Certification Report

OpenText Access Manager 5.1.2.0-95

Sponsor and developer: ***Open Text Corporation***
275 Frank Tompa Drive
Waterloo ON N2L 0A1
Canada

Evaluation facility: ***SGS Brightsight B.V.***
Brassersplein 2
2612 CT Delft
The Netherlands

Report number: **NSCIB-CC-2400081-01-CR**

Report version: **1.0**

Project number: **NSCIB-2400081-01**

Author(s): **Brian Smithson**

Date: **06 January 2026**

Number of pages: **10**

Number of appendices: **0**

CONTENTS

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TrustCB B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TrustCB B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TrustCB B.V. to perform Common Criteria evaluations; a significant requirement for such a licence is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TrustCB B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product or site satisfies the security requirements stated in the (site) security target.

Recognition of the Certificate

Presence of the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and will be recognised by the participating nations.

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see https://www.sogis.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the OpenText Access Manager 5.1.2.0-95. The developer of the OpenText Access Manager 5.1.2.0-95 is Open Text Corporation located in Waterloo ON, Canada and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The TOE is a software product which provides authorized users with intelligent access to secured applications and information based on who they are, what devices they are using and where they are located. Three components comprise the TOE: (1) Administration Console Server, (2) Identity Server, and (3) Access Gateway Service. The TOE and its components execute on general purpose computing hardware and software that are provided by the Operational Environment.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 2026-01-06 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the OpenText Access Manager 5.1.2.0-95, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the OpenText Access Manager 5.1.2.0-95 are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]* [1] for this product provide sufficient evidence that the TOE meets the EAL3: augmented (EAL3+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_FLR.3 (Systematic Flaw Remediation).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CC]* (Parts I, II and III).

TrustCB B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. Note that the certification results apply only to the specific version of the product as evaluated.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not available for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the OpenText Access Manager 5.1.2.0-95 from Open Text Corporation located in Waterloo ON, Canada.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	N/A	N/A
Software	Administration Console Server	5.1.2
	Identity Server	5.1.2
	Access Gateway Service	5.1.2

To ensure secure usage a set of guidance documents is provided, together with the OpenText Access Manager 5.1.2.0-95. For details, see section 2.5 “Documentation” of this report.

2.2 Security Policy

2.2.1 Security Audit

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

2.2.2 Identification & 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.

2.2.3 User Data Protection

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

2.2.4 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.

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

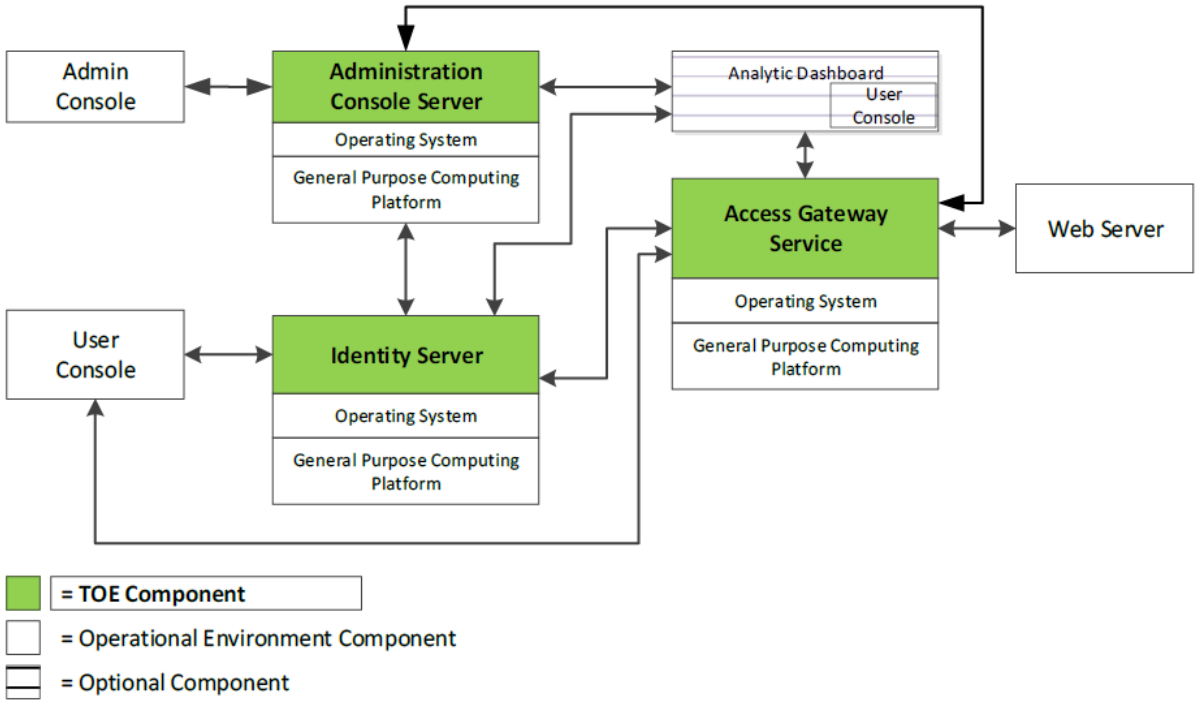
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 4.2 of the *[ST]*.

2.3.2 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

2.4 Architectural Information

The logical architecture, originating from the Security Target [ST] of the TOE can be depicted as follows:



2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Identifier	Version
OpenText Access Manager CE 24.2(v5.1), Administration Guide	May 2024
OpenText Access Manager CE 24.2 (v5.1), Installation and Upgrade Guide	May 2024
OpenText Access Manager System Requirements	May 2024
Access Manager CE 24.2 (v5.1) - Documentation | Micro Focus (online)	May 2024
Access Manager 5.1 Operational Guidance and Installation Procedures (AGD-IGS.1)	v0.11, 12-12-2025

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

The developer provided [ATE] evidence containing both test plan with expected test results and actual test results and the mapping. The developer has executed the tests in November 2024. All actual tests results are identical to the expected ones.

