Swedish Certification Body for IT Security

Certification Report NetIQ Directory Resource Administrator 10.2.3

Issue: 1.0, 2025-maj-08

Authorisation: Jerry Johansson, Lead certifier , CSEC

Table of Contents

1 Executive Summary

The TOE is the software part of the NetIQ Directory Resource Administrator 10.2.3.0.2175 subsystems:

- DRA Server Subsystem
- Console Subsystem

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

The TOE type is a Windows Management Administrative Proxy (WMAP).

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

There are ten assumptions made in the ST regarding the secure usage and environment of the NetIQ Directory Resource Administrator 10.2.3. The TOE relies on these being met to counter the eleven 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 Bromma, Sweden.

The evaluation was completed in 2025-03-28. 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	CSEC2024002
Name and version of the certified IT product	NetIQ Directory Resource Administrator v.10.2.3.0.2175
Security Target Identification	NetIQ Directory and Resource Administrator 10.2.3 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	2025–05–08

3 Security Policy

The TOE provides the following security services:

- Security Audit
- User Data Protection
- Cryptographic Support
- Identification and Authentication
- Security Management
- Windows Management Administrative Proxy Functions
- Trusted Channel/Path

3.1 Security Audit

The TOE provides a capability to audit changes to the Active Directory made through the NetIQ Directory Resource Administrator application. As well as generating audit logs for regular events, the TOE generates audit records for security relevant events. All audit logs are stored. The TOE allows authorized users (administrators) to view these logs.

If a security event occurs, the TOE blocks the source of the event but also logs it. Logs can be reviewed and analyzed. From this, the administrator can formulate a response for these events.

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. The TOE can also be configured to control where functionality can be accessed.

3.3 Cryptographic Support

The TOE leverages encryption as provided by the Operating Environment in the default communication products.

3.4 Identification and Authentication

Users of the TOE depend on the IT Environment to handle access authentication, however, all errors and transactions are logged by the TOE. In addition, the TOE has multiple privileges for individuals or groups of individuals. The TOE depends on the IT Environment for protection of passwords and service credentials, as well as for user authentication, identification, subject binding.

3.5 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.

3.6 Windows Management Administrative Proxy Functions

The TOE also provides additional functions. The TOE will provide authorized users with the ability to collect data, and generate reports in a manner suitable for the user to interpret. The TOE will generate alarms using various notification mechanisms. The TOE will react if the storage capacity has been reached.

3.7 Trusted Channel/Path

The TOE establishes trusted channels for communications between itself and the LDAP server. There is also a trusted path between the Console and the DRA Server.

4 Assumptions and Clarification of Scope

4.1 Assumptions

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

A.ACCESS

The TOE has access to all the IT System data it needs to perform its functions.

A.DYNMIC

The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.

A.ASCOPE

The TOE is appropriately scalable to the IT System the TOE monitors.

A.CRYPTO

The operational environment provides cryptography for the protection of communications.

A.LOCATE

The server components of 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.NETCON

All networks will allow for communications between the components.

4.2 Clarification of Scope

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

T.ADMIN_ERROR

An authorized administrator may incorrectly install or configure the TOE resulting in the exposure of data, applications, or capabilities. Improper installation can also affect the security mechanisms in the product for example access control and audit functions.

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 unauthorized entity may attempt to compromise the integrity of the TOE or assets the TOE controls through denying services provided by the TOE by halting the execution of the entire TOE or one of its 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 via the TOE that enable additional privileges as specified in Appendix A. These privileges may not have been authorized via appropriate channels.

T.TSF_COMPROMISE

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

T.MAL_ACT

A vulnerability in the IT system, on which the TOE is present, may allow for malicious activity, such as the introduction of malware (i.e. Trojan horses and viruses) by either an authorized entity or a vulnerability in the IT system. This may in turn lead to the compromise of the TOE.

T.MIS_NORULE

An unauthorized user, performing an unauthorized activity, indicative of misuse, may occur on an IT System the TOE is installed on. If no event rules are specified in the TOE to cover the action, then the TOE may not issue an alert or log entry.

