Swedish Certification Body for IT Security

Certification Report - Oracle AI Database 26ai

Issue: 1.0, 2025-dec-17

Authorisation: Theodora Arvanitidis, Junior Certifier , CSEC

Table of Contents

1 Executive Summary

Oracle AI Database 26ai is a relational database management system (DBMS) from the Oracle Corporation. The system is built around a relational database framework in which data objects may be directly accessed by users, or an application front end, through structured query language (SQL). Oracle is a fully scalable, multitenant, relational database architecture typically used by global enterprises and governments to manage and process data across wide and local area networks. The security functionality in Oracle AI Database 26ai includes:

- Configurable audit capture.
- Fine-grained access controls on database objects. Discretionary Access Control (DAC) is based on object, schema, and system privileges, as well as roles. Fine-grained access control may be implemented to allow access based on the information itself. For example, a user may be granted access to their own human resources details, but not the details of the other users contained in the same tables.
- User identification and authentication. Users are identified and authenticated before access to database objects is allowed. On login, the user identity is associated with role and privilege information that is used to make access control decisions.
- Security management functionality. The security functionality associated with audit, access control, and user accounts are provided through the SQL command line interface (CLI).
- Consistent replication. The content of a database may be replicated to another server, with assurances that the consistency of the data is maintained. The TOE is a software only TOE.

Requirements corresponding to the evaluated configuration can be found in the ST, under section 1.6.4.

The physical scope of the TOE consists of the Oracle AI Database 26ai software in one of four configurations. The logical boundary of the TOE includes all interfaces and functions within the physical boundary and may be broken down by the security function classes.

Oracle Exadata platform ships with the Oracle Linux operating system installed on the servers.

This Security Target [ST10] claims exact conformance with the collaborative Protection Profile for Database Management Systems, 13 March 2023, Version 1.3 (cPP DBMS). The supporting document Evaluation Activities for the collaborative Protection Profile for Database Management Systems, 15 March 2023, Version 1.1 (SD DBMS) has been taken into account.

This Security Target claims conformance to assurance requirement package EAL2 augmented by ALC_FLR.3, Flaw Reporting Procedures.

Threats:

T.ACCESS_TSFDATA

T.ACCESS_TSFFUNC

T.IA_USER

T.RESIDUAL_DATA

T.UNAUTHORIZED_ACCESS

OSPs:

P.ACCOUNTABILITY

P.ROLES

P.USER

Assumptions:

A.PHYSICAL

A.AUTHUSER

A.MANAGE

A.TRAINEDUSER

A.NO_GENERAL_ PURPOSE

A.PEER_FUNC_& _MGT

A.SUPPORT

A.CONNECT

More information can be found in the ST chapter 3.

The evaluation has been performed by Combitech AB in Växjö and Bromma, where the evaluation activities took place.

The evaluation was completed on 2025-11-26. The evaluation was conducted in accordance with the requirements of Common Criteria (CC), version 3.1 release 5.

Combitech AB is a licensed evaluation facility for Common Criteria under the Swedish Common Criteria Evaluation and Certification Scheme. Combitech AB is also accredited by the Swedish accreditation body 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 the Common Methodology for evaluation assurance level EAL2 augmented by ALC_FLR.3.

The technical information in this report is based on the Security Target (ST) and the Final Evaluation Report (FER) produced by Combitech AB.

2 Identification

Certification Identification	
Certification ID	CSEC2024005
Name and version of the certified IT product	Oracle AI Database 26ai (23.26.0 with Critical Patch Updated October 2025)
Security Target Identification	Oracle AI Database 26ai Security Target, 2025-12-09, Version 1.0
EAL	EAL 2 + ALC_FLR.3
Sponsor	Oracle Corporation
Developer	Oracle Corporation
ITSEF	Combitech AB
Common Criteria version	3.1 revision 5
CEM version	3.1 revision 5
QMS version	2.6.1
Scheme Notes Release	22.0
Recognition Scope	CCRA, SOGIS-MRA, EA-MLA
Certification date	2025-12-17

3 Security Policy

The logical boundary of the TOE includes all interfaces and functions within the physical boundary. The logical boundary of the TOE may be broken down by the security function classes:

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access

3.1 Security Audit

Audit entries are generated for security related events. Audit policies may be created to generate logs based on details such as the user, the object being accessed, event type or success or failure of the operation.

3.2 User Data Protection

The TOE provides a discretionary access control policy to provide fine-grained access control between users and database objects. The TOE provides a multitenant environment where resources in pluggable databases are logically separate and inaccessible by local users in any other pluggable database or Container Database (CDB). Once data is allocated to a resource, the previous information content is no longer available.

3.3 Identification and Authentication

Users must identify and authenticate prior to gaining TOE access. Attributes are maintained to support the access control policy.

