Swedish Certification Body for IT Security

Certification Report

NetIQ Privileged Access Manager 4.5

Issue: 1.0, 2025-apr-10

Authorisation: Jerry Johansson, Lead certifier , CSEC

Accred. no. 1917
Certification of
Products
ISO/IEC 17065

Table of Contents

1 Executive Summary

The TOE is the software part of the Privileged Access Manager 4.5.0.0 components:

- Console (Administrator, PAM User, EndPoint User)
- PAM Manager.
- PAM Agent (AKA Server with Agent)

excluding the operating system and the crypto module Voltage Cryptographic Module v5.0 which are considered part of the environment.

The TOE provides the following functionality:

- control account data and reduce administrative overhead
- provide visibility into privileged user activity
- enable administrators to detect unauthorized user access to sensitive information
- control and monitoring of account (both privileged and non-privileged) access
- acting as an aggregator / consolidator for multiple system accounts including applications, databases, servers, and the cloud
- allowing delegation of privileges to users without exposing privileged account credentials
- enforce administrative access controls on system reports, components, audit logs, and configuration files for all users as well as users based on identity and roles

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

There are nine 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 three threats and the two 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 Alvik, Sweden.

The evaluation was completed in 2025-03-07. 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.

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.

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 the cryptographic primitives has been in the scope of this evaluation, while verification of the correctness of implementation of the cryptographic primitives been outside the scope of the evaluation.

2 Identification

Certification Identification	
Certification ID	CSEC2023014
Name and version of the certified IT product	NetIQ Privileged Access Manager 4.5.0.0
Security Target Identification	NetIQ Privileged Access Manager 4.5 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	2.5.2
Scheme Notes Release	22.0
Recognition Scope	CCRA, SOGIS, EA/MLA
Certification date	2025–04–10

3 Security Policy

The TOE provides the following security services:

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

3.1 Security Audit

The TOE generates audit records for all requested operations. The audit records include elements such as the requestor, requested access, status of request, conditions imposed on the request. For agent environments, the TOE supports the ability to authenticate the individual or rely on a third party for authentication, validate and enable roles and authorizations, and record all transactions that occur while the privilege is being used or the user is active. The TOE records events such as unauthorized access attempts, or privileges. Audit trails are stored for later review and analysis.

3.2 Cryptographic Support

Cryptography for TLS connections is supplied by the Voltage Cryptographic Module v.5.0, which is implemented in the environment. The invocation by the TOE and the effect of the cryptographic functionality is within the scope of the evaluation.

3.3 User Data Protection

The TOE provides two levels of access to the Credential Vault. These are PAM administrator and PAM User (also referred to as System User and User). The Credentials stored in the vault are protected via user account authorizations and permissions.

3.4 Identification and Authentication

The TOE enforces individual I&A in conjunction with group/role based I&A mechanisms. PAM Administrators, system administrators, and users must successfully authenticate using a unique identifier and password prior to performing any actions on the TOE.

3.5 Security Management

The TOE provides administrators with the capabilities to configure, monitor and manage the TOE to fulfill the Security Objectives. Security Management principles relate to management of access control policies as well as control of roles associated with users. Administrators configure the TOE with the Console via a Web-based connection. The TOE provides an inactivity timeout mechanism which locks both the PAM Administrative console as well as for the End User Console. The TOE also provides a disconnect feature if a user attempts to execute unauthorized commands or facilities.

3.6 Protection of the TSF

The TOE protects the contents of the Credential Vault as well as the contents of the audit information from accidental disclosure.

3.7 TOE Access

The TOE terminates interactive sessions after an administrator configurable time. It also allows the user to terminate their own interactive sessions.

3.8 Trusted Path/Channels

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 nine assumptions on the usage and the operational environment of the TOE.

A.AUDIT_PROTECT

The Audit Data (which is used to store transaction logs, and track other audit events) is located within a Database and facility that provides physical and logical controlled access.

A.CDB_PROTECT

The Configuration Database, which contains the Roles and Rules, is located within a facility that provides physical and logical controlled access.

A.HTTPS

Web browsers used to access the TOE shall support HTTPS using TLS.

A.LOCATE

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

A.LOST_CRED

The TOE environment protects against lost or stolen credentials from exposure or compromise.

A.MANAGE

Privileged users (Administrators and PAM Users) of the TOE are assumed to be appropriately trained (and competent) to undertake the installation, configuration and management of the TOE in a secure and trusted manner.

A.NOEVIL

Privileged users (Administrators, PAM Users, and users) of the TOE, are not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the TOE documentation. Privileged Users (Administrators and PAM Users, and users) will not leave their systems unattended and unlocked.

A.TIMESOURCE

The TOE has a trusted source for system time via an NTP server.

A.UPDATE

The TOE, and the TOE environment are regularly updated by an administrator to address potential and actual vulnerabilities.

4.2 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 TOE configuration. The asset is the configuration of the TOE.

T.NO_PRIV

An authorized user of the TOE exceeds their assigned security privileges resulting in unauthorized modification of the TOE configuration and/or data. The assets are the:

- audit data that is collected
- configuration of the TOE
- privileges / rights / roles assigned to users
- stored credentials

T.SENSDATA

An unauthorized user may be able to view sensitive data passed between the TOE and its remote users, and between the TOE and external web servers, and exploit this data to gain unauthorized privileges on the TOE.

