Oracle® Database

Security Assessment Tool User Guide

Release 4.1

G44164-01

December 2025

The Oracle Database Security Assessment Tool

In the age of data breaches and ever-evolving data protection and privacy regulations, it is more important than ever for organizations to be confident that their databases are secure. However, it can be difficult to know whether the databases are configured correctly, who has access to it, and where sensitive data is stored. The Oracle Database Security Assessment Tool (DBSAT) helps identify areas where your database configuration, operation, or implementation introduces risks. DBSAT will recommend changes and controls to help mitigate those risks.

Why the Need for a Security Assessment?

Misconfigured databases are a major contributor to database breaches. Human errors could leave your database open to everyone, or an attacker could maliciously exploit configuration mistakes to gain unauthorized access to sensitive data. This can have a devastating impact on your reputation and bottom line. Knowing where your database configuration introduces risk is the first step in minimizing that risk.

About the Oracle Database Security Assessment Tool

The Oracle Database Security Assessment Tool (DBSAT) is a lightweight, command-line utility designed to enhance the security posture of Oracle Databases. It analyzes database configurations, user accounts, their entitlements, security policies in place, and sensitive data location to help identify risks.

DBSAT supports regulatory compliance efforts, accelerates the adoption of security best practices, and helps mitigate risks. DBSAT is free for customers with an active Oracle support contract.

Benefits of Using Oracle Database Security Assessment Tool

Using DBSAT, you can:

- Quickly and easily assess the current security status and identify sensitive data within the Oracle Database.

- Reduce risk exposure using proven Oracle Database security best practices, CIS Benchmark recommendations and Security Technical Implementation Guides (STIG) rules.
- Leverage security findings to accelerate compliance with EU GDPR and other regulations.
- Improve the security posture of your Oracle Databases and promote security best practices.

> **Note**
>
> DBSAT is a lightweight utility that will not impair system performance in a measurable way.

You can use DBSAT report findings to:

- Minimize immediate short term risks
- Implement a comprehensive security strategy
- Support your regulatory compliance program
- Promote security best practices

Oracle Database Security Assessment Tool Components

The DBSAT consists of the following components:

- **Collector:**

  The **Collector** executes SQL queries and runs operating system commands to collect data from the system to be assessed. It does this primarily by querying database dictionary views. The collected data is written to a JSON file that is used by the DBSAT Reporter in the analysis phase. Note that if the collector is executed remotely it will not collect operating system data. It is recommended to run it in the database server to collect all relevant data.

- **Reporter:**

  The **Reporter** analyzes the collected data and generates the Oracle Database Security Assessment Report in HTML, Excel, JSON, and Text formats. The Reporter can run on any machine: PC, laptop, or server. You are not limited to running the Reporter on the database server or the same machine as the Collector.

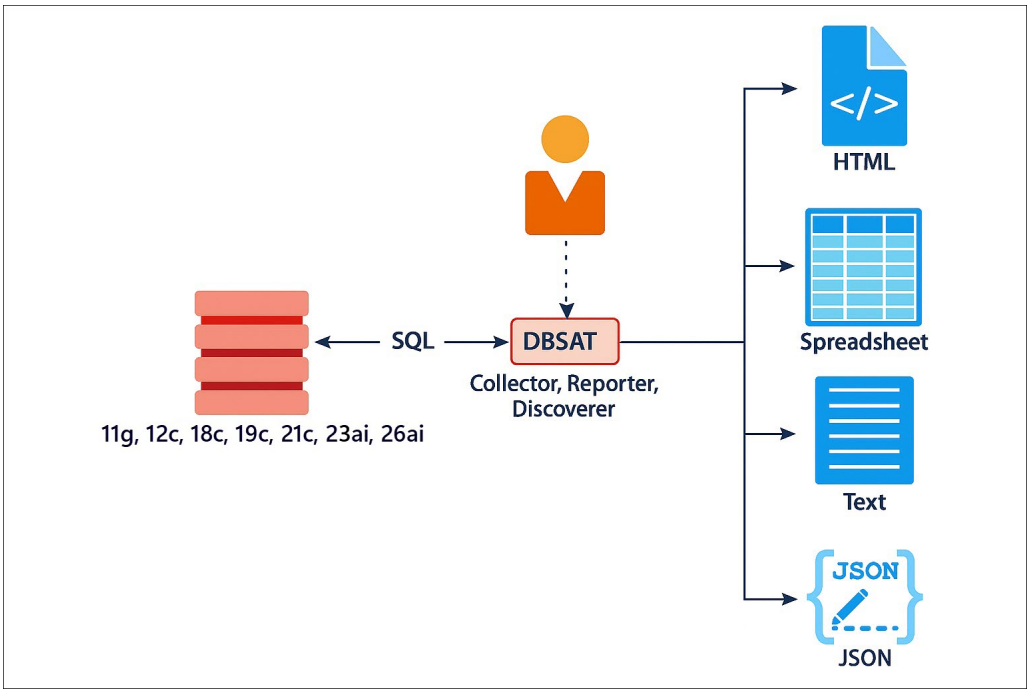
- **Discoverer:**

  The **Discoverer** executes SQL queries and collects metadata from the database to be assessed, based on the settings specified in the configuration files. It does this primarily by querying database dictionary views. The collected data is then used to generate the Oracle Database Sensitive Data Assessment Report in HTML, CSV, and JSON formats. The Discoverer can run on any machine: PC,

laptop, or server. You are not limited to running the Discoverer on the database server or the same machine as the Collector or Reporter.

The following figure shows the components, sources, and reports of the Oracle Database Security Assessment Tool.

Figure 1-1 DBSAT Components, Sources, and Reports



DBSAT, by default, generates encrypted output files. To decrypt the files, you will need to use the dbsat extract command.

For more information about the Collector, Reporter, and Discoverer, see Using the Collector and Reporter.

Prerequisites

The following sections outline the prerequisites for the Oracle Database Security Assessment Tool:

Supported Operating Systems

Database configuration collection queries can be executed on most supported Oracle Database platforms. However, DBSAT does not collect operating system (OS) data for databases running on Windows platforms or when the Collector is executed remotely.

DBSAT runs on:

- Linux x86-64 and Linux 64-bit ARM
- Windows x64

For the following platforms, Oracle JDK 17 is not available. Therefore, you must run the Collector without encrypting the output by using the `-n` flag:

- Oracle Solaris on x86–64 (64-Bit)
- Oracle Solaris on SPARC (64-bit)
- IBM AIX on POWER Systems (64-Bit)
- IBM: Linux on System z
- HP-UX Itanium (64-Bit)

Supported Database Versions

You can run the DBSAT on Oracle Database 11.2.0.4 and later releases on-premises or in the Cloud, on Oracle AI Database Standard Edition 2 and Oracle AI Database Enterprise Edition. You can also run DBSAT against Oracle Autonomous AI Databases (Serverless, Dedicated, and Cloud@Customer), Oracle Autonomous AI JSON Database, Oracle Exadata Database Service (Dedicated and Cloud@Customer), and Oracle Base Database Service (BaseDB Enterprise Edition and Standard Edition). Some findings will do different checks and provide targeted remarks for these databases. For more information about the target-specific checks and recommendations, see Appendix A.

Security Requirements

DBSAT output files are sensitive because they may reveal weaknesses in the security posture of your database. To prevent unauthorized access to these files, you must implement the following security guidelines:

- Ensure that the directories holding these files are secured with the appropriate permissions.
- Delete the files securely after you implement the recommendations they contain.
- Share them with others in their (by default) encrypted form.
- Grant user permissions to the DBSAT user on a short-term basis and revoke these when no longer necessary.

  For more information about DBSAT user privileges, see Collector Prerequisites.
  For more information about DBSAT best practices, see: Best Practices

> ⚠ **Caution**
>
> This tool is intended to assist you in identifying potential sensitive data and vulnerabilities in your system. Further, the output generated by this tool may include potentially sensitive system configuration data and information that could be used by a skilled attacker to penetrate your system. You are solely responsible for ensuring that the output of this tool, including any generated reports, is handled in accordance with your company's policies.

Oracle Database Security Assessment Tool Prerequisites

DBSAT on Unix/Linux systems must execute under the BASH shell. If the server does not have this shell, you can install it or run DBSAT remotely from a different server that has it (or from a laptop running Windows, from where you can connect to the database).

UnZip

You will require `unzip` to uncompress the dbsat binary file.

Collector Prerequisites

To gather all necessary data, run the DBSAT Collector on the server that hosts the database. The collector uses operating system commands to gather process and file system information that the database alone cannot provide. Besides, the Oracle DBSAT Collector must be run as an OS user with read permissions on files and directories under `ORACLE_HOME` using SQL*Plus (through Oracle Database or Oracle Instant Client) to collect and process file system data using OS commands. If TDE is being used, make sure wallet is open.

The Oracle DBSAT Collector collects most of its data by querying database views. It must connect to the database as a user with sufficient privileges to select from these views. Grant the DBSAT user the following privileges:

- `CREATE SESSION`
- `READ` or `SELECT` on `SYS.REGISTRY$HISTORY`
- Role `SELECT_CATALOG_ROLE`
- Role `DV_SECANALYST` (if Database Vault is enabled or if Database Vault Operations Control is enabled)
- Role `AUDIT_VIEWER` (12*c* and later)
- Role `CAPTURE_ADMIN` (12*c* and later)
- `READ` or `SELECT` on `SYS.DBA_USERS_WITH_DEFPWD`
- `READ` on `SYS.DBA_AUDIT_MGMT_CONFIG_PARAMS`
- `READ` on `SYS.DBA_CREDENTIALS`

- `EXECUTE` on `SYS.DBMS_SQL`

> **Note**
>
> By default, DBSAT Collector encrypts output files to protect sensitive data, which requires Oracle JDK 17 or higher to be installed on the system. Since Oracle JDK 17 is not available on IBM AIX, Oracle Solaris, and HP-UX Itanium, use `dbsat collect -n` to disable encryption when running on those platforms.
>
> If the Oracle Database under assessment is running on one of these platforms, you have two options:
>
> - Collect the data with `-n`, transfer the file to a system with Oracle JDK 17, and run the Reporter there.
> - Run `dbsat collect` remotely from a system that has Oracle JDK 17 installed and can connect to the database.
>
> Always handle unencrypted files with care and delete them securely after use.