3.4 Security Management

The TOE provides management capabilities via SQL statements. Management functions allow the administrators to:

- configure auditing and access control options (including granting and revoking privileges)
- configure users (including the maximum number of concurrent sessions) and roles
- configure replication options
- configure separate domains for pluggable databases within a container database
- assess roles and privileges in use at run-time

3.5 Protection of the TSF

Data may be consistently replicated to a secondary DBMS server.

3.6 TOE Access

The number of concurrent user sessions may be limited by policy. User login may be restricted based on user identity.

4 Assumptions and Clarification of Scope

4.1 Assumptions

The Security Target [ST10] makes eight assumptions on the operational environment of the TOE.

A.PHYSICAL

The operational environment is assumed to provide the TOE with appropriate physical protection such that the TOE is not subject to physical attack that may compromise the security and/or interfere with the platform's correct operation. This includes protection for the physical infrastructure on which the TOE depends for correct operation and hardware devices on which the TOE is executing.

A.AUTHUSER

Authorized users possess the necessary authorization to access the information managed by the TOE in accordance with organization information access policies.

A.MANAGE

The TOE security functionality is managed by one or more competent, authorized administrators. The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the guidance documentation.

A.TRAINEDUSER

Authorized users are sufficiently trained to accomplish a task or a group of tasks within a secure IT environment by exercising control over their user data.

A.NO_GENERAL_ PURPOSE

There are no general-purpose computing capabilities (e.g., compilers or user applications) available on DBMS servers, other than those services necessary for the operation, administration, and support of the DBMS.

A.PEER_FUNC_& _MGT

All external IT systems trusted by the TSF to provide TSF data or services to the TOE, or to support the TSF in the enforcement of security policy decisions are assumed to correctly implement the functionality used by the TSF consistent with the assumptions defined for this functionality and to be properly managed and operate under security policy constraints compatible with those of the TOE.

A.SUPPORT

Any information provided by a trusted entity in the IT environment and used to support the provision of time and date, information used in audit capture, user authentication, and authorization that is used by the TOE is correct and up to date.

A.CONNECT

All connections to and from remote trusted IT systems and between separate parts of the TSF are physically and/or logically protected within the TOE environment to ensure the integrity and confidentiality of the data transmitted and to ensure the authenticity of the communication end points.

4.2 Clarification of Scope

The Security Target contains five threats, which have been considered during the evaluation:

T.ACCESS_TSFDATA

A user or a process may read or modify TSF data using functions of the TOE without being identified, authenticated and authorized.

T.ACCESS_TSFFUNC

A user or a process may use, manage or modify the TSF, bypassing the protection mechanisms of the TSF.

T.IA_USER

A user who has not successfully completed identification and authentication may gain unauthorized access to user data or TOE resources beyond public objects.

T.RESIDUAL_DATA

A user or a process acting on behalf of a user may gain unauthorized access to user or TSF data through reallocation of TOE resources from one user or process to another.

T.UNAUTHORIZED_ACCESS

An authenticated user or a process, in conflict with the TOE security policy, may gain unauthorized access to user data.

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

P.ACCOUNTABILITY

The authorized users of the TOE shall be held accountable for their actions within the TOE.

P.ROLES

Administrative authority to TSF functionality shall be given to trusted personnel and be as restricted as possible while supporting only the administrative duties the person has. This role shall be separate and distinct from other authorized users.

P.USER

Authority shall only be given to users who are trusted to perform the actions correctly and are permitted by the organization to access user data.

5 Architectural Information

The TOE consists of the Oracle AI Database 26ai software in one of the four configurations shown in Figure 1.

