TLP:WHITE

Communications Security Establishment | Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

COMMON CRITERIA CERTIFICATION REPORT

Oracle Identity Governance 12c

9 October 2024

604-LSS

V1.0

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 Identity Governance 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 **9 October 2024** 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 Identity Governance 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 Identity and Credential Management Version 2.1, October 24, 2013

1.2 TOE DESCRIPTION

The TOE is an enterprise identity and credential management solution. The primary functionality of the TOE is to maintain the identity and credential lifecycle for organizational users. The TSF can define and maintain the organizational attributes of users, enroll and unenroll users, and impose controls that ensure that their authentication credentials are sufficiently secure.

1.3 TOE ARCHITECTURE

The TOE, Oracle Identity Governance (OIG), is an application software that is installed on top of the WebLogic Server and the connectors that are used to provision endpoint systems.

The TOE consists of the following components in the evaluated configuration:

- **Application Logic.** A component that runs on the environmental WebLogic server and is responsible for all back end TSF behavior.
- **Connectors.** Components that translate the TSF's application logic into configuration instructions that can be interpreted by endpoint systems.
- **Web GUI.** A component that runs on the environmental WebLogic server and is responsible for providing a visual administrative interface.

A diagram of the TOE architecture is as follows:

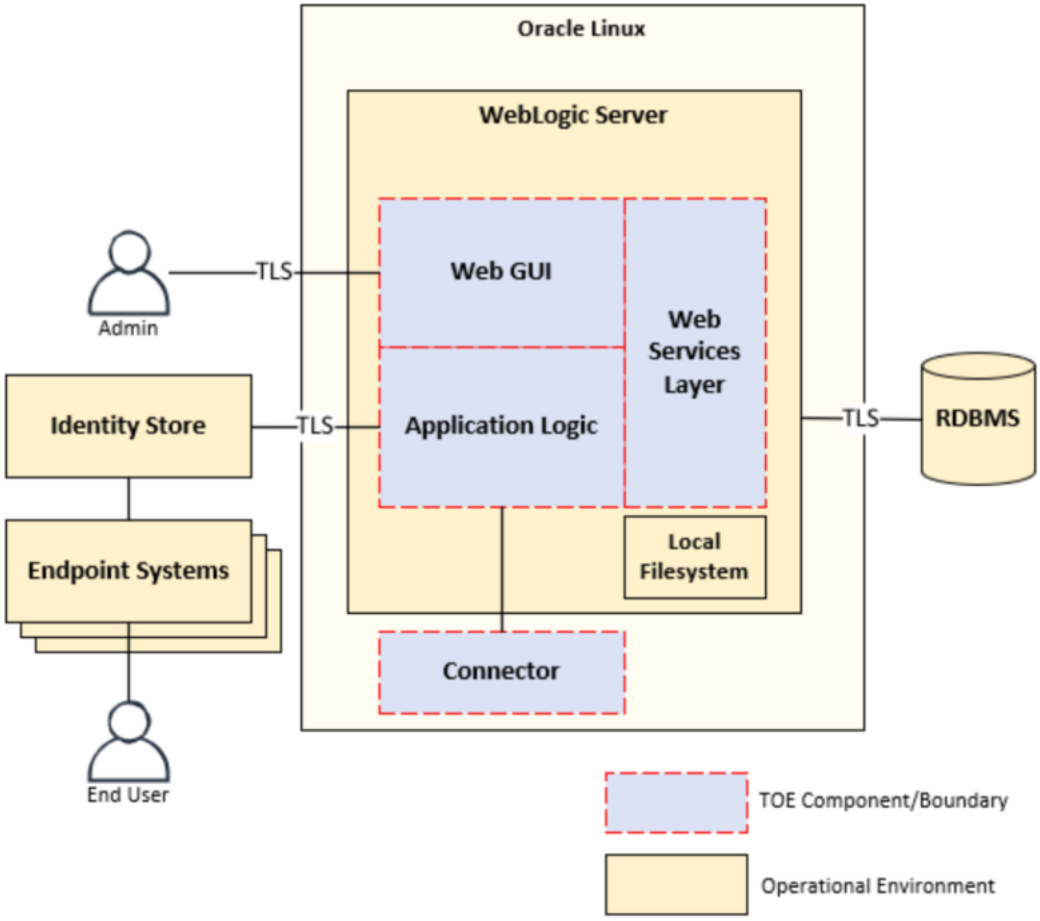

Figure 1: TOE Architecture

2 SECURITY POLICY

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

- Enterprise Security Management
- Security Audit
- Identification and Authentication
- Security Management
- Protection of the TSF
- Trusted Path/Channels

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 TOE uses a cryptographic module in the Operating Environment.

