Communications Security Establishment | Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

COMMON CRITERIA CERTIFICATION REPORT

Oracle Access Management 12c

20 September 2023

572-LSS

Canada

FOREWORD

This certification report is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE).

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved testing laboratory established under the Canadian Centre for Cyber Security (a branch of CSE). This certification report, and its associated certificate, applies only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the Canadian Common Criteria Program, and the conclusions of the testing laboratory in the evaluation report are consistent with the evidence adduced.

This report, and its associated certificate, are not an endorsement of the IT product by Canadian Centre for Cyber Security, or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the Canadian Centre for Cyber Security, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

If your organization has identified a requirement for this certification report based on business needs and would like more detailed information, please contact:

Canadian Centre for Cyber Security
Contact Centre and Information Services
contact@cyber.gc.ca | 1-833-CYBER-88 (1-833-292-3788)

OVERVIEW

The Canadian Common Criteria Program provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Testing Laboratory (CCTL) under the oversight of the Certification Body, which is managed by the Canadian Centre for Cyber Security.

A CCTL is a commercial facility that has been approved by the Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of ISO/IEC 17025, the General Requirements for the Competence of Testing and Calibration Laboratories.

By awarding a Common Criteria certificate, the Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, the evaluated security functionality, and the testing and analysis conducted by the CCTL.

The certification report, certificate of product evaluation and security target are posted to the Common Criteria portal (the official website of the International Common Criteria Program).

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

Oracle Access Management 12c (hereafter referred to as the Target of Evaluation, or TOE), from **Oracle Corporation** , was the subject of this Common Criteria evaluation. A description of the TOE can be found in Section 1.2. The results of this evaluation demonstrate that the TOE meets the requirements of the conformance claim listed in Section 1.1 for the evaluated security functionality.

Lightship Security is the CCTL that conducted the evaluation. This evaluation was completed on **20 September 2023** and was carried out in accordance with the rules of the Canadian Common Criteria Program.

The scope of the evaluation is defined by the Security Target, which identifies assumptions made during the evaluation, the intended environment for the TOE, and the security functional/assurance requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations, and recommendations in this Certification Report.

The Canadian Centre for Cyber Security, as the Certification Body, declares that this evaluation meets all the conditions of the Arrangement on the Recognition of Common Criteria Certificates and that the product is listed on the Certified Products list (CPL) for the Canadian Common Criteria Program and the Common Criteria portal (the official website of the International Common Criteria Program).

1 IDENTIFICATION OF TARGET OF EVALUATION

The Target of Evaluation (TOE) is identified as follows:

Table 1: TOE Identification

TOE Name and Version	Oracle Access Management 12c
Developer	Oracle Corporation

1.1 COMMON CRITERIA CONFORMANCE

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5.

The TOE claims the following conformance:

Standard Protection Profile for Enterprise Security Management Policy Management Version 2.1, October 24, 2013

Standard Protection Profile for Enterprise Security Management Access Control Version 2.1, October 24, 2013

1.2 TOE DESCRIPTION

The TOE, Oracle Access Management (OAM), is an enterprise web access control and policy management solution. The TOE enforces administrator-configurable rules ensuring that organization's users given appropriate and consistent access to managed resource based on organizationally defined policy.

1.3 TOE ARCHITECTURE

The TOE, Oracle Access Management (OAM), is a distributed application software that consists of the following components:

- **OAM Server.** The Policy Decision Point. The OAM Server is deployed on an instance of Oracle WebLogic Server. The OAM Server retrieves policy data from the Policy Store, evaluates access requests from WebGates and responds with policy decisions for enforcement.
- **OAM Console.** The Policy Administration Point - a management Web GUI for configuration and policy definition. Deployed on a WebLogic Administration Server. The OAM Console is itself protected by a dedicated OAM WebGate. The OAM Console transmits policy data to the Policy Store.
- **OAM WebGate.** The Policy Enforcement Point(s) that intercept HTTP requests to enforce access decisions. OAM WebGate(s) are deployed on Oracle HTTP Servers (web server).