T.SC_MISCFG

An administrator may improperly define the security configuration settings in the IT System the TOE is operating within. The lack of proper IT system configuration could make the TOE security features, such as access control or audit features, 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.SENSDATA

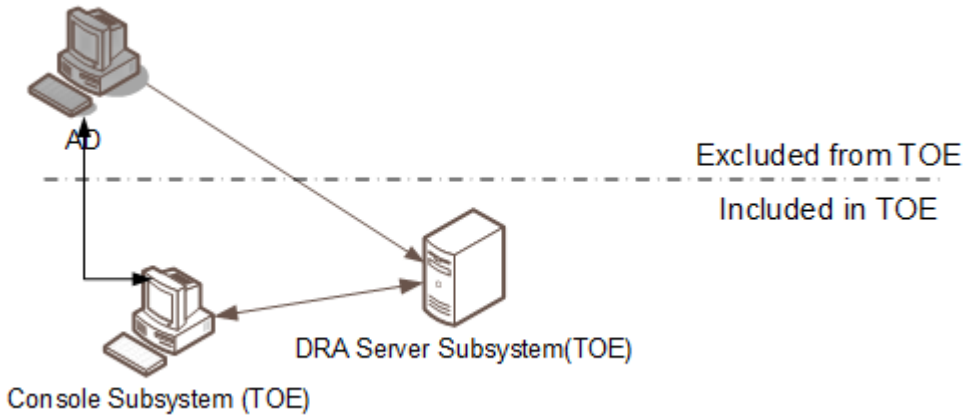
An unauthorized user can observe or modify data in transit between TOE components which causes a security exposure.

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:

- Console Subsystem v. 10.2.3
- DRA Server Subsystem v.10.2.3



For the purpose of this certification, the TOE includes:

The Console Subsystem which includes the following functionality:

- Delegation and Configuration Console – Provides a mechanism to securely delegate administrative tasks in the managed domain, set policies and automation triggers, and configure the Administration server.
- Directory and Resource Reporting – Provides a mechanism to view and print administration activity reports. This enables auditing of your enterprise security and track administration activities.
- Web Console – Part Provides a mechanism for Administrators to view configurations in the TOE.

The DRA Server Subsystem which provides audit, authentication, authorization, management and communications functionality.

6 Documentation

The TOE includes the following guidance documentation:

NetIQ DRA 10.2.3 AGD, Operation User Guidance and Preparative Procedures

Directory and Resource Administrator 10.2.3 Administrator Guide

Directory and Resource Administrator 10.2.3 Installation Guide

Directory and Resource Administrator 10.2.3 User Guide

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 SFRs. 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. 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:

DRA Server Subsystem v10.2.3:	Windows Server 2016, and Windows Server 2016 on ESXi 7.0.3
Console Subsystem v10.2.3:	Windows Server 2016, and Windows Server 2016 on ESXi 7.0.3

Supporting IT equipment in the environment:
Active Directory Domain Controller

The following features are excluded from the evaluation:

- CLI
- REST API
- Email alarm
- Power shell
- ADSI Provider
- DRA Reporting Center Setup (NRC)
- SSH

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
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
WMAP	Windows Management Administrative Proxy

12 Bibliography

ST — NetIQ Directory and Resource Administrator 10.2.3, Security Target, OpenText Corporation, 2025-03-24, document version 1.14.

AGD — NetIQ DRA 10.2.3 AGD, Operation User Guidance and Preparative Procedures, OpenText,Corporation, 2024-12-16, document version 2.9

ADM — Directory and Resource Administrator 10.2.3 Administrator Guide, OpenText,Corporation, November 2023

IG — Directory and Resource Administrator 10.2.3 Installation Guide, OpenText,Corporation, November 2023.

UG — Directory and Resource Administrator 10.2.3 User Guide, OpenText Corporation, November 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 2024-02-15:

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	Application	No impact

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