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:

- The TOE will use cryptographic primitives provided by the Operational Environment to perform cryptographic services.
- There will be a defined enrollment process that confirms user identity before the assignment of credentials.
- The TOE will be able to establish connectivity to other ESM products in order to share security data.
- Third-party entities that exchange attribute data with the TOE are assumed to be trusted.
- There will be one or more competent individuals assigned to install, configure, and operate the TOE.
- 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.

3.2 CLARIFICATION OF SCOPE

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

- Oracle Access Manager (OAM) - Authentication/authorization application that governs access to the TOE's administrative interface.
- SMTP Server - Email server used to send notifications and self-service data to administrators and end users.
- OIG Design Console - A local server application that is used to set initial configuration parameters for OIG that are not pertinent to the security functionality of the TOE.
- Other Connectors – The TOE supports many connectors. Only the OID connector was evaluated.

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

- SPML – The Services Provisioning Markup Language (SPML) Interface may be used to manage the TOE. It is disabled by default and requires configuration prior to use. The SPML Interface was not configured, used or tested in the evaluated configuration.

4 EVALUATED CONFIGURATION

The evaluated configuration for the TOE comprises:

TOE Software/Firmware	Oracle Identity Governance 12c, Build 12.2.1.4, with patches 36822804, 36770738, 36553894, 1221422, 36805124, and 36513778
TOE Platform Requirements	• Oracle WebLogic Server 12.2.1.4.0 • Oracle Linux 8.4 UEK 5 • jdk 1.8.0_421
Environmental Support	Database Server - Oracle Database 19c Identity Store - Oracle Unified Directory / Oracle Internet Directory 12c

4.1 DOCUMENTATION

The following documents are provided to the consumer to assist in the configuration and installation of the TOE:

a) Oracle Identity Governance 12c Common Criteria Guide, v1.4 https://www.oracle.com/corporate/security-practices/assurance/development/external-security-evaluations/common-criteria/certifications.html

b) Oracle Fusion Middleware Administering Oracle Identity Governance, 12c (12.2.1.4.0) https://docs.oracle.com/en/middleware/idm/identity-governance/12.2.1.4/omadm/administering-oracle-identity-governance.pdf

c) Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance, 12c (12.2.1.4.0) https://docs.oracle.com/en/middleware/idm/identity-governance/12.2.1.4/omusg/performing-self-service-tasks-oracle-identity-governance.pdf

d) Oracle Fusion Middleware Help Topics for Oracle Identity Governance, 12c (12.2.1.4.0) https://docs.oracle.com/en/middleware/idm/identity-governance/12.2.1.4/omhlp/help-topics-oracle-identity-governance.pdf

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 operational user guidance and determined that it sufficiently and unambiguously describes how to use and administer the product. The TOE must be deployed by Oracle Support to ensure it is in the evaluated 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:

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

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 **2 October 2024** and included the following search terms:

Oracle Identity Governance	Ehcache	Jackson-module-jaxb-annotations
Oracle OIG	Quartz	Jackson-annotations
OIG	Javassit	Jackson-dataformat-xml
Oracle Identity Self Service	Commons FileUpload	Jackson-jars-xml-provider
Oracle Identity Management	Opencsv	Jackson-databind
Weblogic 12.2.1.4.0	JGroups	Commons validator
Dell BSafe Crypto-J v6.2.5	Ehcache-jgroupsreplication	Jackson-dataformat-yaml
Dell BSafe SSL-J v6.5	Reflections	Log4J
Commons Codec	Commons Lang3	OWASP Java Encoder
Commons Pool	Spring Framework v5.3.27	Jackson-datatype-joda
Commons Collections	Commons Logging	Commons Digester
Cglib	Jackson-jaxrs-base	Commons DBCP
Jettison	Jackson-core	OGNL
Oracle ASM	Jackson-jaxrs-json-provider	

Vulnerability searches were conducted using the following sources:

Oracle Critical Patch Updates, Security Alerts and Bulletins https://www.oracle.com/security-alerts/	CISA - Known Exploited Vulnerabilities Catalog: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
NIST National Vulnerabilities Database https://web.nvd.nist.gov/view/vuln/search	CCCS – Alerts and advisories: https://cyber.gc.ca/en/alerts-advisories

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 Section 1.1. 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 operate the TOE. The TOE must be deployed by Oracle Support to ensure it is in the evaluated configuration.

It is recommended that the TOE be supported by people trained explicitly on the product, with extensive experience with Oracle products in general.

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
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 Identity Governance 12c Security Target, Version 1.5, 3 October 2024
Oracle Corporation Oracle Identity Governance 12c Evaluation Technical Report, Version 0.9, 9 October 2024
Oracle Corporation Oracle Identity Governance 12c Assurance Activity Report, Version 0.8, 9 October 2024