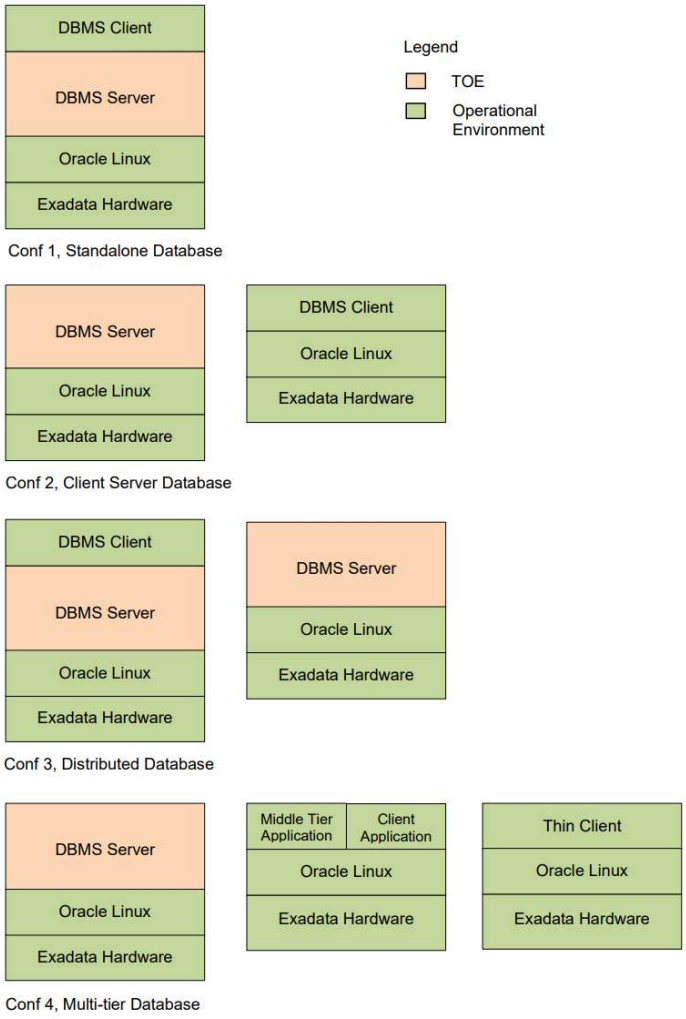

Figure 1, TOE configurations

The configurations are:

1. The DBMS server operated with a co-located client
2. The DBMS server operated with a remote client
3. A primary DBMS server and a secondary DBMS server with replicated data
4. A DBMS server accessed by a thin client through a middle tier application proxy

6 Documentation

The TOE includes the following guidance documentation:

INST_CONF	Oracle® Exadata Database Machine, Installation and Configuration Guide for Exadata Database Machine, 25.2 F29249-41, October 2025
INST	Oracle® AI Database, Database Installation Guide, 26ai for Linux, G43069-01, October 2025
ADM	Oracle® AI Database, Database Administrator's Guide, 26ai G42927-01, October 2025
SQL	Oracle® AI Database, SQL Language Reference, 26ai G43935-01, October 2025
PL/SQL	Oracle® AI Database, Database PL/SQL Language Reference, 26ai G43964-01, October 2025
SEC	Oracle® AI Database, Security Guide, 26ai G43025-02, October 2025
DG	Oracle® AI Database, Data Guard Concepts and Administration, 26ai G43580-01, October 2025
TPR	Test Plan and Report – Oracle AI Database 26ai, Combitech AB, 24FMV2697-35, November 2025
M-ADM	Oracle® AI Database, Multitenant Administrator’s Guide, G43631-01, Oktober 2025

7 IT Product Testing

7.1 Developer Testing

The testing effort, outlining the testing approach, configuration, depth and results for the developer testing is described in the developer test reports.

All developer tests are in the form of scripts to be started manually one by one or automatically in a test sequence.

The actual results from each test script are compared with the results from previous, approved, execution of the script. The evaluator examined the test scripts in order to verify that the security functionality claimed by the developer's test coverage analysis to be tested actually was covered by the expected test results.

The developer testing was done between 31 October and 4 November 2025.

All developer tests result in a Pass.

7.2 Evaluator Testing

The test performed by the evaluator is presented in the [TPR]. Testing was performed on the entirety of the OCI/JDBC interface, meaning all SFRs connected to the interface, with a passing result.

The evaluator testing was performed twice, once with Oracle Label Security, OLS, and Oracle Database Vault configured and turned on, and once without OLS and Database Vault. Configuration of both is described in [M-ADM]. The evaluator performed the configuration on all of the relevant nodes used in the testing. Both configurations gave the same result, pass.

The tests are in [TPR] divided into the following test groups:

- Test Group 1: TOE Installation
- Test Group 2: Identification and Authentication
- Test Group 3: Access Control Policies
- Test Group 4: Audit Management
- Test Group 5: Active Data Guard
- Test Group 6: Session Handling
- Test Group 7: Penetration Tests

The complete testing effort can be found in [TPR], each test case contains descriptions of the test steps, expected result of each test step, and if the test reaches this expected result or not. Additional evidence of the test steps and result are reported under each test case's table of test execution description.

7.3 Penetration Testing

The following types of penetration tests were performed:

- Port scan
- Vulnerability scan

Port scans were run after installation and configuration had been done according the guidance documentation. The purpose was to check that no unexpected ports were opened unfiltered and no unexpected services available. The Nmap (www.nmap.org) port scan tool was used.

The following software tools was used:

- Nmap port scanning tool, v7.92, https://nmap.org/
- Nessus vulnerability scanner, version : 10.10.1, plugin feed version: 202511052236

All penetration testing had negative outcome, i.e. no vulnerabilities were found.

8 Evaluated Configuration

The following features are excluded from this evaluation:

• Authentication features

- Although Oracle AI Database 26ai supports several authentication mechanisms, including Kerberos and Public Key Infrastructure, only Oracle password authentication was demonstrated for the purposes of this evaluation.

• Real Application Clusters (RAC)

• External clients

• DBaaS databases

- Oracle Cloud Infrastructure (OCI) DBaaS databases which is the Oracle Database deployed in the cloud and offered as a service, were not evaluated.

• Database Vault

- Oracle Database Vault adds mandatory access controls within the Oracle AI Database that restrict access to specific schemas, objects, and SQL operations regardless of system or DBA privileges, with enforcement handled by the database kernel. These controls are implemented using realms to protect database objects, command rules to govern execution of SQL statements, and secure application roles that are enabled only under defined conditions. Database Vault was not evaluated.

• Oracle Label Security

- Oracle Label Security (OLS), controls the display of data within a table using labels that are assigned to data objects and to application users. When access is requested, OLS compares the data label with the user's label authorizations. Access to specific data objects can be restricted based on authorization level, compartments and groups. OLS was not evaluated.

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 [ST10] 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/Assurance Family	*Class/Component*	*Verdict*
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.1	PASS
TOE summary specification	ASE_TSS.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
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 guideance	AGD_OPE.1	PASS
Preparative procedures	AGD_PRE.1	PASS
Tests	ATE	PASS
Coverage	ATE_COV.1	PASS
Functional tests	ATE_FUN.1	PASS
Independent testing	ATE_IND.2	PASS
Vulnerability Assessment	AVA	PASS
Vulnerability analysis	AVA_VAN.2	PASS

Evaluator Comments and Recommendations

None.

10 Glossary

CEM	Common Methodology for Information Technology Security, document describing the methodology used in Common Criteria evaluations
CC	Common Criteria for Information Technology Security, a set of three documents describing different aspects of Common Criteria evaluations
DBMS	Database Management Security
SQL	Structured Query Language
ITSEF	IT Security Evaluation Facility, test laboratory licensed to operate within a evaluation and certification scheme
ST	Security Target, document containing security requirements and specifications , used as the basis of a TOE evaluation
TOE	Target of Evaluation

11 Bibliography

FER_12	Final Evaluation Report, Vulnerability Analysis - Oracle AI Database 26ai, Combitech AB, 2025-12-17, document version 1.2, 24FMV2697-49
ST11	Oracle AI Database 26ai, Security Target, Oracle Corporation, 2025-12-17, version 1.1, 24FMV2697-50
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
CCADD	CC and CEM Addenda: Exact Conformance, Selection-Based SFRs, Optional SFRs, CCDB, 2021-Sep-30, version 2.0
EP-002	002 Evaluation and Certification, CSEC, 2023-06-02, Document version 35.0
INST_CONF	Oracle® Exadata Database Machine, Installation and Configuration Guide for Exadata Database Machine, 25.2 F29249-41, 24FMV2697-35, October 2025
DG	Oracle® AI Database, Data Guard Concepts and Administration, 26ai G43580-01, 24FMV2697-35, October 2025
SEC	Oracle® AI Database, Security Guide, 26ai G43025-02, 24FMV2697-35, October 2025
PL/SQL	Oracle® AI Database, Database PL/SQL Language Reference, 26ai G43964-01, 24FMV2697-35, October 2025
INST	Oracle® AI Database, Database Installation Guide, 26ai for Linux, G43069-01, 24FMV2697-35, October 2025
ADM	Oracle® AI Database, Database Administrator's Guide, 26ai G42927-01, 24FMV2697-35, October 2025
SQL	Oracle® AI Database, SQL Language Reference, 26ai G43935-01, 24FMV2697-35, October 2025
TPR	Test Plan and Report – Oracle AI Database 26ai, Combitech AB 24FMV2697-35, November 2025, v1.0
M-ADM	Oracle® AI Database, Multitenant Administrator’s Guide, G43631-01, 24FMV2697-35, October 2025

Appendix A Scheme Versions

During the certification the following versions of the Swedish Common Criteria Evaluation and Certification scheme have been used.

A.1 Scheme/Quality Management System

Version	Introduced	Impact of changes
2.6.1	2025-10-16	None
2.6	2025-03-27	None
2.5.1	Application	Original version

A.2 Scheme Notes

The following Scheme Notes have been considered during the evaluation:

- Scheme Note 15 – Testing
- Scheme Note 18 – Highlighted Requirements on the Security Target
- Scheme Note 22 – Vulnerability assessment
- Scheme Note 23 – Evaluation reports for NIAP PPs and cPPs
- Scheme Note 25 – Use of CAVP-tests in CC
- Scheme Note 27 – ST Requirements at the Time of Application for Certification
- Scheme Note 28 – Updated procedures for application, evaluation and certification