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

P.EVENTS

All PAM administrator, System Administrators, and user activities involving the TOE shall be monitored.

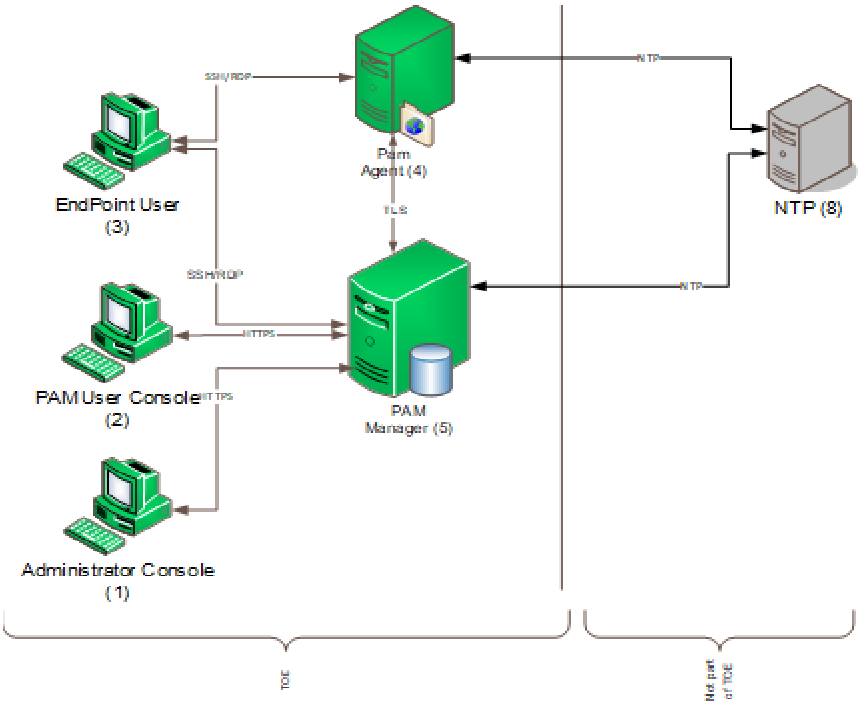
P.INCIDENTS

Activities representing potential issues should be managed to resolution. This enables the detection and potential prevention of harm to the TOE or the infrastructure the TOE is used to monitor and or protect.

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:

- Privileged Access Manager v4.5.0.0
- Console v4.5.0.0
- Agents v4.5.0.0



Privileged Access Manager

The PAM Manager is responsible for validating access requests against the rules database to determine access and authorization. The PAM Manager is also responsible for generating audit records and enabling their review as well as storing them in the database.

Console (EndPoint User , PAM User, and Administrator)

The Console is a web-based interface accessed through supported web browsers. The Console provides access to Administrator or PAM Users to provide functions based on user associated roles and rules. The Console serves three functions. First, to enable the configuration of the system (Administrator). Second is to allow for the review and output from the product (EndPoint User). Outputs include alerts (indicating anomalies) and reports indicating status and events. Lastly, the console enables commands to be forwarded to systems or applications for which PAM is controlling access (PAM User).

Agent

The PAM Agent forwards requests to the PAM Manager and either allows or rejects request as appropriate to the response from the PAM Manager. The PAM Agent is also responsible for creating operational recordings.

6 Documentation

The TOE includes the following guidance documentation:

Privileged Access Manager 24.3 (v4.5) Release Notes July 2024

Privileged Access Manager CE 24.2 (v4.5) Installation Guide July 2024

Privileged Access Manager CE 24.3 (v4.5) Administration Guide July 2024

Privileged Access Manager CE 24.2 (v4.5) User Guide July 2024

Privileged Access Manager CE 24.2 (v4.5) Security Guide June 2024

7 IT Product Testing

7.1 Developer Testing

The developer's testing covers the security functional behaviour of all TSFIs and 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 all developer tests, and performed a few 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:

PAM Console	Suse Linux Enterprise Server 15 SP4 64-bit
	Windows 10 64-bit
PAM Agent	Suse Linux Enterprise Server 15 SP4 64-bit
	Windows Server 2019 64-bit
PAM Manager	Suse Linux Enterprise Server 15 SP4 64-bit

All running on X86 64-bit Dual CPU servers.

Supported functionality Excluded from the Evaluated Configuration:

- While the product may use a Database to store information, it is not included in the evaluation
- PAM is not evaluated with RDP and NLA enabled.
- RDP with NLA and FIPS mode enabled are excluded from the evaluated configuration.
- Agentless server.
- PAM CLI

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

12 Bibliography

ST NetIQ Privileged Access Manager 4.5 Security Target, OpenText, 2024-07-30 document version 1.16

REL Privileged Access Manager 24.3 (v4.5) Release Notes, OpenText, July 2024

IG Privileged Access Manager CE 24.2 (v4.5) Installation Guide, Open Text, July 2024

AG Privileged Access Manager CE 24.3 (v4.5) Administration Guide, OpenText, July 2024

UG Privileged Access Manager CE 24.2 (v4.5) User Guide, OpenText, July 2024

SG Privileged Access Manager CE 24.2 (v4.5) Security Guide, OpenText, June 2024

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:

Version	Introduced	Impact of changes
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	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