Swedish Certification Body for IT Security

Certification Report

NetIQ Group Policy Administrator 6.9.4

Issue: 1.0, 2025-apr-24

Authorisation: Jerry Johansson, Lead certifier , CSEC

Table of Contents

1 Executive Summary

The TOE is the software part of the Group Policy Administrator 6.9.4 subsystems:

- NetIQ Group Policy Administrator Server
- NetIQ Group Policy Administrator Console

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

The TOE type is a Windows Management Policy Proxy (WMP).

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 Privileged Access Manager 4.5. The TOE relies on these being met to counter the twelve threats (no organisational security policies) 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 Växjö and Bromma, Sweden.

The evaluation was completed in 2025-03-11. 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 2, 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 2 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.

2 Identification

Certification Identification	
Certification ID	CSEC2023011
Name and version of the certified IT product	NetIQ Group Policy Administrator 6.9.4
Security Target Identification	NetIQ Group Policy Administrator 6.9.4 Security Target
EAL	EAL 2 + 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	2025–04–24

3 Security Policy

The TOE provides the following security services:

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management

3.1 Security Audit

The TOE can be set up to produce detailed audit reports for events and to aid in their analysis via the use of the Console Subsystem. The TOE reporting capabilities are completely configurable.

3.2 User Data Protection

The TOE implements multiple levels of access as well as functions to enforce them. In addition, the transactions are authenticated, and exportable. Data can be imported and exported from the TOE as well as moved across different components in the TOE. In addition, residual data created by the TOE is cleaned up. Inter-TSF data confidentiality transfers are protected by use of the Operating Environments native communications process.

3.3 Identification and Authentication

Users of the TOE depend on the IT Environment to handle initial access authentication. However, errors and transactions are logged by the TOE. While the TOE depends on the IT Environment for protection of passwords and service credentials (via file protections and access controls), the subject binding is enabled at the SQL Server and the GPA Server.

The subject binding allows the TOE to provide privileges (or groups of privileges) for individuals or groups of individuals.

3.4 Security Management

Security functions and attributes in the TOE are controlled / managed and specified at different levels or roles by the TSF and the IT Environment. The TOE and IT Environment can also be used to revoke individual access.

4 Assumptions and Clarification of Scope

4.1 Assumptions

The Security Target [ST] makes seven assumptions on the usage and the operational environment of the TOE.

A.LOCATE

The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

A.MANAGE

There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

A.NOEVIL

The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

A.AVAIL

The systems, networks and all components will be available for use.

A.CONFIG

The systems will be configured to allow for proper usage of the application.

A.TIME

The environment will provide a reliable time source for the TOE.

A.DOMAIN

The environment will provide a secure domain for execution for the TOE.

4.2 Clarification of Scope

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

T.ADMIN_ERROR

An authorized administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.

T.AUDIT

An unauthorized user may compromise the audit records so events are not associated with a user.

T.MASQUERADE

An unauthorized user, process, or external IT entity may masquerade as an authorized entity to gain access to TOE data or TOE resources.

T.NO_HALT

An authorized administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms. An.unauthorized entity may attempt to compromise the continuity of the TOE by halting execution of the TOE or TOE Components.

T.PRIV

An unauthorized entity may gain access to the TOE and exploit functionality to gain access or privileges to TOE security functions and data.

T.MAL_INTENT

An authorized user could initiate changes that grant themselves additional unauthorized privileges.

T.TSF_COMPROMISE

A malicious user may cause configuration data to be inappropriately accessed (viewed, modified or deleted).

T.MAL_ACT

Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.

T.MIS_NORULE

Unauthorized accesses and activity, indicative of misuse, may occur on an IT System the TOE is installed on and the TOE response may not occur if no event rules are specified in the TOE.

T.SC_MISCFG

Improper security configuration settings may exist in the IT System the TOE is on and could make the TOE audit ineffective.

T.SC_MALRUN

Users could execute malicious code on an IT System that the TOE is installed on which causes modification of the TOE protected data or undermines the IT System security functions.