A diagram of the TOE architecture is as follows:

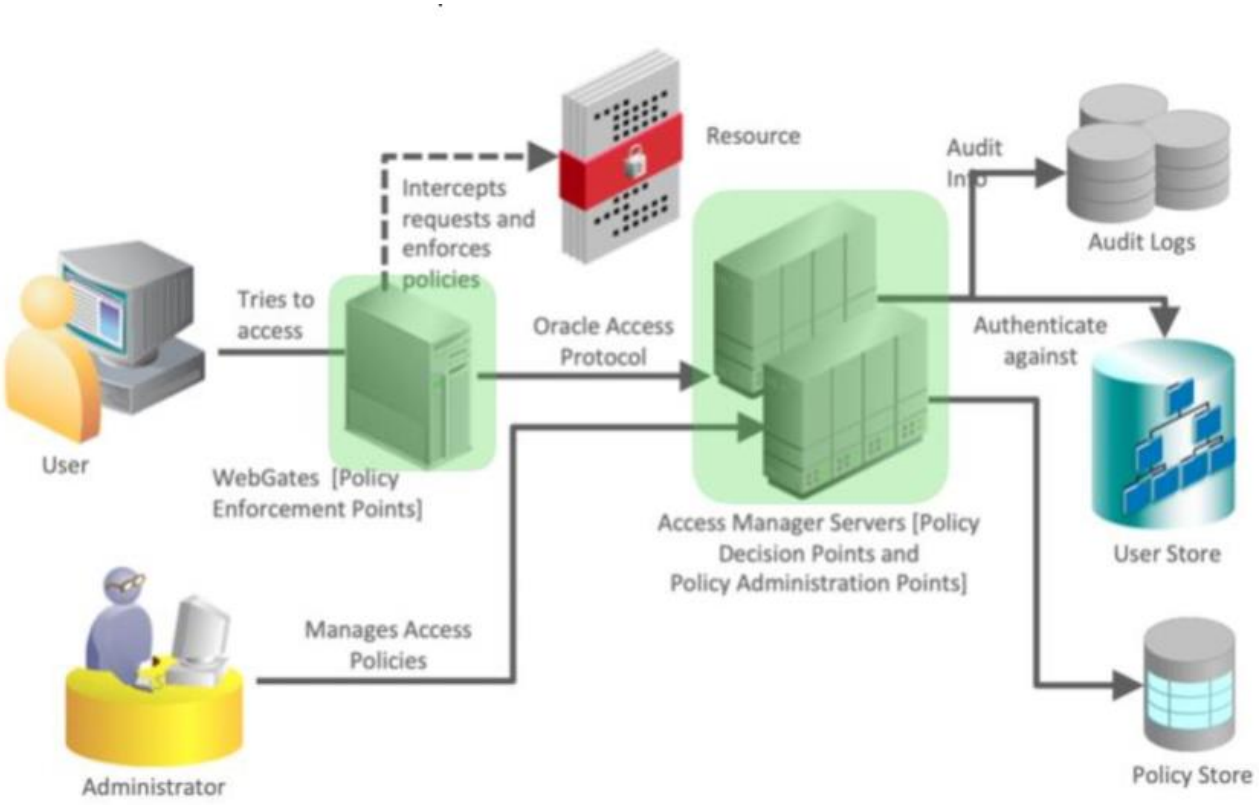

Figure 1: TOE Architecture

2 SECURITY POLICY

The TOE implements and enforces policies pertaining to the following security functionality:

- Access Control Policy Definition
- Access Control Policy Enforcement
- Policy Security
- Security Audit
- Secure Administration
- Continuity of Enforcement
- Cryptographic Support

Complete details of the security functional requirements (SFRs) can be found in the Security Target (ST) referenced in section 8.2.

2.1 CRYPTOGRAPHIC FUNCTIONALITY

The following cryptographic implementations are used by the TOE and have been evaluated by the CAVP:

Table 2: Cryptographic Implementation(s)

Cryptographic Module/Algorithm	Certificate Number
RSA BSAFE Crypto-C Micro Edition v4.1.2.2	C810
RSA BSAFE Crypto-J JSAFE and JCE Software Module v6.2.5	C652

Note: These CIs are provided by the operational environment (OE).

3 ASSUMPTIONS AND CLARIFICATION OF SCOPE

Consumers of the TOE should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will ensure the proper and secure operation of the TOE.