Sample Script to Create a User with Minimum Privileges

You can create a user with required minimum privileges to run the Oracle Database Security Assessment Tool Collector with a script.

Purpose

Create a DBSAT user to run the DBSAT Collector script with required privileges.

Sample Script

```
create user dbsat_user identified by dbsat_user;
--If Database Vault is enabled, connect as DV_ACCTMGR to run this
command
grant create session to dbsat_user;
grant select_catalog_role to dbsat_user;
grant select on ctxsys.ctx_indexes to dbsat_user;
grant select on sys.registry$history to dbsat_user;
grant read on sys.dba_audit_mgmt_config_params to dbsat_user;
grant select on sys.dba_users_with_defpwd to dbsat_user;
grant read on sys.dba_credentials to dbsat_user;
grant execute on sys.dbms_sql to dbsat_user;
grant audit_viewer to dbsat_user; // 12c and later
grant capture_admin to dbsat_user;// 12c and later covers
sys.dba_priv_captures, sys.priv_capture$, sys.capture_run_log$
--If Database Vault is enabled, connect as DV_OWNER to run these
commands
  grant DV_SECANALYST to dbsat_user;
  exec dbms_macadm.authorize_audit_viewer('dbsat_user'); // 23ai and
```

```
later
  exec dbms_macadm.add_auth_to_realm('Oracle Label Security',
'dbsat_user', null, dbms_macutl.g_realm_auth_participant);
```

Reporter Prerequisites

The Reporter is an Oracle Java program and requires the Oracle Java Runtime Environment (Oracle JRE) 17 (Oracle JDK 17) or later to run.

The `JAVA_HOME` environment variable must be set and should point to the installation directory on your system, which contains the bin and lib directories. For example:

```
$ export JAVA_HOME=/usr/lib/jvm/jdk-17.0.14-oracle-x64/
```

> **Note**
>
> The Reporter component of DBSAT require Oracle JDK17 at minimum. For IBM AIX, Oracle Solaris, and HP-UX Itanium platforms, the latest available Oracle JDK is version 11. For the platforms without Oracle JDK17, encryption of the collected JSON is not feasible. The user should use `-n` option and explicitly use zip or other commands to encrypt the same
>
> Oracle customers of Oracle products that use the Oracle JDK or Oracle JRE are entitled, without the need to separately purchase Oracle Java SE Subscriptions, to download and use Oracle Java SE updates, patches, and tools for use with the licensed Oracle product. Customers are only entitled to download such Oracle Java SE versions as are required by their Oracle product. Please check the Oracle AI Database Licensing Information User Manual for more details.

Discoverer Prerequisites

The Discoverer is an Oracle Java program and requires the Oracle Java Runtime Environment (Oracle JRE) 17 (Oracle JDK 17) or later to run.

The `JAVA_HOME` environment variable must be set and should point to the installation directory on your system, which contains the `bin` and `lib` directories. For example:

```
$ export JAVA_HOME=/usr/lib/jvm/jdk-17.0.14-oracle-x64/
```

The Discoverer collects metadata from database dictionary views and matches them against the patterns specified to discover sensitive data. The Discoverer must connect to the database as a user with sufficient privileges to select from these views. For more information about DBSAT user privileges, see Collector Prerequisites.

> **Note**
>
> The Discoverer component of DBSAT require Oracle JDK 17 at minimum. For IBM AIX, Oracle Solaris, and HP-UX Itanium platforms, the latest available Oracle JDK is version 11. For these platforms, you should execute the Discoverer remotely from a separate laptop or server that supports Oracle JDK 17.
>
> The Discoverer relies on table statistics to get row counts. In order to get accurate row count results, `DBMS_STATS` should be executed by the Database Administrator before the DBSAT user runs the Discoverer.

Installing the Oracle Database Security Assessment Tool

To install the DBSAT:

1. Log in to the database server.
2. Create the `dbsat` directory:

   ```
   mkdir –p /home/oracle/dbsat
   ```
3. Download or copy the `dbsat.zip` file to the database server, and unzip the file.

   ```
   unzip dbsat.zip –d /home/oracle/dbsat
   ```
   Where `-d` refers to the directory path.

These commands are for Linux / Unix. If the installation takes place on Windows, you will use similar commands for Windows.

The DBSAT is installed on the database server.

You can run the Collector, Reporter, and Discoverer from the `/home/oracle/dbsat` directory.

You can also add this directory to your `PATH` and skip the step of going to the directory every time you want to run the tool.

Using the Collector and Reporter

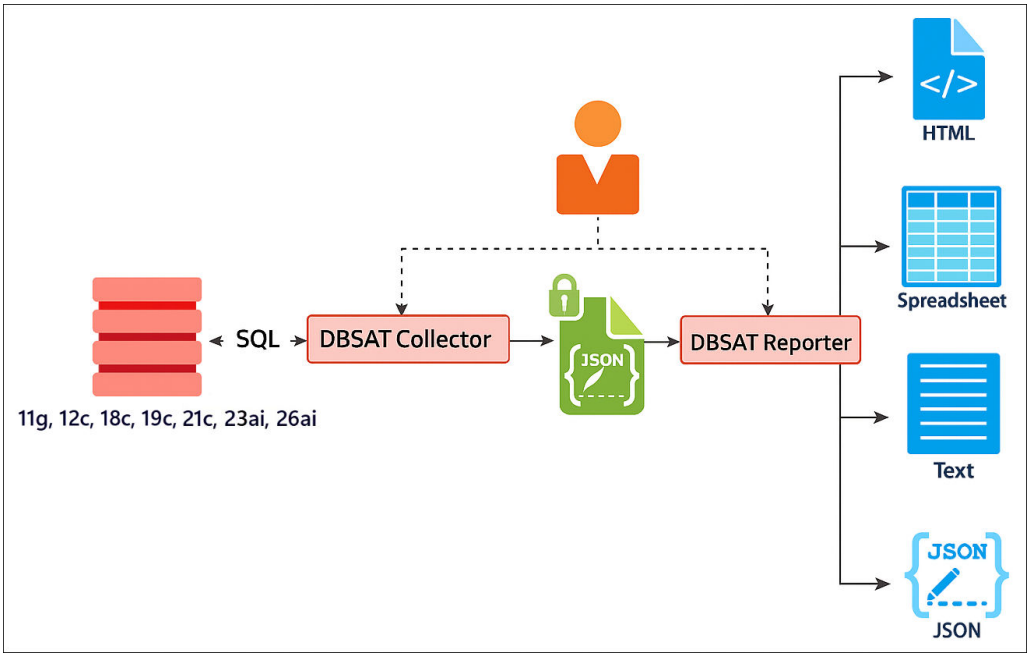
You can generate the Oracle Database Security Assessment Report and the Oracle Database Sensitive Data Assessment Report with the Collector, Reporter, and Discoverer components.

Oracle Database Security Assessment Report

The Collector and Reporter components are used to generate the Oracle Database Security Assessment Report.

The following figure shows the components and architecture of the Collector and Reporter.

Figure 1-2 Collector and Reporter Components and Architecture



Running the Collector

The Collector queries the database to collect data that will be analyzed by the Reporter.

> **Note**
>
> The Collector connects to the database. Ensure that the target database and listener are running before running the Collector.

To run the Collector, do the following:

1. Specify the arguments to run the Collector:

   ```
   $ dbsat collect [ -n ] [ -d ] [-r row limit number]
   <database_connect_string> <output_file>
   ```

   The `dbsat collect` command has the following options and arguments:

   - `-n`
     Specifies no encryption for output.

> **Note**
>
> For security reasons, this is not recommended.

- `-d`

  Shows additional diagnostics information and generates a log.

- `-r <number>`

  Row limit to control maximum number of rows collected for each query, minimum allowed value is 1.

- *`database_connect_string`*

  Specifies the connection string to connect to the database.

  Example: `system@ORCL`

- *`output_file`*

  Specifies the location and file name for the Database Security Assessment report. Do not add an extension.

  Example: `/home/oracle/dbsat/output_ORCL`

2. Run the Collector.

```
$ ./dbsat collect dbsat_user@ORCL output_ORCL
```

If running on Windows: `c:\> dbsat.bat collect "dbsat_user@ORCL" output_ORCL`

The following output is displayed:

```
Connecting to the target Oracle database...

SQL*Plus: Release 23.26.0.0.0 - for Oracle Cloud and Engineered
Systems on Wed Jun 25 17:16:41 2025
Version 23.26.0.0.0

Copyright (c) 1982, 2024, Oracle.  All rights reserved.


Connected to:Oracle AI Database 26ai Enterprise Edition Release
23.26.0.0.0 - for Oracle Cloud and Engineered Systems Version
23.26.0.0.0

Setup complete.
SQL queries complete.
OS commands complete.
Disconnected from Oracle AI Database 26ai Enterprise Edition
Release 23.26.0.0.0 - for Oracle Cloud and Engineered Systems
Version 23.26.0.0.0
DBSAT Collector completed successfully.
```

```
Encrypting output_ORCL.json...

Enter an encryption key:
Re-enter the encryption key:
  Encryption completed successfully.
$
```

> **Note**
>
> DBSAT can display warnings informing that some checks were skipped. These can be safely ignored as the execution proceeds. Some reasons to skip checks include wrong permissions, missing .ora files, not applicable to that target type, and more. For details, please refer to My Oracle Support.
>
> Running the Collector in the root container in a multitenant container database collects data specific to the root container and not from its pluggable databases. If you need to access specific pluggable databases, you must run the Collector for these pluggable databases separately.
>
> If you do not want to encrypt the file invoke the `dbsat collect` script with the `-n` option. This is not recommended.
>
> If DBSAT Collector is run remotely or on a WInfows platform operating system checks are skipped and `ORA-20002: Complete without OS Commands` is raised.

Running the Reporter

The Reporter analyzes the data collected by the Collector and makes recommendations to improve the security of the database.

You can invoke the Reporter with `dbsat report`.