T.SC_NVUL

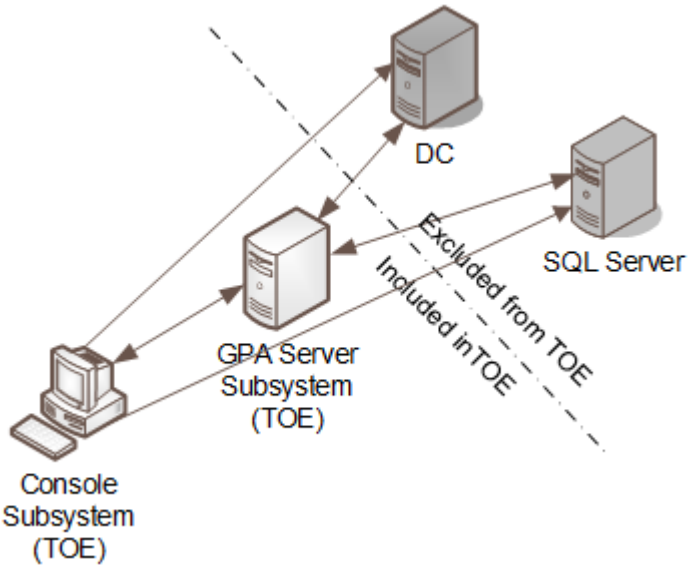
Vulnerabilities may exist in the IT System the TOE is installed on which causes the TOE to be compromised.

The Security Target does not contain any Organisational Security Policies (OSPs).

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 parts:

- NetIQ Group Policy Administrator Server Subsystem v6.9.4
- Console Subsystem v6.9.4



For the purpose of this certification includes:

The NetIQ Group Policy Administrator Server Subsystem enables the extension and management of Microsoft Group Policies. GPA extends GPA management capability to individuals while:

- Protecting Group Policy Objects (GPO) consistency
- Providing improved audit capability

The NetIQ Group Policy Administrator Console Subsystem includes the following functionality:

- Enables / disables group policies
- Allows you to edit Group Policy Objects(GPO) Offline
- Enables access to versions
- Provides notification of changes
- Enables workflows

6 Documentation

The TOE includes the following guidance documentation:

NetIQ GPA 6.9.4

Group Policy Administrator User Guide

7 IT Product Testing

7.1 Developer Testing

The developer's testing covers the security functional behaviour of all TSFIs and nearly all SFRs, on TOE version 6.9.4. 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 most developer tests, and performed a few complementary tests. The evaluator tested TOE version 6.9.4. All test results were as expected.

7.3 Penetration Testing

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

No anomalities or vulnerabilities were discovered.

8 Evaluated Configuration

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

The TOE subsystems were tested on the following OS platforms:

GPA Server Subsystem v6.9.3.1:	Windows Server 2019
GPA Server Subsystem v6.9.4:	Windows Server 2019
Console Subsystem v6.9.3.1:	Windows Server 2019
Console Subsystem v6.9.4:	Windows Server 2019

Supporting IT equipment in the environment:

Domain Controller

SQL Server

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.2	PASS
TOE Design	ADV_TDS.1	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.2	PASS
CM Scope	ALC_CMS.2	PASS
Delivery	ALC_DEL.1	PASS
Flaw Remediation	ALC_FLR.3	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.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
ITSEF	IT Security Evaluation Facility, test laboratory licensed to operate within a evaluation and certification scheme
NLA	Network Level Authentication
PAM	Privileged Access manager
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
WMP	Windows Management Policy Proxy

12 Bibliography

ST	NetIQ Group Policy Administrator 6.9.4 Security Target, OpenText, 2024-11-13 document version 0.10
AGD	NetIQ GPA 3.9.4, OpenText, 2024 Nov 8, document version 0.4
USER	Group Policy Administrator User Guide, OpenText, October 2023
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 2023-08-31:

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	Application	Original version

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