3.1 USAGE AND ENVIRONMENTAL ASSUMPTIONS

The following assumptions are made regarding the use and deployment of the TOE:

Enterprise Security Management Policy Management (PM)

- The TOE will use cryptographic primitives provided by the Operational Environment to perform cryptographic services.
- The TOE will be able to establish connectivity to other ESM products in order to share security data.
- There will be one or more competent individuals assigned to install, configure, and operate the TOE.
- The TOE will receive policy data from the Operational Environment.
- The Operational Environment will provide mechanisms to the TOE that reduce the ability for an attacker to impersonate a legitimate user during authentication.
- The TOE will receive reliable time data from the Operational Environment.
- The TOE will receive identity data from the Operational Environment.

Enterprise Security Management Access Control (AC)

- The TOE will use cryptographic primitives provided by the Operational Environment to perform cryptographic services.
- The TOE will be able to establish connectivity to other ESM products in order to share security data.
- The TOE will receive policy data from the Operational Environment.
- The Operational Environment will provide mechanisms to the TOE that reduce the ability for an attacker to impersonate a legitimate user during authentication.
- The TOE will receive reliable time data from the Operational Environment.
- The TOE will receive identity data from the Operational Environment.
- There will be a competent and trusted administrator who will follow the guidance provided in order to install the TOE.

3.2 CLARIFICATION OF SCOPE

The following functions are outside of the logical TOE scope and have not been evaluated:

- Deploying Oracle Access Management (OAM) on Cloud Infrastructure environment
- Oracle Access Management (OAM) domain deployment on Kubernetes or Docker environment

4 EVALUATED CONFIGURATION

The evaluated configuration for the TOE comprises:

TOE Software	Oracle Access Management 12.2.1.4 with patch 35371374
TOE Platform Requirements	OAM Server & Console • Oracle WebLogic Server 12c • Oracle Linux 7.6 UEK 5 • Oracle JRE 8 OAM WebGate 12.2.1.4.0 with patch 33974688 • Oracle HTTP Server 12c • Oracle Linux 7.6 UEK 5
Environmental Support	Audit Store – Oracle Database 19c Policy Store – Oracle Database 19c Identity Store – Oracle Unified Directory / Oracle Internet Directory 12c OAM Console Identity Store - LDAPv3 directory server

4.1 DOCUMENTATION

The following documents are provided (and also available for download) to assist the consumer in the configuration and installation of the TOE:

a) Oracle Access Management 12c Common Criteria Guide, v1.6 (PDF) - https://www.oracle.com/corporate/security-practices/assurance/development/external-security-evaluations/common-criteria/certifications.html

b) Oracle Access Management 12c Information Library - https://docs.oracle.com/en/middleware/idm/access-manager/12.2.1.4/aiaag/introducing-oracle-access-management.html

5 EVALUATION ANALYSIS ACTIVITIES

The evaluation analysis activities involved a structured evaluation of the TOE. Documentation and process dealing with Development, Guidance Documents, and Life-Cycle Support were evaluated.

5.1 DEVELOPMENT

The evaluators analyzed the documentation provided by the vendor; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces and how the TSF implements the security functional requirements. The evaluators determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained.

5.2 GUIDANCE DOCUMENTS

The evaluators examined the TOE preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance and determined that they are complete and sufficiently detailed to result in a secure configuration.

Section 4.1 provides details on the guidance documents.

5.3 LIFE-CYCLE SUPPORT

An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the TOE configuration items were clearly marked.

The evaluators examined the delivery documentation and determined that it described all the procedures required to maintain the integrity of the TOE during distribution to the consumer.

6 TESTING ACTIVITIES

Testing consists of the following three steps: assessing developer tests, performing independent tests, and performing a vulnerability analysis.

6.1 ASSESSMENT OF DEVELOPER TESTS

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the Evaluation Test Report (ETR). The correspondence between the tests identified in the developer's test documentation and the functional specification was complete.

6.2 CONDUCT OF TESTING

The TOE was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

6.3 INDEPENDENT TESTING

During this evaluation, the evaluator developed independent functional & penetration tests by examining design and guidance documentation.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The following testing activities were performed:

a. PP Assurance Activities: The evaluator performed the assurance activities listed in the claimed PP

b. Cryptographic Implementation Verification: The evaluator verified that the claimed cryptographic implementations were present in the OE.