To run the Reporter, do the following:

1. Check that Oracle Java Runtime Environment (Oracle JRE) 17 (Oracle JDK 17) or later is installed.

   ```
   $ java -version
   ```

   A similar output is displayed:

   ```
   java version "21.0.7" 2025-04-15 LTS
   ```

2. Specify the arguments to run the Reporter.

   ```
   $  dbsat report [-a] [-n] [-d] [-g] [-x <section>][-u <user> ][-f
   <output_format>] <input_file>
   ```

   Where the argument *`input_file`* stands for the full or relative path to the data file `output_ORCL` produced by the DBSAT Collector. If this file was encrypted during

data collection, you will need to supply the encryption password when prompted by the Reporter.

The Reporter supports the following command-line options:

- *-a*

  Runs the report for all the database accounts including locked or schema only accounts that are Oracle-supplied.

- *-n*

  Specifies no encryption for output.

  > **Note**
  >
  > For security reasons, this is not recommended.

- *-d*

  Shows additional diagnostics information and generates a log.

- *-f*

  Generate only one report file in the specified format.

  Valid formats are:

  – *html*
  – *txt*
  – *xlsx*
  – *json*

- *-g*

  Shows all grants including common grants in a pluggable database.

- `-u`

  Specify users to exclude from report.

  To exclude multiple users use a comma-separated list, for example: `-u SCOTT,DEBRA`

- *-x*

  Excludes a section from the report.

  Valid sections are:

  – `USER`: **User Accounts**
  – `PRIV`: **Privileges and Roles**
  – `AUTHZ`: **Authorization Control**
  – `ENCRYPT`: **Encryption**
  – `ACCESS`: **Fine-Grained Access Control**
  – `AUDIT`: **Auditing**

- `CONF`: **Database Configuration**
- `NET`: **Network Configuration**
- `OS`: **Operating System**

To exclude multiple sections use a comma-separated list, for example:

```
-x USER,PRIV
```

Or:

```
-x USER -x PRIV
```

Omitting this option will include all sections of the report.

The same path name is used to generate the report files produced by the Reporter in HTML, Excel, JSON, and Text formats with the appropriate file extensions.

3. Run the Reporter.

```
$ ./dbsat report output_ORCL
```

The following output appears:

```
Enter an encryption key:
Extracted: output_ORCL/output_ORCL.json
Decompression complete.
DBSAT Reporter ran successfully.

Encrypting the generated reports...

Enter an encryption key:
Re-enter the encryption key:
Encryption completed successfully.
```

> **Note**
>
> When prompted for an encryption key, the Reporter will require the original key used to encrypt the Collector output file. Ensure you have this key readily available to proceed. Additionally, be cautious when running a DBSAT command with an existing output file name, as pre-existing reports will be overwritten. If you specify a file name that already exists, the dbsat report command will replace the existing report.

4. Specify a password to encrypt the output report `.dbsat` encrypted file.

   The `.dbsat` encrypted file is created.

5. Extract the contents of the `.dbsat` file to access the Oracle Database Security Assessment Report.

```
$ ./dbsat extract output_ORCL_report
```

6. When prompted, enter the password to decrypt the `.dbsat` file specified in Step *4*.

The contents of the `.dbsat` file are extracted.

7. Use the appropriate tools to read the recommendations from the report files.

   Example: Use `vi` on Linux to read the `.txt` files.

   Example: Use a browser to display the `.html` files.

> **Note**
>
> DBSAT recommendations do not adjust for individual applications. In cases where the application requirements differ from DBSAT, you will frequently have to accept the finding as-is, possibly mitigating the finding through some other control. Unless the risk is too high for you to accept, the application requirements should usually supersede the DBSAT recommendation.

Oracle Database Security Assessment Report

The Collector and Reporter components are used to generate the Oracle Database Security Assessment (DBSAT) Report in HTML, Excel, JSON, and Text formats. All reports contain similar information but in different formats.

The HTML report provides detailed assessment results in a format that is easy to navigate. The Excel format provides a high-level summary of each finding without the detailed output included in the HTML report. It also allows you to add columns for your tracking and prioritization purposes. A report in text format makes it convenient to copy portions of the output for other usages. Finally, a JSON document containing the report contents is provided for easier filtering, comparison, aggregation, and integration with other tools.

The following Database Security Assessment Report sections will use the HTML report as an example and highlight the findings along with the sections they belong to, the rule ID, and a short description.

At the top of the report, you will find information about the Collector and Reporter run details, such as the data collection and report generation dates, along with the reporter version. Follows the Database Identity information, where you will find details about the target database. Then, the Summary table presents all the findings per section/ domain and their severity level.

Findings

DBSAT reporter resulting analysis is reported in units called Findings, and in each Finding, you see:

1. **Rule ID**: The Rule ID has two parts: the prefix identifies the report section, and the suffix identifies the specific rule.
2. **One-line summary**: One-line summary highlighting the objective and context of each check.

3. **Status**: The Status helps you prioritize implementing DBSAT recommendations. It indicates the level of risk associated with the finding, allowing you to make informed decisions about remediation.

    - **High Risk**
      Needs immediate attention.
    - **Medium Risk**
      Plan to address these in the short term.
    - **Low Risk**
      Might be fixed during scheduled downtime or bundled with other maintenance activities.
    - **Evaluate**
      Needs manual analysis.
    - **Advisory**
      Poses an opportunity for improvement and raises awareness about other security controls available in the Oracle Database.
    - **Pass**

      No risks were found.

4. **Summary**: Provides a summary of the Finding. When the Finding is informational, the summary typically reports only the number of examined data elements.
5. **Details**: Provides detailed information to explain the finding summary, typically results from the assessed database, followed by any recommendations for changes.
6. **Remarks**: Explain the reason for the rule and recommended actions for remediation.
7. **References**: If the finding is an Oracle Recommended Practice (ORP) related to an Oracle Database 19c STIG V1R1, Oracle Database 19c CIS Benchmark v1.2 recommendation, or related to a GDPR Article/Recitals, it will be mentioned here
8. **Documentation**: When the assessed Oracle Database is version 19c or 26ai, DBSAT will display documentation links relevant to each finding's remarks.

Security Frameworks and Recommended Practices

DBSAT integrates Oracle Recommended Practices, Center for Internet Security (CIS) Benchmark, and the US Department of Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) for the Oracle Database to identify potential security risks in Oracle databases.

Initially, DBSAT primarily focused on STIGs and CIS benchmarks, but with version 3.0 and later, it also highlights findings aligned or that are Oracle's own recommended practices.

Some checks are designated as Oracle Recommended Practices (ORP) only. This could be due to various factors, such as differences in release cycles or a deeper understanding of Oracle's inner workings. For example, while Oracle releases new features or capabilities, it can take years for standards to include them. For instance,

Oracle introduced Gradual Password Rollover in Oracle Database 19c in 2021, but until April 2024, it wasn’t reflected in STIG or CIS.

Multiple security frameworks often cover similar requirements, and DBSAT tags findings accordingly. For instance, if both CIS and STIG recommend avoiding default passwords for database user accounts, DBSAT marks that finding with both frameworks' tags, and as this is an Oracle recommended practice, it would be as well flagged with the ORP tag.

DBSAT's tagging system lets users focus on findings relevant to their compliance standards. Whether seeking STIG compliance, adherence to CIS benchmark, or alignment with Oracle's best practices, users can easily find and prioritize findings based on their specific requirements.

DBSAT maps findings to:

- STIG 19c V1R1
- Oracle Database 19c CIS Benchmark v1.2.
- Oracle Recommended Practices
- European Union General Data Protection Regulation (EU GDPR) 2016/679 articles and recitals

> **Note**
>
> Recommendations reflect best practices for database security and should be part of any strategy for data protection by design and by default.
>
> EU GDPR tagged findings highlight technology that may help you address EU GDPR articles and recitals and other data privacy regulations with similar requirements. Technical controls alone are not sufficient for compliance. Passing all findings does not guarantee compliance.

Sections

DBSAT Security Assessment report starts with a Summary and follows with findings organized in the following categories:

- Database Security Basics
- User Accounts
- Privileges and Roles
- Auditing
- Encryption
- Authorization Control
- Fine-Grained Access Control
- Database Configuration
- Network Configuration

- Operating System

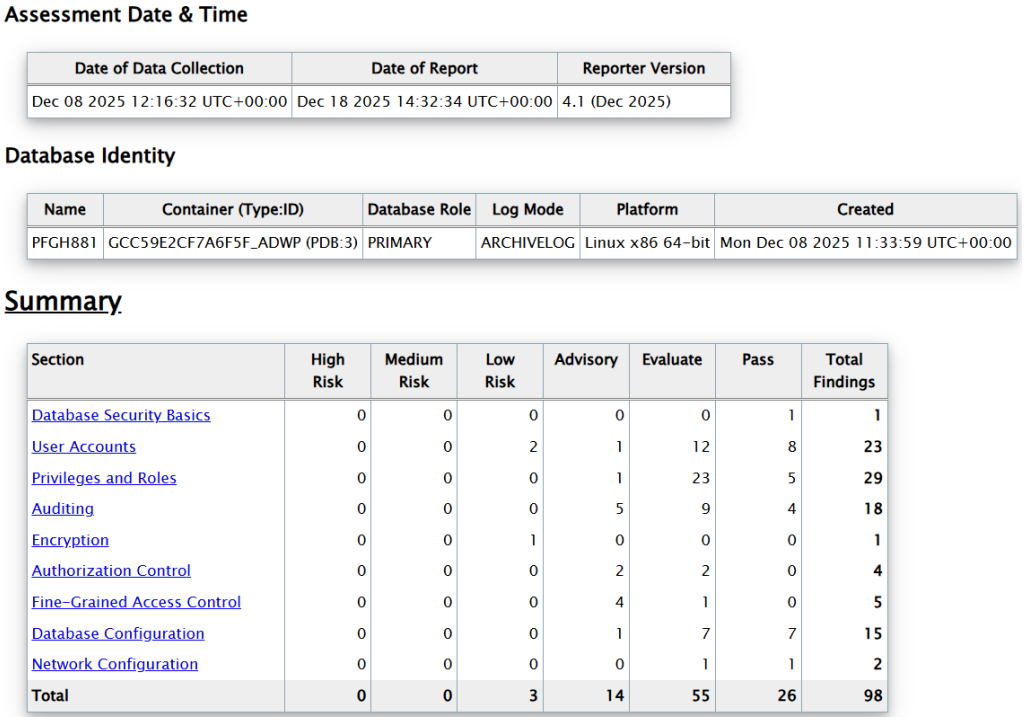
Oracle Database Security Assessment Report — Summary

The Oracle Database Security Assessment Report — Summary section contains the following information:

Section	Description
Assessment Date & Time	Displays the date on which the data was collected and the date on which the final Database Security Assessment report was generated. The DBSAT Reporter version is also displayed.
Database Identity	Displays the details of the database assessed by DBSAT.
Summary	Displays a high level summary of the resulting analysis.

