.0.2



Note that the Administration Workstation is required in the evaluated configuration, but is considered part of the environment.

The Security Target section 1.8 contains more detailed descriptions of the components of the TOE.

6 Documentation

The TOE includes the following guidance documentation:

Identity Manager 4.9 Release Notes

Quick Start Guide for Installing NetIQ Identity Manager 4.9

Quick Start Guide for Installing or Upgrading NetIQ Identity Manager 4.9 Standard Edition

NetIQ Identity Manager Overview and Planning Guide

NetIQ Identity Manager Install and Upgrade Guide for Linux

NetIQ Identity Manager Install and Upgrade Guide for Windows

NetIQ Identity Manager Administrator's Guide to the Identity Applications

NetIQ Identity Manager User's Guide to the Identity Applications

NetIQ Identity Manager Administrator's Guide for Drivers

NetIQ Identity Manager Understanding Designer Concepts

NetIQ Identity Manager Jobs Guide

NetIQ Identity Manager E-mail Notification Guide

NetIQ Identity Manager Administrator's Guide to Configure Auditing

NetIQ Identity Manager Security Guide

The documentation is available for download from the download portal:
https://sld.microfocus.com/mysoftware/download/downloadCenter
in the form of a gnu zip file (.gz), or an iso formatted optical disk (.iso).

7 IT Product Testing

7.1 Developer Testing

The developer’s testing covers the most of the security functional behaviour of the TSFIs and nearly all SFR functionality. Developer testing was performed at the developer's site in Bangalore, India. All test results were as expected.

7.2 Evaluator Testing

The evaluator performed the installation and configuration of the TOE into the evaluated configuration, repeated a majority of the developer tests, and added a number of complementary tests to make the SFR coverage complete. The evaluator testing was performed at the evalator's site in Bromma. All test results were as expected.

7.3 Penetration Testing

The evaluator performed (NMAP) port scans, and (Nessus) vulnerability scans.

The penetration testing was performed at the evalator's site in Bromma.

No anomalities or vulnerabilities were discovered.

8 Evaluated Configuration

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

Identity Manager (engine) v4.9.0.0000
- Identity Vault v4.9.0.0000
- ID Console v1.7.2.0000

Identity Applications (RBPM) v4.9.0.0000
- Identity Manager Designer v4.9.0.0000
- Identity Manager Analyzer v4.9.0.0000

Identity Reporting Module
- NetIQ Identity Reporting v7.2.0000

Log Manager
- Sentinel Log Management for Identity Governance and Administration v8.6.1.0000

SSO Provider
- One SSO Provider (OSP) v6.7.0.0000

Self Service Password Reset
- Self Service Password Reset (SSPR) v4.7.0.2

Required IT equipment in the environment:

Administration Workstation	Mozilla 65
Operating system	SUSE Linux Enterprise Server 15 SP5
Crypto module	OpenSSL v2.0.10

During the evaluation, the TOE components were tested as virtual machines, including SUSE Linux Enterprise Server 15 SP5, running on ESXi version 7.0.3.
Instead of on a hypervisor the TOE components and the operating system can also be installed directly on hardware.

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 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.3	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 Analysis	AVA	PASS
Vulnerability Analysis	AVA_VAN.2	PASS

10 Evaluator Comments and Recommendations

None.

11 Acronyms

CC	Common Criteria for Information Technology Security
CEM	Common Methodology for Information Technology Security, document describing the methodology used in Common Criteria evaluations
CLI	Command Line Interface
EAL	Evaluation Assurance Level
IDM	Identity Manager
ITSEF	IT Security Evaluation Facility, test laboratory licensed to operate within a evaluation and certification scheme
NLA	Network Level Authentication
OSP	Organisational Security Policy
RDP	Remote Desktop Protocol
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target, document containing security requirements and specifications, used as the basis of a TOE evaluation
TOE	Target of Evaluation
TSF	TOE Security Functionality

12 Bibliography

ST	NetIQ Identity Manager 4.9.0 Security Target, OpenText Corporation, 2025-01-16, document version 0.14.
RN	Identity Manager 4.9 Release Notes, OpenText, May 2024, FMV ID 23FMV2873-23
QSIM	Quick Start Guide for Installing NetIQ Identity Manager 4.9, OpenText, May 2024, FMV ID 23FMV2873-23
QSSE	Quick Start Guide for Installing or Upgrading NetIQ Identity Manager 4.9 Standard Edition, OpenText, May 2024, FMV ID 23FMV2873-23
OPG	NetIQ Identity Manager Overview and Planning Guide, OpenText, May 2024, FMV ID 23FMV2873-23
SUL	NetIQ® Identity Manager Install and Upgrade Guide for Linux, OpenText, May 2024, FMV ID 23FMV2873-23
SUW	NetIQ® Identity Manager Install and Upgrade Guide for Windows, OpenText, May 2024, FMV ID 23FMV2873-23
ADMIA	NetIQ® Identity Manager Administrator’s Guide to the Identity Applications, OpenText, April 2024, FMV ID 23FMV2873-23
UG	NetIQ® Identity Manager User’s Guide to the Identity Applications, OpenText, May 2024, FMV ID 23FMV2873-23
DG	NetIQ Identity Manager Administrator’s Guide for Drivers, OpenText, May 2024, FMV ID 23FMV2873-23
DES	NetIQ Identity Manager Understanding Designer Concepts, OpenText, May 2024, FMV ID 23FMV2873-23
JOB	NetIQ Identity Manager Jobs Guide, OpenText, May 2024, FMV ID 23FMV2873-23
MAIL	NetIQ Identity Manager E-mail Notification Guide, OpenText, May 2024, FMV ID 23FMV2873-23

ACA	NetIQ® Identity Manager Administrator's Guide to Configure Auditing, OpenText, October 2019, FMV ID 23FMV2873-29
IMSG	NetIQ® Identity Manager Security Guide, OpenText, May 2024, FMV ID 23FMV2873-23
CC/CEM	Common Criteria for Information Technology Security Evaluation, and Common Methodology for Information Technology Security Evaluation, CCMB-2017-04, 001 through 004, document version 3.1 revision 5

Appendix A Scheme Versions

A.1 Scheme/Quality Management System

During the certification the following versions of the Swedish Common Criteria Evaluation and Certification scheme have been applicable since the certification application was registered 2023-05-24:

Version	Introduced	Impact of changes
2.6	2025-04-23	No impact
2.5.2	2024-06-14	No impact
2.5.1	2024-02-29	No impact
2.5	2024-01-25	No impact
2.4.1	2023-09-14	No impact
2.4	2023-06-15	No impact
2.3.1	Application	

A.2 Scheme Notes

Scheme Notes applicable to the certification:

Scheme Note	Version	Title	Applicability
SN-15	5.0	Testing	Compliant
SN-18	4.0	Highlighted Requirements on the Security Target	Compliant
SN-22	4.0	Vulnerability Assessment	Compliant
SN-27	1.0	ST Requirements at the Time of Application for Certification	Compliant
SN-28	2.0	Updated Procedures for Application, Evaluation and Certification	Compliant