The repeated developer tests are chosen based on security relevancy and main functionality. Hence, the evaluator picked the tests about management such as managing correlation rules and asset protection such as audit record deletion prevention. Based on the picking criteria, evaluator sampled 7 test scenarios out of 18 sub-test cases.

The evaluator analysed the developer test plan against the SFRs and based on the completeness of the tests the evaluator test plan is devised. As a result of this, evaluator created 12 independent test scenarios in order to cover:

- AGD_PRE.1.2 requirements.
- Negative test cases, such as tests that a non-administrator user performs activities that need administrators' privileges.
- Communication related SFRs such as: IND03.Test TLS for communication between identity server and access gateway service, and IND04.Test TLS for communication between user console to identity server.
- Verify secure initialization.
- Nessus/NMAP scan.
- Verify TOE management functionalities

In total, 12 independent tests were devised.

2.6.2 Independent penetration testing

To identify potential vulnerabilities the evaluator performed the following activities:

SFR design analysis: SFR implementation details were examined in the SFR design analysis. During this examination potential vulnerabilities were identified.

CWE vulnerability focus: Using the CWE weaknesses collection, the evaluator collected a list of security questions and related answers. This approach ensured that the evaluator was forced to think in terms of vulnerabilities from all different angles and improved completeness in the vulnerability analysis. Also, during this examination several potential vulnerabilities were identified.

Use of Scanning tools: The evaluator runs vulnerability scanning tools to identify potential vulnerabilities

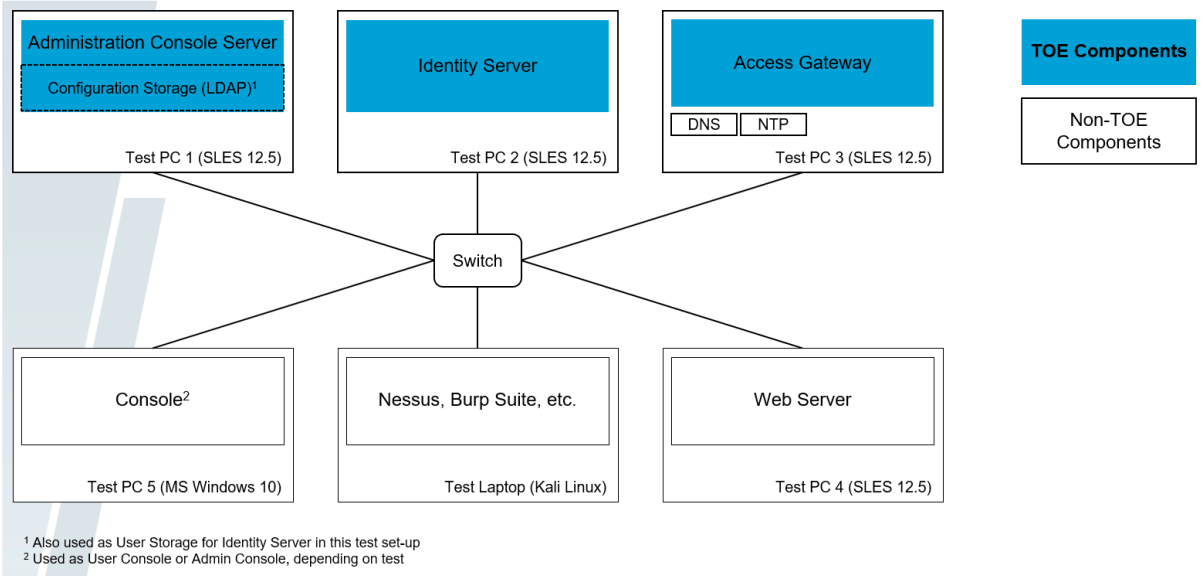
Public vulnerability search: Several additional potential vulnerabilities were identified during a search in the public domain.

In total, 7 penetration tests were devised. All were logical tests.

2.6.3 Test effort

The total test effort expended by the evaluators (for repeated, independent, and penetration tests) was 160 hours.

2.6.4 Test configuration



[1] Also used as User Storage for Identity Server in this test set-up
[2] Used as User Console or Admin Console, depending on test

2.6.5 Test results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

2.7 Reused Evaluation Results

There is no reuse of evaluation results in this certification.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number OpenText Access Manager 5.1.2.0-95.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents including Site Audit Checklists.

The verdict of each claimed assurance requirement is "**Pass**".

Based on the above evaluation results the evaluation lab concluded the OpenText Access Manager 5.1.2.0-95, to be **CC Part 2 conformant, CC Part 3 conformant**, and to meet the requirements of **EAL 3 augmented with ALC_FLR.3**.This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 "Documentation" contains necessary information about the usage of the TOE.

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself must be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. For the evolution of attack methods and techniques to be covered, the customer should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: <*none*>, which are out of scope as there are no security claims relating to these.

3 Security Target

The OpenText Access Manager 5.1.2 Security Target, v0.18, 2025-12-12 *[ST]* is included here by reference.

4 Definitions

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PP	Protection Profile
TOE	Target of Evaluation

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report.

[CC]	Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017
[ETR]	Evaluation Technical Report NetIQ Access Manager 5.1.2 – EAL3+, 24-RPT-1070, v2.0, 2025-12-22
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022
[ST]	OpenText Access Manager 5.1.2 Security Target, v0.18, 2025-12-12

(This is the end of this report.)