6.3.1 INDEPENDENT TESTING RESULTS

The developer's tests and the independent tests yielded the expected results, providing assurance that the TOE behaves as specified in its ST and functional specification.

6.4 VULNERABILITY ANALYSIS

The vulnerability analysis focused on 4 flaw hypotheses.

- Public Vulnerability based (Type 1)
- Technical community sources (Type 2)
- Evaluation team generated (Type 3)
- Tool Generated (Type 4)

The evaluators conducted an independent review of all evaluation evidence, public domain vulnerability databases and technical community sources (Type 1 & 2). Additionally, the evaluators used automated vulnerability scanning tools to discover potential network, platform, and application layer vulnerabilities (Type 4). Based upon this review, the evaluators formulated flaw hypotheses (Type 3), which they used in their vulnerability analysis.

Type 1 & 2 searches were conducted on **31 May 2023** and included the following search terms:

Oracle OAM version 12c	ASM 6.0	Mina 2.0.19
Oracle WebGate 12c	Commons Codec 1.13	Jettison 1.4.0
Oracle Weblogic 12c	Commons Validator 1.6	Jython 2.7.1
Geronimo-stax-api 1.0.1	Jackson-Core-ASL 1.9.13	Commons FileUpload 1.4
Felix 4.4.0	jackson-jaxrs 1.9.13	Commons Beanutils 1.9.4
Commons Logging 2.17.1	jackson-mapper-asl 2.10.2	jackson-core 2.9.9
Bean Validation API 1.1.0.Final	jackson-xc 1.9.13	jackson-databind 2.10.2
ini4j 0.5.5	Higgins Framework T1-0-1	HttpComponents HttpClient 4.5.10
Zip4j 1.3.2	ZXing 3.3.0	HttpCore 4.4.10
Jose4j 0.5.5	Simple Logging Façade for Java (SLF4J) 1.7.28	jackson-annotations 2.9.9

Vulnerability searches were conducted using the following sources:

Oracle Critical Patch Updates, Security Alerts and Bulletins https://www.oracle.com/security-alerts/	Open Source Vulnerability Database https://security.snyk.io/
Apache bug reporting sites a) https://logging.apache.org/ b) https://issues.apache.org/jira/issues/ c) https://hc.apache.org/httpcomponents-core-4.4.x	Offensive Security Exploit Database https://www.exploit-db.com/

NIST National Vulnerabilities Database https://web.nvd.nist.gov/view/vuln/search	

6.4.1 VULNERABILITY ANALYSIS RESULTS

The vulnerability analysis did not uncover any security relevant residual exploitable vulnerabilities in the intended operating environment.

7 RESULTS OF THE EVALUATION

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved testing laboratory established under the Canadian Centre for Cyber Security. This certification report, and its associated certificate, apply only to the specific version and release of the product in its evaluated configuration.

This evaluation has provided the basis for the conformance claim documented in Table 1. The overall verdict for this evaluation is **PASS**. These results are supported by evidence in the ETR.

7.1 RECOMMENDATIONS/COMMENTS

It is recommended that all guidance outlined in Section 4.1 be followed to configure the TOE in the evaluated configuration.

The CCTL also recommends:

The TOE is a complicated piece of software with many dependent pieces of software. The online guidance for the TOE is extensive and allows for a clear understanding of the TOE and how it interacts with the operational environment. The evaluator recommends that administrators review the online guide in depth prior to deploying the TOE, and make use of the developer provided support extensively. This includes the Oracle Online Guidance "Administering Oracle Access Management" Appendix B which includes the steps to generate certificates, enable FIPS mode and configure the TLS channels.

8 SUPPORTING CONTENT

8.1 LIST OF ABBREVIATIONS

Term	Definition
CAVP	Cryptographic Algorithm Validation Program
CCTL	Common Criteria Testing Laboratory
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITS	Information Technology Security
PP	Protection Profile
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

8.2 REFERENCES

Reference
Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.
Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 5, April 2017.
Oracle Access Management 12c Security Target, Version 2.0, 19 September 2023
Oracle Access Management 12c Evaluation Technical Report, Version 1.1 , 20 September 2023
Oracle Access Management 12c Assurance Activity Report, Version 1.0, 20 September 2023