The following figure displays an example of the Oracle Database Security Assessment Report — Summary section.

Figure 1-3 Oracle Database Security Assessment Report - Summary



Assessment Date & Time

Date of Data Collection	Date of Report	Reporter Version
Dec 08 2025 12:16:32 UTC+00:00	Dec 18 2025 14:32:34 UTC+00:00	4.1 (Dec 2025)

Database Identity

Name	Container (Type:ID)	Database Role	Log Mode	Platform	Created
PFGH881	GCC59E2CF7A6F5F_ADWP (PDB:3)	PRIMARY	ARCHIVELOG	Linux x86 64-bit	Mon Dec 08 2025 11:33:59 UTC+00:00

Summary

Section	High Risk	Medium Risk	Low Risk	Advisory	Evaluate	Pass	Total Findings
Database Security Basics	0	0	0	0	0	1	1
User Accounts	0	0	2	1	12	8	23
Privileges and Roles	0	0	0	1	23	5	29
Auditing	0	0	0	5	9	4	18
Encryption	0	0	1	0	0	0	1
Authorization Control	0	0	0	2	2	0	4
Fine-Grained Access Control	0	0	0	4	1	0	5
Database Configuration	0	0	0	1	7	7	15
Network Configuration	0	0	0	0	1	1	2
Total	**0**	**0**	**3**	**14**	**55**	**26**	**98**

The Summary section is followed by the Database Security Basics section.

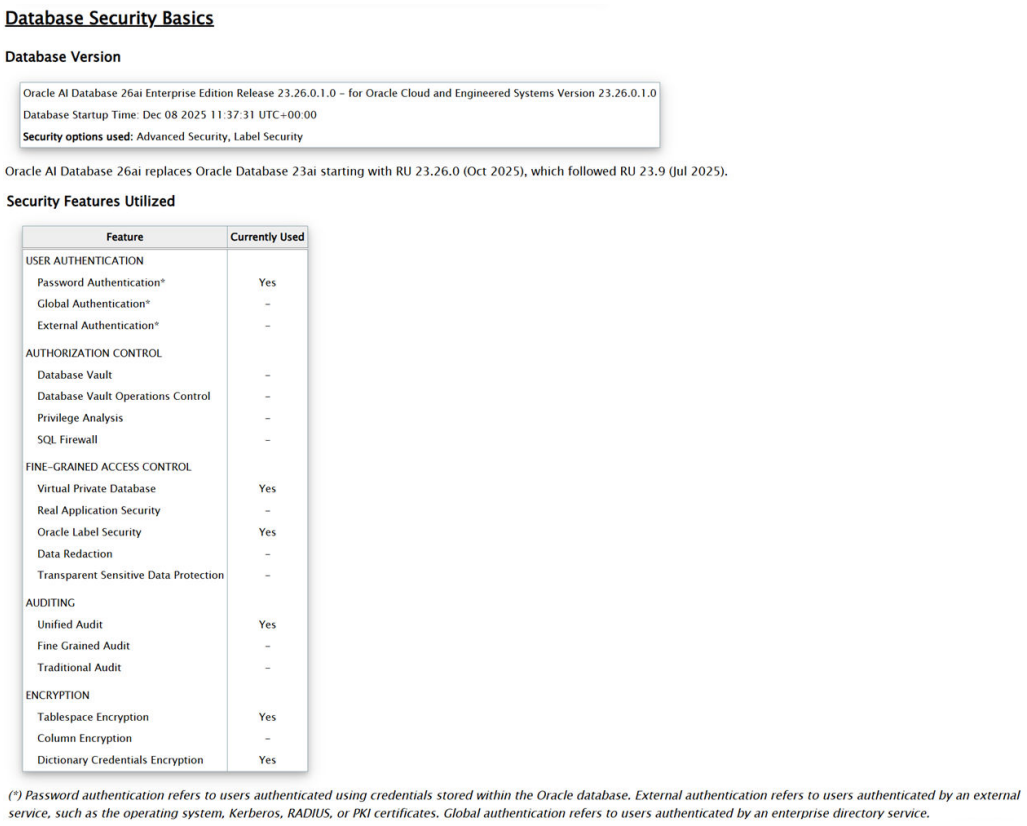
Oracle Database Security Assessment Report — Database Security Basics

The Oracle Database Security Assessment Report — Database Security Basics section contains the following information:

Section	Finding ID	Description	Link(s)
Database Version	-	Displays the version of the database assessed by the Collector and Reporter. Includes security options used and database startup time.	-
Security Features Utilized	-	Displays the security features and indicates if they are in use.	-
Patch Check	INFO.PATCH	Displays information about the patches installed and the CVEs the database is exposed to. It is vital to keep the database software up-to-date with security fixes as they are released. Oracle issues comprehensive patches in the form of Release Updates on a regular quarterly schedule. Patch Set Updates and Bundle Patches were available for database versions up to 12.1.0.2.	• Download Security Patches • View Patch and Maintenance window information • Map of CVE to Advisory/Alert

The following figure displays an example of the Oracle Database Security Assessment Report — Database Security Basics section.

Figure 1-4 Oracle Database Security Assessment Report -Database Security Basics



Database Security Basics

Database Version

Oracle AI Database 26ai Enterprise Edition Release 23.26.0.1.0 – for Oracle Cloud and Engineered Systems Version 23.26.0.1.0
Database Startup Time: Dec 08 2025 11:37:31 UTC+00:00
Security options used: Advanced Security, Label Security

Oracle AI Database 26ai replaces Oracle Database 23ai starting with RU 23.26.0 (Oct 2025), which followed RU 23.9 (Jul 2025).

Security Features Utilized

Feature	Currently Used
USER AUTHENTICATION	
Password Authentication*	Yes
Global Authentication*	–
External Authentication*	–
AUTHORIZATION CONTROL	
Database Vault	–
Database Vault Operations Control	–
Privilege Analysis	–
SQL Firewall	–
FINE-GRAINED ACCESS CONTROL	
Virtual Private Database	Yes
Real Application Security	–
Oracle Label Security	Yes
Data Redaction	–
Transparent Sensitive Data Protection	–
AUDITING	
Unified Audit	Yes
Fine Grained Audit	–
Traditional Audit	–
ENCRYPTION	
Tablespace Encryption	Yes
Column Encryption	–
Dictionary Credentials Encryption	Yes

(*) Password authentication refers to users authenticated using credentials stored within the Oracle database. External authentication refers to users authenticated by an external service, such as the operating system, Kerberos, RADIUS, or PKI certificates. Global authentication refers to users authenticated by an enterprise directory service.

The Database Security Basics section is followed by the User Accounts section.

Oracle Database Security Assessment Report — User Accounts

The Oracle Database Security Assessment Report — User Accounts section displays the following information:

Name	Finding ID	Description	Link(s)
User Accounts	-	Displays the user accounts and the following information about each account: • User Name — Displays the name of the user. • Profile — Displays the profile assigned to the account. • Status — Displays whether the account is, for example, Open, Locked, Expired, or in Rollover. • Authentication Type — Displays the type of authentication used. • Default Tablespace — Displays the default tablespace for the account. • Oracle Defined — Displays whether the user account is oracle maintained or not. • Read Only — Displays whether the account is read-only or not. • Last Password Change — Displays the last date and time the user's password was changed.	-
Users with DEFAULT Profile	USER.DEFAULTPROFILE	Displays the DEFAULT user profile password and resource parameters and the number of users in it.	• Assigning a Profile to a User • Query to List All Profiles and Assigned Limits
Users with Default Passwords	USER.DEFPWD	Displays information about the user accounts with default passwords. Default account passwords for predefined Oracle accounts are well known. Active accounts with default passwords provide a trivial means of entry for attackers, but well-known passwords should be changed for locked accounts as well.	• Guidelines for Securing Passwords • Finding User Accounts That Have Default Passwords • Configuring Authentication • DBA_USERS_WITH_DEFPWD

Name	Finding ID	Description	Link(s)
Users with Expired Passwords	USER.EXPIRED	Displays information about the user accounts with expired passwords. Password expiration is used to ensure that users change their passwords regularly. Unlocked accounts with an expired password can present a security risk, especially as those accounts age. Although the password is expired, because the account is unlocked, it can easily be used by anyone who knows the old password. You should investigate accounts that have been unused for an extended period to determine whether they should remain active.	• About Controlling Password Aging and Expiration • Password Change Lifecycle • Query to List All Profiles and Assigned Limits
Inactive Users	USER.INACTIVE	Displays information about the user accounts that are not in use and also accounts that are not configured to be locked when inactive. If a user account is no longer in use, it increases the attack surface of the system unnecessarily while providing no corresponding benefit. Furthermore, unauthorized use is less likely to be noticed when no one is regularly using the account. Accounts that have been unused for more than 30 days should be investigated to determine whether they should remain active. A solution is to set `INACTIVE_ACCOUNT_TIME` in the profiles assigned to users.	• Automatically Locking Inactive Database User Accounts • Logon and Logoff Predefined Unified Audit Policy • Query to List All Profiles and Assigned Limits
Sample Schemas	USER.SAMPLE	Displays information about potential sample schemas in the database, such as `SCOTT`, `HR`, `OE`, `SH`, `PM`, `IX`, `ADAMS`, `BLAKE`, `CLARK`, and `BI`. Sample schemas are well-known accounts provided by Oracle to serve as simple examples for developers. They generally serve no purpose in a production database and should be removed because they unnecessarily increase the attack surface of the database.	• Predefined Schema User Accounts Provided by Oracle Database • Drop User • Uninstalling Sample Schemas • Use Sample Data Sets in Autonomous AI Database

Name	Finding ID	Description	Link(s)
Application Owner Account	USER.APPOWNER	Checks the database for the account that could be considered the application owner and for objects accessible by the application owner. Any user not "oracle maintained" that owns most objects in the database is considered the Application Owner. This check: • Lists application owners • Lists users who can login into database • Lists app owners and the objects owned by it along with the non-app owners who can access those objects	• Schema-only accounts
Shared Accounts	USER.SHARED	Displays users that have multiple administrative privileges and proxy users.	• About Proxy Authentication • Use of the DBMS_SESSION PL/SQL Package to Set and Clear the Client Identifier • SET_IDENTIFIER
Users with Objects	USER.OBJOWNER	Displays application users who own objects and can grant access to those objects to other users	• Data Dictionary Views That List Information About Users and Profiles
Users Authorized for Object Ownership	USER.OBJAUTHZ	Displays non-oracle maintained users who own objects	• Data Dictionary Views That List Information About Users and Profiles
Users with Security Objects	USER.SECURITYOBJS	Displays users who own security objects	• Data Dictionary Views That List Information About Users and Profiles
Users with Grant Option	USER.GRANTOPTION	Checks for users that have been granted privileges with `WITH GRANT OPTION`.	• Grant (SQL Reference)

Name	Finding ID	Description	Link(s)
Users with Sensitive Data	USER.SENSITVEDATA	Displays users that own tables with columns marked as sensitive with TSDP and users that can access those tables. To ensure secure access to sensitive information, review these users. It is best to grant access to data through roles rather than directly to individual accounts.	• Using Transparent Sensitive Data Protection
User Schemas in SYSTEM or SYSAUX Tablespace	USER.TABLESPACE	Displays information about regular user accounts that use reserved Oracle-supplied tablespaces as their default tablespace or that have objects stored in them. The SYSTEM and SYSAUX tablespaces are reserved for Oracle-supplied user accounts. To avoid a possible denial of service caused by exhausting these resources, regular user accounts should not use these tablespaces. Prior to Oracle Database 12c Release 2 (12.2), the SYSTEM tablespace cannot be encrypted, and this is another reason to avoid user schemas in this tablespace.	• Managing the SYSAUX tablespace • Altering user accounts • Default Tablespace for the User
Case-Sensitive Passwords	USER.PASSWORDCASE	Displays whether case-sensitive passwords are enabled. Case-sensitive passwords are recommended because including both upper and lower-case letters greatly increases the set of possible passwords that must be searched by an attacker who is attempting to guess a password by exhaustive search. Setting SEC_CASE_SENSITIVE_LOGON to TRUE ensures that the database distinguishes between upper and lower-case letters in passwords. **Note**: In 21c USER.PASSWORDCASE is not expected to be shown as SEC_CASE_SENSITIVE_LOGON because it is desupported.	• Default Tablespace for the User

Name	Finding ID	Description	Link(s)
Legacy Password Versions	USER.AUTHLEGACY	Displays information about the user accounts with obsolete password verifiers. For each user account, the database may store multiple verifiers, which are hashes of the user password. Each verifier supports a different version of the password authentication algorithm. Every user account should include a verifier for the latest password version supported by the database so that the user can be authenticated using the latest algorithm supported by the client. When all clients have been updated, the security of user accounts can be improved by removing the obsolete verifiers. HTTP password verifiers are used for XML Database authentication. Use the ALTER USER command to remove these verifiers from user accounts that do not require this access.	• Management of Password Versions of Users
User Profiles	-	Displays information about the user profiles.	-
Users with no Password Complexity Requirements	USER.PASSWORDFUNCTION	Displays information about profiles with and without a password complexity verification function. Users not subject to password complexity verification are also displayed. Password verification functions are used to ensure that user passwords meet minimum requirements for complexity, which may include factors such as length, use of numbers or punctuation characters, difference from previous passwords, etc. Oracle supplies several predefined functions, or a custom PL/SQL function can be used. Every user profile should include a password verification function.	• Managing the Complexity of passwords

Name	Finding ID	Description	Link(s)
Account Locking after Failed Login Attempts	USER.NOLOCK	Displays information about user profile failed login attempt enforcement. Attackers sometimes attempt to guess a user's password by simply trying all possibilities from a set of common passwords. To defend against this attack, it is advisable to use the `FAILED_LOGIN_ATTEMPTS` and `PASSWORD_LOCK_TIME` profile resources to lock user accounts for a specified time when there are multiple failed login attempts without a successful login.	• ALTER PROFILE • Automatically Locking User Accounts After a Specified Number of Failed Log-in Attempts • Query to List All Profiles and Assigned Limits • User Profiles in ADB-S
Users with Passwords About to Expire	USER.TOEXPIRE	Displays information about user accounts that will expire their passwords within 30 days. You should review accounts about to expire and, if appropriate, change their passwords to maintain uninterrupted database access.	• About Controlling Password Aging and Expiration • Password Change Lifecycle
Users with Unlimited Password Lifetime	USER.NOEXPIRE	Displays information about user profile password expiration enforcement. Password expiration is used to ensure that users change their passwords on a regular basis. It also provides a mechanism to automatically disable temporary accounts. Passwords that never expire may remain unchanged for an extended period of time. When passwords do not have to be changed regularly, users are also more likely to use the same passwords for multiple accounts.	• About Controlling Password Aging and Expiration • Password Management • Query to List All Profiles and Assigned Limits • User Profiles in ADB-S
Users with Unlimited Concurrent Sessions	USER.SESSIONS	Displays all users that have a Profile Resource Limit for `SESSIONS_PER_USER` set to `UNLIMITED`. With `SESSIONS_PER_USER = UNLIMITED` users can have any number of concurrent sessions.	• ALTER PROFILE • Query to List All Profiles and Assigned Limits • User Profiles in ADB-S

Name	Finding ID	Description	Link(s)
Unlimited Session Idle Time	USER.IDLETIME	This check lists users with UNLIMITED IDLE TIME	• ALTER PROFILE • Configure user resource limits • Query to List All Profiles and Assigned Limits • User Profiles in ADB-S
Users with Gradual Password Rollover	USER.PASSWORDROLLOVER	Displays information about the Gradual Password Rollover. Gradual Password Rollover allows administrators to change database passwords for applications without having to schedule downtime. Prior to the advent of the gradual password rollover feature, the database administrator needed to take the application down while the database password was being rotated. This was because the password update required changes on both the database and the application side. With gradual database password rollover, the application can continue to use the older password until the new password is configured in the application. To accomplish this, the database administrator can associate a profile having a non-zero limit for the `PASSWORD_ROLLOVER_TIME` password profile parameter with an application schema. This allows the database password of the application user to be altered while allowing the older password to remain valid for the time specified by the `PASSWORD_ROLLOVER_TIME` limit. Try to limit the use of this feature to application schemas that need to undergo password maintenance and keep the rollover period to the minimum.	• ALTER PROFILE • Managing Gradual Password Rollover for Applications • Query to List All Profiles and Assigned Limits • Profiles in ADB-S

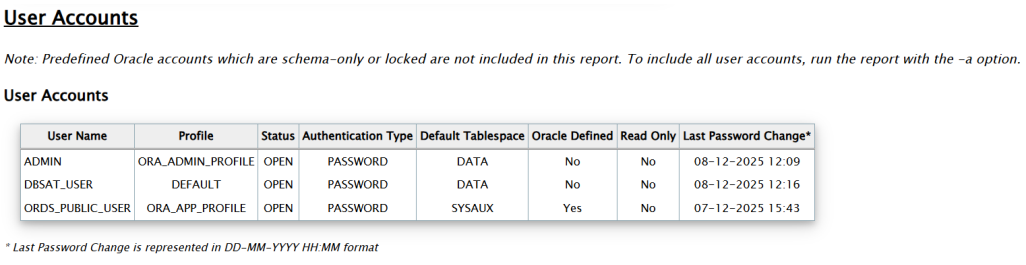
Name	Finding ID	Description	Link(s)
Temporary Users	USER.TEMP	Displays users associated with the DEFAULT profile. Users specifically created to execute temporary tasks should be on a profile tailored for that purpose.	• Automatically Locking Inactive Database User Accounts • Create profile • Alter user • Query to List All Profiles and Assigned Limits • Remove Users • Managing User Profiles in ADB
Development Users in Production Databases	USER.DEV	There should not be developer accounts in production systems. Verify if such accounts exist in your database.	• Command Rule That Allows Actions from Specified IP Addresses Only • Drop user
Advanced Replication Users	USER.REPCAT	Checks if Oracle Advanced Replication is being used and lists the dblinks used for replication. Checks to see if `enable_goldengate_replication` is set to `TRUE`. Also checks if `DBA_REPCAT%` views are present or `count(*) from DBA_REPCATLOG > 0`.	-
Minimum Client Authentication Version	USER.AUTHVERSION	Displays information about the user accounts that do not have minimum client version specified in the `ALLOWED_LOGON_VERSION_SERVER` parameter in the `sqlnet.ora` file. Over time, Oracle releases have added support for increasingly secure versions of the algorithm used for password authentication of user accounts. In order to remain compatible with older client software, the database continues to support previous password versions as well. The `sqlnet.ora` parameter `ALLOWED_LOGON_VERSION_SERVER` determines the minimum password version that the database will accept. For maximum security, this parameter should be set to the highest value supported by the database once all client systems have been upgraded.	• SQLNET.ALLOWED_LOGON_VERSION_SERVE • SQLNET.ALLOWED_LOGON_VERSION_CLIENT

Name	Finding ID	Description	Link(s)
New Users Who Need to Reset Password	USER.NEW	Displays information about user accounts who have not logged in since account creation. You should verify that the database management system is configured to require immediate selection of a new password upon account creation or recovery.	No documentation links
Locally Managed Accounts	USER.LOCALAUTH	This is a STIG speficic check. Displays information about non-oracle maintained accounts that are locally managed (use password-based authentication). Under STIG, all user accounts managed by the database need to have explicit approval and be in the system documentation. System documentation should be reviewed for justification and approval of the accounts listed.	No documentation links
PKI-based Authentication	USER.EXTERNALAUTH	Displays information about externally authenticated user accounts.	No documentation links

> **Note**
>
> Predefined Oracle accounts which are schema-only or locked are not included in this report. To include all user accounts, run the report with the `-a` option.

The following figure displays an example of the Oracle Database Security Assessment Report — User Accounts section.

Figure 1-5 Oracle Database Security Assessment Report - User Accounts



User Accounts

Note: Predefined Oracle accounts which are schema-only or locked are not included in this report. To include all user accounts, run the report with the -a option.

User Accounts

User Name	Profile	Status	Authentication Type	Default Tablespace	Oracle Defined	Read Only	Last Password Change*
ADMIN	ORA_ADMIN_PROFILE	OPEN	PASSWORD	DATA	No	No	08-12-2025 12:09
DBSAT_USER	DEFAULT	OPEN	PASSWORD	DATA	No	No	08-12-2025 12:16
ORDS_PUBLIC_USER	ORA_APP_PROFILE	OPEN	PASSWORD	SYSAUX	Yes	No	07-12-2025 15:43

** Last Password Change is represented in DD-MM-YYYY HH:MM format*

The User Accounts section is followed by the Privileges and Roles section.

Oracle Database Security Assessment Report — Privileges and Roles

The Oracle Database Security Assessment Report — Privileges and Roles section displays the following information:

Name	Finding ID	Description	Link(s)
Access to Password Verifier Tables	PRIV.ACCESSVERIFIERS	Displays access to password verifier tables granted to users. Users with these privileges can access objects that contain user password verifiers. The verifiers can be used in offline attacks to discover user passwords.	• Revoke object privileges
Users with Administrative Privileges SYS* Privileges	PRIV.SYSADMIN	Displays the administrative privileges granted to user accounts. Administrative privileges allow a user to perform maintenance operations, including some that may occur while the database is not open. The SYSDBA privilege allows the user to run as SYS and perform virtually all privileged operations. Starting with Oracle Database 12c Release 1 (12.1), less powerful administrative privileges were introduced to allow users to perform common administrative tasks with less than full SYSDBA privileges. To achieve the benefit of this separation of duty, each of these administrative privileges should be granted to at least one user account.	• Administrative Privileges • Managing Administrative Privileges • Granting and Revoking Administrative Privileges
Users with DBA Role	PRIV.DBA	Displays the user accounts that have been granted the DBA or PDB_DBA role. The DBA role is very powerful and can be used to bypass many security protections. It should be granted to only a small number of trusted administrators. Furthermore, each trusted user should have an individual account for accountability reasons. As with any powerful role, avoid granting the DBA role with admin option unless absolutely necessary.	• Performing Privilege Analysis to Identify Privilege Use • Administrative User Accounts • Revoke

Name	Finding ID	Description	Link(s)
Users with Powerful Roles	PRIV.BIGROLES	Displays the user accounts that have been granted roles with maximum data access privileges. Like the DBA role, these roles (`AQ_ADMINISTRATOR_ROLE`, `EM_EXPRESS_ALL`, `EXP_FULL_DATABASE`, `IMP_FULL_DATABASE`, `SELECT_CATALOG_ROLE`, `EXECUTE_CATALOG_ROLE`, `DELETE_CATALOG_ROLE`, `OEM_MONITOR`, `DBA`, `AUDIT_VIEWER`) contain powerful privileges that can be used to bypass security protections. They should be granted only to a small number of trusted administrators.	• Users With System Privileges • Granting and Revoking Administrative Privileges
System Privilege Grants	PRIV.SYSTEM	Displays the system privileges granted to users. System privileges provide the ability to access data or perform administrative operations for the entire database. Consistent with the principle of least privilege, these privileges should be granted sparingly. System privileges should be granted with admin option only when the recipient needs the ability to grant the privilege to others. `-g` option reports all grants including common grants in a PDB. The report displays `(*)` for privileges being granted with admin option, `(D)` for privileges being granted directly, and `(C)` for privileges being granted commonly.	• Users With System Privileges • Revoke
Schema Privilege Grants	PRIV.SCHEMA	Displays information about user accounts with ANY system privileges and schema-level grants. This will allow reviewing cases where `SELECT ANY TABLE` system privilege was granted to simplify management and replace them with schema-level grants instead.	• Managing Schema Privileges • Revoke
System Privileges Granted to PUBLIC	PRIV.SYSPUBLIC	Displays the system privileges granted to `PUBLIC`. Privileges granted to `PUBLIC` are available to all users. This generally should include few, if any, system privileges since these will not be needed by ordinary users who are not administrators.	• ANY Privileges and the PUBLIC Role • Revoke • PUBLIC role

Name	Finding ID	Description	Link(s)
Roles Granted to PUBLIC	PRIV.ROLEPUBLIC	Displays the roles granted to PUBLIC. Roles granted to PUBLIC are available to all users. Most roles contain privileges that are not appropriate for all users.	• Grants to PUBLIC on a CDB • How the PUBLIC Role Works in a Multitenant Environment • PUBLIC role
Column Privileges Granted to PUBLIC	PRIV.COLPUBLIC	Displays the column access privileges granted to PUBLIC. Privileges granted to PUBLIC are available to all users. This should include column privileges only for data that is intended to be accessible to everyone.	• Grants and Revokes of Privileges to and from the PUBLIC Role • PUBLIC role
Objects Accessible by PUBLIC	PRIV.OBJPUBLIC	Displays objects that are accessible by PUBLIC.	• Grants and Revokes of Privileges to and from the PUBLIC Role • PUBLIC role
Encryption Packages Granted to PUBLIC	PRIV.ENCRYPTPACKAGEPUBLIC	Displays DBMS_CRYPTO, DBMS_OBFUSCATION_TOOLKIT, and DBMS_RANDOM grants to PUBLIC.	• DBMS_CRYPTO • DBMS_RANDOM • PUBLIC role
Scheduler Job Packages Granted to PUBLIC	PRIV.JOBSCHPACKAGEPUBLIC	Display DBMS_SCHEDULER and DBMS_JOB EXECUTE grants to PUBLIC and Scheduler/Job system privileges (CREATE JOB, MANAGE SCHEDULER, CREATE EXTERNAL JOB, CREATE ANY JOB) grants to PUBLIC.	• Grants and Revokes of Privileges to and from the PUBLIC Role • PUBLIC role
Credential Package Granted to PUBLIC	PRIV.CREDPACKAGEPUBLIC	Displays EXECUTE grant on DBMS_CREDENTIAL package to PUBLIC. Also checks for privilege grants of CREATE CREDENTIAL and CREATE ANY CREDENTIAL to users.	• DBMS_CREDENTIAL • Grants and Revokes of Privileges to and from the PUBLIC Role • PUBLIC role
File System Packages Granted to PUBLIC	PRIV.FILESYSTEMPACKAGEPUBLIC	Displays EXECUTE grant on DBMS_LOB, UTL_FILE, and DBMS_ADVISOR packages to PUBLIC. Also checks for system privilege grants of CREATE ANY DIRECTORY and DROP ANY DIRECTORY to users.	• Grants and Revokes of Privileges to and from the PUBLIC Role • PUBLIC role

Name	Finding ID	Description	Link(s)
Network Packages Granted to PUBLIC	PRIV.NETPACKAGEPUBLIC	Displays EXECUTE grant on DBMS_LDAP, UTL_HTTP, UTL_INADDR, UTL_SMTP, and UTL_TCP packages to PUBLIC. Also checks for users that are authorized to execute packages via ACLs.	• Managing Fine-Grained Access in PL/SQL Packages and Types • Grants and Revokes of Privileges to and from the PUBLIC Role • PUBLIC role
SQL Packages Granted to PUBLIC	PRIV.QUERYPACKAGEPUBLIC	Displays EXECUTE grant on DBMS_XMLQUERY, DBMS_XMLSAVE, DBMS_XMLSTORE, DBMS_REDACT, DBMS_XMLGEN, and DBMS_SQL packages to PUBLIC.	• DBMS_SQL • DBMS_XMLGEN deprecation • PUBLIC role
Oracle JAVA Permissions Granted to PUBLIC	PRIV.JAVAPACKAGEPUBLIC	Displays EXECUTE grant on DBMS_JAVA and DBMS_JAVA_TEST packages to PUBLIC. Also checks for grants of JAVA_ADMIN role to users.	• Database Contents and Oracle JVM Security • DBMS_JAVA • Overview of Setting Permissions
Broad Data Access Privileges	PRIV.ANYSYSTEM	Displays information about user accounts that have been granted system privileges (ANY).	No documentation links
Access Privilege Grants	PRIV.CONTAINERACCESS	Displays information about common users with set container privilege grants. This check is only for CDB$ROOT.	• Switching to a Container Using the ALTER SESSION Statement • How the Oracle Multitenant Option Affects Privileges
All Roles	PRIV.ALLROLES	Displays all roles granted to users. Roles are a convenient way to manage groups of related privileges, especially when the privileges are required for a particular task or job function. Beware of broadly defined roles, which may confer more privileges than an individual recipient requires. Roles should be granted with admin option only when the recipient needs the ability to modify the role or grant it to others.	• Performing Privilege Analysis to Identify Privilege Use

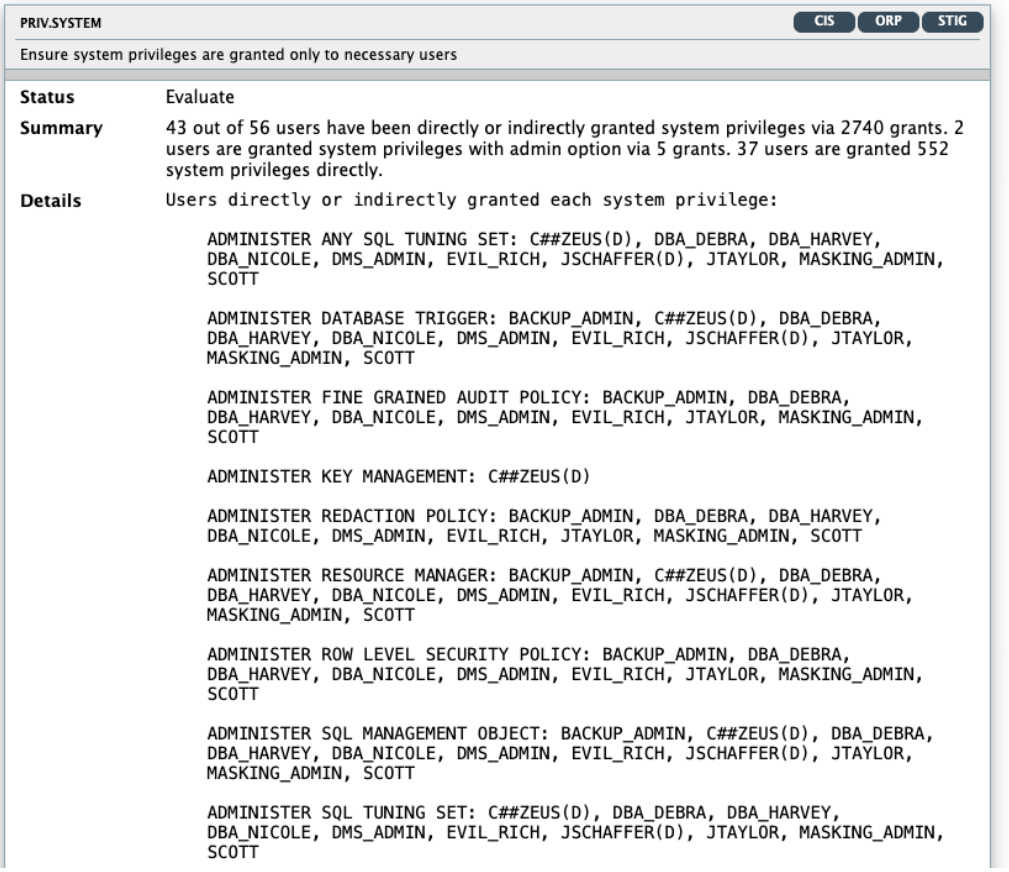
Name	Finding ID	Description	Link(s)
Account Management Privileges	PRIV.ACCOUNTMGMT	Displays account management privileges granted to users. User management privileges (`ALTER USER`, `CREATE USER`, `DROP USER`) can be used to create and modify other user accounts, including changing passwords. This power can be abused to gain access to another user's account, which may have greater privileges.	• Revoke
Role and Privilege Management Privileges	PRIV.ROLEPRIVMGMT	Displays privilege management privileges granted to users. Users with privilege management privileges (`ALTER ANY ROLE`, `CREATE ROLE`, `DROP ANY ROLE`, `GRANT ANY OBJECT PRIVILEGE`, `GRANT ANY PRIVILEGE`, `GRANT ANY ROLE`) can change the set of privileges granted to themselves and other users. This ability should be granted sparingly, since it can be used to circumvent many security controls in the database.	• Revoke
Database Management Privileges	PRIV.DBMGMT	Displays database management privileges granted to users. Database management privileges (`ALTER DATABASE`, `ALTER SYSTEM`, `CREATE ANY LIBRARY`, `CREATE LIBRARY`) can be used to change the operation of the database and potentially bypass security protections. This ability should be granted only to trusted administrators.	• Revoke
Audit Management Package	PRIV.AUDITMGMTPKG	Displays audit management tool access granted to users. The `DBMS_AUDIT_MGMT` package allow for execution of Audit management tools. Access should be strictly limited and granted only to users with a legitimate need for this functionality.	• Revoke • DBMS_AUDIT_MGMT
Audit Management Privileges	PRIV.AUDITMGMT	Displays audit management privileges granted to users. Audit management privileges (`AUDIT ANY`, `AUDIT SYSTEM`) can be used to change the audit policies for the database. This ability should be granted sparingly, since it may be used to hide malicious activity.	• Revoke

Name	Finding ID	Description	Link(s)
Access to Audit Objects	PRIV.ACCESSAUDITOBJ	Displays access to audit objects granted to users. Users with these privileges can directly access and modify objects containing audit information. Access to these objects may allow a malicious user deduce privilege settings for other users and to manipulate the audit information by replacing or deleting audit records.	• Revoke • Who Can Perform Auditing?
Access Control Exemption Privileges	PRIV.ACCESSEXEMPT	Displays access control exemption privileges that are enforced. Users with exemption privileges (`EXEMPT ACCESS POLICY`, `EXEMPT REDACTION POLICY`) can bypass the row and column access control policies enforced by Virtual Private Database and Data Redaction. Most administrative tasks do not require access to the data itself, so these privileges should be granted rarely even to administrators.	• Revoke • Oracle Virtual Private Database and Oracle Label Security Exceptions • Exemption of Users from Oracle Data Redaction Policies
Write Access to Restricted Objects	PRIV.RESTRICTEDOBJ	Displays access to restricted objects granted to users. Users with these privileges can directly modify objects in the `SYS`, `DVSYS`, `AUDSYS` or `LBACSYS` schemas. Manipulating these system objects may allow security protections to be circumvented or otherwise interfere with normal operation of the database. Object permissions granted to `PUBLIC` must be restricted for objects in the `SYS`, `DVSYS`, `AUDSYS` or `LBACSYS` schemas.	• Revoke
Users Who Can Impersonate Other Users	PRIV.IMPERSONATEUSER	Displays the user accounts that have been granted rights to impersonate other users. The `BECOME USER` privilege and these PL/SQL packages (`DBMS_AQADM_SYS`, `DBMS_AQADM_SYSCALLS`, `DBMS_IJOB`, `DBMS_PRVTAQIM`, `DBMS_REPCAT_SQL_UTL`, `DBMS_SCHEDULER`, `DBMS_STREAMS_ADM_UTL`, `DBMS_STREAMS_RPC`, `DBMS_SYS_SQL`, `INITJVMAUX`, `LTADM`, `WWV_DBMS_SQL`, `WWV_EXECUTE_IMMEDIATE`) allow for execution of SQL code or external jobs using the identity of a different user. Access should be strictly limited and granted only to users with a legitimate need for this functionality.	• Revoke • System Privileges (Organized by the Database Object Operated Upon)

Name	Finding ID	Description	Link(s)
Privilege for Data Exfiltration in Bulk	PRIV.EXFILTRATION	Displays the user accounts that have been granted rights to access or copy any data from a client or server. These PL/SQL packages (DBMS_BACKUP_RESTORE, UTL_DBWS, UTL_ORAMTS) can send data from the database using the network or file system. Access should be granted only to users with a legitimate need for this functionality.	• DBMS_FILE_TRANSFER • Revoke
Code Based Access Control	PRIV.CBAC	Displays all program units granted CBAC roles. Code Based Access Control(CBAC) can be used to grant additional privileges on program units. CBAC allows you to attach database roles to a PL/SQL function, procedure, or package. These database roles are enabled at run time, enabling the program unit to execute with the required privileges in the calling user's environment.	• Using CBAC for Definer's Rights and Invoker's Rights
Oracle Java Permissions	PRIV.JAVAPERMISSIONS	Displays the user accounts that have been granted privileges to run Oracle Java classes within the database. Oracle Java permission grants control the ability of database users to run Oracle Java classes within the database server. A database user running Oracle Java code must have both Oracle Java security permissions and database privileges to access resources within the database. These resources include database resources, such as tables and PL/SQL packages, operating system resources, such as files and sockets, Oracle JVM classes, and user-loaded classes. Make sure that these permissions are limited to the minimum required by each user.	-

The following figure displays an example of the Oracle Database Security Assessment Report — Privileges and Roles section.

Figure 1-6 Oracle Database Security Assessment Report — Privileges and Roles



The Privileges and Roles section is followed by the Auditing section.

Oracle Database Security Assessment Report — Auditing

The Oracle Database Security Assessment Report — Auditing section displays the following information:

Name	Finding ID	Description	Link(s)
Audit Management Configuration Parameters	-	Displays information on audit management configuration parameters	-

Name	Finding ID	Description	Link(s)
Audit Records	AUDIT.ENABLED	Displays information about audit trails. Auditing is an essential component for securing any system. The audit trail allows for monitoring the activities of highly privileged users.	• Unified Auditing and Its Benefits • Best Practices for Auditing
Unified Audit Policies	AUDIT.UNIFIED POLICIES	Displays whether unified audit policies are enabled. Unified Audit, available in Oracle Database 12c Release 1 (12.1) and later releases, combines multiple audit trails into a single unified view. It also introduces new syntax for specifying effective audit policies.	• Syntax for Creating a Custom Unified Audit Policy • Enabling and Applying Unified Audit Policies to Users and Roles
Fine Grained Audit	AUDIT.FGA	Displays whether fine grained audit policies are enabled. Fine Grained Audit policies can record highly specific activity, such as access to particular table columns or access that occurs under specified conditions. This is a useful way to monitor unexpected data access while avoiding unnecessary audit records that correspond to normal activity.	• Value-Based Auditing with Fine-Grained Audit Policies • DBMS_FGA
Audit Conditions	AUDIT.CONDITION	Lists all audit policies with conditions and, if enabled, lists users/roles it's enabled for.	• About Conditions in Unified Audit Policies
Audit Administrative (SYS*) Users	AUDIT.ADMINACTIONS	Displays whether the actions of the SYS user are audited by enabled audit policies. It is important to audit administrative actions performed by the SYS user. Traditional audit policies do not apply to SYS, so the `AUDIT_SYS_OPERATIONS` parameter must be set to record SYS actions to a separate audit trail.	• Auditing Administrative Users
Audit User Logon and Logoff	AUDIT.CONNECTIONS	Displays whether Database connections are audited by enabled audit policies. Successful user connections to the database should be audited to assist with future forensic analysis. Unsuccessful connection attempts can provide early warning of an attacker's attempt to gain access to the database.	• Logon and Logout Predefined Unified Audit Policy
Audit Database Management Activities	AUDIT.DBMGMT	Displays whether the actions related to database management are audited by enabled audit policies. Actions that affect the management of database features should always be audited. Each action or privilege listed should be included in at least one enabled audit policy.	-

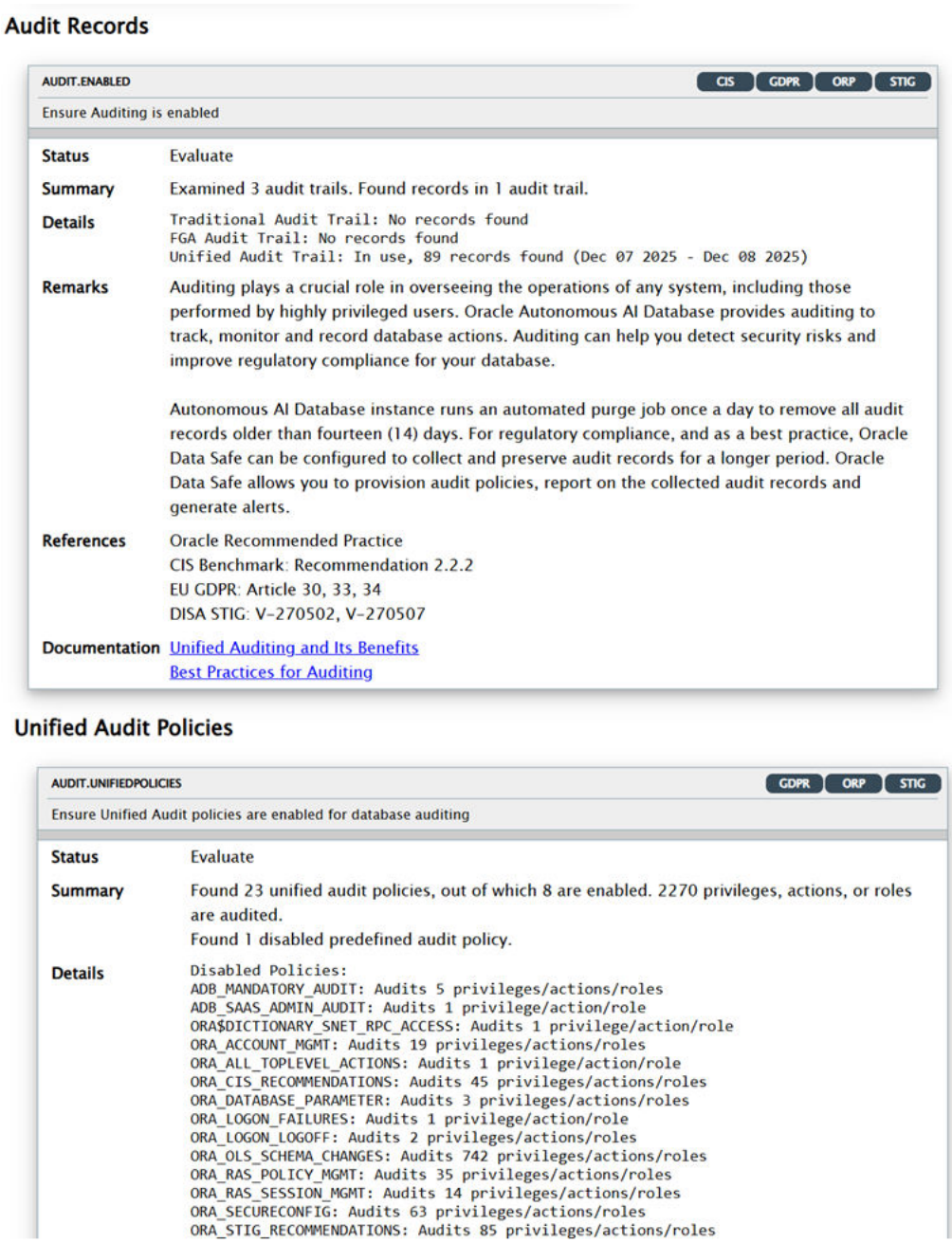
Name	Finding ID	Description	Link(s)
Audit Account Management Activities	AUDIT.ACCOUNTMGMT	Displays whether account management activities are audited.	• Secure Options Predefined Unified Audit Policy
Audit System Privileges	AUDIT.SYSTEMPRIVS	Displays information on whether system privileges are audited by enabled audit policies.	• Auditing System Privileges • System Privileges That Can Be Audited
Audit Roles with System Privileges	AUDIT.ROLESYSTEMPRIVS	Displays information about unified audit policies that audit roles with system privileges.	• Auditing Roles
Audit Privilege Management	AUDIT.PRIVMGMT	Displays whether the actions related to privilege management are audited by enabled audit policies. Granting additional privileges to users or roles potentially affects most security protections and should be audited. Each action or privilege listed should be included in at least one enabled audit policy.	• Secure Options Predefined Unified Audit Policy
Audit SQL Statements	AUDIT.STATEMENTS	Displays information about SQL statements audited by enabled audit policies. Applies to targets with Traditional Auditing policies.	-
Audit Object Actions	AUDIT.SENSITIVEOBJS	Displays information about the object access audited by enabled audit policies.	• Auditing Object Actions
Audit Synonym Management Activities	AUDIT.SYNONYMS	Displays information on whether synonym management activities (CREATE ANY SYNONYM, CREATE PUBLIC SYNONYM, CREATE SYNONYM, DROP PUBLIC SYNONYM, DROP SYNONYM) are audited.	-
Audit Conditions	AUDIT.CONDITION	Lists all audit policies with conditions and, if enabled, lists users/roles it's enabled for.	• About Conditions in Unified Audit Policies
Audit Shared Accounts	AUDIT.SHAREDPROXY	Checks to see if users listed in USER.SHARED are being audited.	• Auditing for Multitier or Multitenant Configurations
Audit Storage	AUDIT.TABLESPACE	Displays information about tablespaces used by different audit trails. Checks include: • Audit trail is SYSTEM • Audit trail is SYSAUX • Tablespace is non-autoextensible & 80% or more full (MEDIUM) • Tablespace is non-autoextensible & 90% or more full (HIGH)	• SET_AUDIT_TRAIL_LOCATION Procedure

Name	Finding ID	Description	Link(s)
Audit Trail Cleanup	AUDIT.CLEANUPJOBS	Lists enabled jobs that cleanup audit trails and checks cleanup jobs that are not present	• Purging Audit Trail Records • Auto Purge in Data Safe • AVDF - Audit Trail Cleanup
Audit Data Pump	AUDIT.DATAPUMP	Displays whether data pump exports and imports are being audited.	• Auditing Oracle Data Pump Events
Audit STIG Actions	AUDIT.STIGPOLICY	Oracle provides out-of-the-box audit policies that aim to answer DoD- auditable events requirements - `ORA_STIG_RECOMMENDATIONS`, `ORA_ALL_TOPLEVEL_ACTIONS` and `ORA_LOGON_LOGOFF`. This check will validate if these policies are audited.	• Auditing STIG
Audit Database Vault	AUDIT.DATABASEVAULT	Displays users that can administer Database Vault but are not audited and lists policies enabled to audit Database Vault actions	• Auditing Oracle Database Vault Events • Configuring a Unified Audit Policy for Oracle Database Vault
Audit Oracle Label Security	AUDIT.LABELSECURITY	Displays information regarding enabled audit policies used to audit OLS. • Checks to see if Oracle Label Security (OLS) is enabled and no audit policy is found with OLS action • Reports if OLS is enabled and audit policies were found for OLS actions	• Auditing Oracle Label Security Events

> **Note**
>
> The details of the audit findings can vary depending on whether the database has unified audit or traditional audit in place. Starting in Oracle Database 12c Release 2 (12.2), the best practice is to use Unified Audit. In addition, Traditional Audit has been desupported starting with Oracle Database 23ai.

The following figure displays an example of the Oracle Database Security Assessment Report — Auditing section.

Figure 1-7 Oracle Database Security Assessment Report — Auditing



The Auditing section is followed by the Encryption section.

Oracle Database Security Assessment Report — Encryption

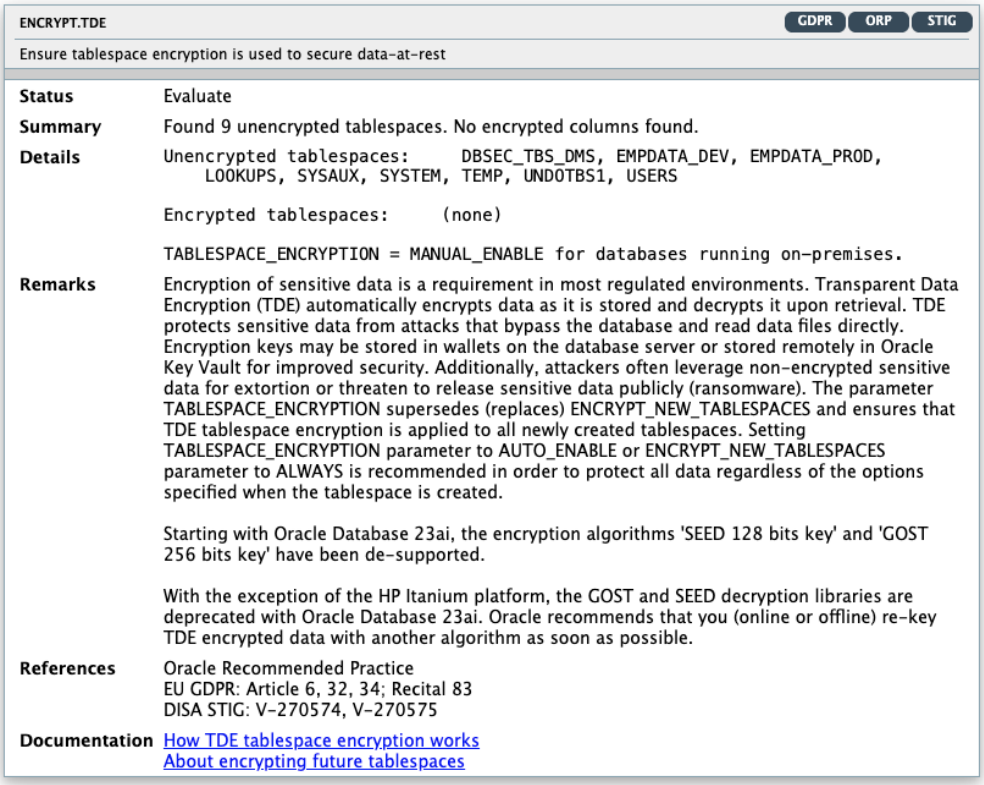
The Oracle Database Security Assessment Report — Encryption section displays the following information:

Name	Finding ID	Description	Link(s)
Transparent Data Encryption	ENCRYPT.TDE	Displays whether column or tablespace encryption is in use. Also, shows encrypted and unencrypted tablespaces along with the number of days since the master encryption key was last rotated. Encryption of sensitive data is a requirement in most regulated environments. