Oracle AI Database 26ai Common Criteria Guidance Supplement

Version: 1.0
Date: 2026-01-07

Oracle Corporation
2300 Oracle Way
Austin, TX 78741
U.S.A.

Prepared by:

Combitech AB
351 80 Växjö
Sweden

DOCUMENT HISTORY

Version	Status	Issue date	Revision description	Edited by
0.1	Draft	2024-05-27	First draft version	Anders Staaf
0.2	Draft	2024-06-27	Updated after peer review	Anders Staaf
0.3	Draft	2024-08-30	Fixed heading numbering	Anders Staaf
0.4	Draft	2024-12-03	Minor update	Anders Staaf
0.5	Draft	2025-09-02	Changed platform to Exadata. Updated 3.1. Initialization Parameters, bullet c).	Anders Staaf
0.6	Draft	2025-10-06	Changes after comments from Oracle	Anders Staaf
0.7	Draft	2025-10-16	TOE name changed to Oracle AI Database 26ai	Anders Staaf
0.8	Draft	2025-11-03	Patch id added.	Anders Staaf
0.9	Draft	2025-11-06	Minor changes.	Anders Staaf
1.0	Approved	2026-01-07	Version updated to 1.0. No other changes from the certified version.	Anders Staaf

Contents

1 Security Acceptance Procedures

Secure acceptance procedures ensure that the correct version of the TOE has been received by the customer as intended by the developer. It is strongly recommended that Oracle AI Database 26ai is installed on the Exadata platform as a service from Oracle or from our certified partners. Installation services uses Oracle Exadata Deployment Assistant (OEDA) to install the Oracle database software and create a starter database.

However, if you choose to install the database without professional services, instructions for using OEDA to configure your engineered system can be found in Chapter 6 of Oracle® Exadata Database Machine, Installation and Configuration Guide for Exadata Database Machine, [1].

1.1 Patch and Critical Updates (PPU/CSU)

Information on the October 2025 Patch/Critical Patch Update can be found at:

https://www.oracle.com/security-alerts/

1. To download the patch a user needs to access the Oracle support website: https://support.oracle.com.
2. Click “*Log In to My Oracle Support*”.

   Note: First time users must first register by clicking “*Register as a new user*”.
3. Select the ‘Patches & Updates’ tab.
4. Search by Patch Number/name: 38404116, Platform Linux x86-64.
5. Click Search.
6. Select the 38404116 patch for the Linux operating system. Once the screen for this patch appears, click on the Readme button to access prerequisite information and installation instructions. Follow the Readme instructions.
7. Click ‘Download’ to download the patch.
8. Click on p38404116_230000_Linux-x86-64.zip.
9. Additional patching guidance for the Exadata platform can be found in My Oracle Support note Doc ID 888828.1

2 Secure Installation Procedure

This section describes the steps necessary for secure installation of the TOE and the secure preparation of the operation environment in the evaluated configuration.

2.1 Secure Preparation of the Operational Environment

The following security objectives for the operational environment are defined with respect to the secure installation and operation of the TOE in its operational environment.

2.1.1 OE.ADMIN

OE.ADMIN	Those responsible for the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of the information it contains.

Those responsible for the Oracle AI Database 26ai must ensure that only known, competent, trusted employees are made responsible for managing the security of the database and the data contained therein. Employees should be subject to background checks and undergo Oracle AI Database 26ai database training before being put into a position of trust.

2.1.2 OE.INFO_PROTECT

OE.INFO_ PROTECT Those responsible for the TOE shall establish and implement procedures to ensure that information is protected in an appropriate manner. In particular:

- All network and peripheral cabling shall be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques.
- DAC protections on security-relevant files (such as audit trails and authorization databases) shall always be set up correctly.
- Users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.

Adherence to ISO/IEC 11801 standards is required for the implementation of cabling associated with any device connected to the network which includes an Oracle AI Database 26ai implementation. Both copper and fibre optic cabling are permitted.

Users of the Oracle AI Database 26ai must ensure that all implementations are fully planned prior to system installation and configuration. All access controls must be put in place before the database is populated.

The Oracle AI Database 26ai must be implemented using a ‘least privilege’ approach. Users may only be permitted access to the data to which access is required in order to perform assigned functions. Only those users fully trained in the use of the Oracle AI Database 26ai, and who have been advised of their privileges and responsibilities may be given access.

2.1.3 OE.NO_GENERAL_PURPOSE

OE.NO_ GENERAL_ PURPOSE There shall be 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.

Installers of the database must ensure a fresh installation of the underlying operating system has been implemented and hardened in accordance with the organization’s best practices prior to database installation. Access to the operating system must be strictly controlled, and no other services may be installed on the database server.

2.1.4 OE.PHYSICAL

OE.PHYSICAL Those responsible for the TOE shall ensure that those parts of the TOE critical to enforcement of the security policy are protected from physical attack that might compromise IT security objectives. The protection shall be commensurate with the value of the IT assets protected by the TOE.

Installers are instructed to only install the Oracle AI Database 26ai in locations that provide physical security against possible attack in accordance with the organization’s policy. Security should be increased in accordance with the value of the data to be protected within the database.

2.1.5 OE.IT_I&A

OE.IT_I&A Any information provided by a trusted entity in the environment and used to support user authentication and authorization used by the TOE is correct and up to date.

Prior to configuring an Oracle AI Database 26ai with an external authentication mechanism, the implementers must ensure that every entry in the authentication system is correct and up to date.

2.1.6 OE.IT_TRUSTED_SYSTEM

OE. IT_ TRUSTED_ SYSTEM External IT systems may be required by the TOE for the enforcement of the security policy. These external trusted IT systems shall be managed according to known, accepted, and trusted policies based on the same rules and policies applicable to the TOE, and are physically and shall be sufficiently protected from any attack that may cause those functions to provide false results.

The Oracle AI Database 26ai implementation team must ensure that any system that connects to the database must be implemented securely and protected from possible physical attack. Only remote systems that are under control of those implementing the database, and subject to the same physical and access control security policies should be allowed to access the database.

2.2 Initial Setup and Configuration

Administrators should perform the initial setup and configuration of the TOE in accordance with the instructions provided in the following chapters from the *Oracle® Exadata Database Machine Installation and Configuration Guide for Exadata Database Machine,* [1]:

- Chapter 1, Site Requirements for Oracle Exadata and Oracle Exadata Storage Expansion Rack
- Chapter 2, Understanding the Network Requirements for Oracle Exadata
- Chapter 3, Using Oracle Exadata Deployment Assistant
- Chapter 4, OEDA Command Line Interface
- Chapter 5, Installing Oracle Exadata or Oracle Exadata Storage Expansion Rack at the Site
- Chapter 6, Configuring Oracle Exadata Database Machine

Administrators managing a multitenant environment should refer to Part II and Part III of the *Oracle® AI Database, Multitenant Administrator's Guide, 26ai,* [4]. Initial setup and configuration are performed in accordance with the instructions provided in the following chapters:

- Chapter 2 Preparing to Create a CDB
- Chapter 3 Creating a CDB: Basic Steps
- Chapter 4 Creating a CDB: Advanced Topics
- Chapter 6 Overview of PDB Creation
- Chapter 7 Creating a PDB from Scratch
- Chapter 8 Cloning a PDB

Administrators should also be aware of the contents of the *Oracle® AI Database, Database Administrator's Guide, 26ai, [3].*

2.3 Password Configuration

Administrators are required to manually enable the password complexity checking function using the `Ora12c_strong_verify_function`. Instructions on enabling this function can be found in the *Oracle® AI Database, Security Guide, 26ai,* [2], Section 3. ora12c_strong_verify_function Function Password Requirements can be found in section 3.2.6.5.

3 Other Procedures

This section describes the user-accessible functions and privileges that should be controlled in a secure processing environment and includes the security-critical information and security-critical actions required for secure use of the TOE.

3.1 Initialization Parameters

The following steps must be completed for the TOE to operate in the evaluated configuration.

a) Check the following initialization parameters using the SQL*Plus command: show parameters.
   - To connect to the DBMS as a privileged user, such as a database administrator, the following parameters shall be set in the appropriate initialization file:

     ```
     Remote_login_passwordfile = EXCLUSIVE
     ```

   - The following parameter ensures that a user must have SELECT privilege on a table when executing an UPDATE or DELETE statement that references table column values in a WHERE or SET clause:

     ```
     sql92_security = TRUE
     ```

b) In the evaluated configuration, the operating system does not authenticate remote users nor perform role associations. Therefore, the following parameters must be set:

   SQLNET.AUTHENTICATION_SERVICES = (NONE) shall be set in SQLNET.ORA.

   ```
   os_roles = FALSE
   ```

c) Make sure that the following predefined unified audit policies are enabled:

   ```
   audit policy ora_login_logout whenever not successful;

   audit policy ora_secureconfig;
   ```

3.2 Evaluated Configuration

For the purposes of the evaluation, Oracle AI Database 26ai was configured to demonstrate the Security Functional Requirements in the Security Target. In order to replicate the evaluated configuration, the steps shown in the below subsections must be followed.

3.2.1 Previous Login Information

The date and time of the last successful login are displayed when a user logs in.

In order to display the date and time of the last unsuccessful attempt to login and the number of unsuccessful attempts since the last successful login, the user must run a custom query. The user must be granted the SELECT_CATALOG_ROLE and AUDIT_VIEWER role in order to have the permissions required to run this query. The following steps provide the instructions for granting these permissions to a user, and for running the query as a test user. An organization would be required to customize these instructions to accommodate the usernames, passwords and filenames required for the organization’s own implementation. Note that the user name must be in capital letters and the password must be at least nine characters in length. Instead of using capital letters in the user name, the administrator may choose to surround the username parameter with double quotes (i.e. “&user_name”). This would be done wherever the user name appears in the script, with the exception of within the SELECT commands. It is suggested that passwords be read as a parameter from the command line. Otherwise, the correct password may be entered in the following script in place of <password>.

-- Invoke as follows:

```
SQL> sqlplus /nolog
```

```
SQL> @commoncriteria.sql <dba_user_name> <dba_pwd> <user_name>
<user_pwd> <tns_alias>
```

-- dba_user_name can be any user with DBA ROLE. This is required for provisioning the test user and DB.

-- Example:

```
SQL> sqlplus /nolog
```

```
SQL> @commoncriteria SYSTEM Sys_Pwd User1 User1_Pwd testpdb
```

-- The commoncriteria.sql script:

```
SPOOL commoncriteria.log
SET ECHO ON
SET FEEDBACK ON
DEFINE dba_usr = &1
DEFINE dba_pwd = &2
DEFINE user_name = &3
DEFINE pass = &4
DEFINE tns = &5
-- Setup script
-- Execute as user with DBA ROLE
CONN &dba_usr/&dba_pwd@&tns as sysdba
DROP USER "&user_name" CASCADE;
CREATE USER "&user_name" IDENTIFIED BY &pass;
GRANT CREATE SESSION TO "&user_name";
GRANT SELECT_CATALOG_ROLE, AUDIT_VIEWER TO "&user_name";
-- Enable ORA_LOGON_FAILURES audit policy
AUDIT POLICY ORA_LOGON_FAILURES WHENEVER NOT SUCCESSFUL;
-- Attempt Successful logins
CONN "&user_name"/&pass@&tns
COLUMN login_time FORMAT a40
VAR login_timestamp varchar2(1024);
EXECUTE :login_timestamp := TO_CHAR(current_timestamp AT LOCAL);
SELECT :login_timestamp AS login_time FROM DUAL;
-- Attempt unsuccessful logins
CONN "&user_name"/pass1@&tns
CONN "&user_name"/pass2@&tns
CONN "&user_name"/pass3@&tns
CONN "&user_name"/&pass@&tns
-- Query login time
-- FTA_TAH_(EXT).1.1/FTA_TAH_(EXT).1.2
-- a. Query the date and time of the session establishment attempt of
the user
COLUMN username FORMAT a30
COLUMN last_successful_login_time FORMAT a40
SELECT username, last_login AT LOCAL as last_successful_login_time FROM
dba_users WHERE username = '&user_name';
-- b. The incremental count of successive unsuccessful session
establishment attempt(s).
COLUMN unsuccessful_attempts FORMAT 9999
-- Should record 3 unsuccessful attempts.
SELECT dbusername as username, count(*) as unsuccessful_attempts
FROM unified_audit_trail
WHERE unified_audit_policies like '%ORA_LOGON_FAILURES%'
AND dbusername = '&user_name'
AND return_code = 1017
AND event_timestamp AT LOCAL >= TO_TIMESTAMP_TZ(:login_timestamp)
GROUP BY dbusername;
REM QUIT;
```

3.3 Network Encryption Configuration

Network encryption is outside the scope of the evaluation. However, an administrator can manually enable the encryption of data that is sent over the network. Administrators should configure the network encryption in accordance with the instructions provided in the following chapters of the *Oracle® AI Database, Security Guide, 26ai,* [2]:

- Chapter 20, Configuring Oracle Database Native Network Encryption and Data Integrity
- Chapter 21, Configuring Transport Layer Security Encryption

Appendix B - Referenced Documents

The following installation and administrative guides are referenced within this document:

[1] Oracle® Exadata Database Machine, Installation and Configuration Guide for Exadata Database Machine, 25.2, F29249-41, October 2025

[2] Oracle® AI Database, Security Guide, 26ai G43025-02, October 2025

[3] Oracle® AI Database, Database Administrator's Guide, 26ai G42927-01, October 2025

[4] Oracle® AI Database, Multitenant Administrator's Guide, 26ai G43631-01, October 2025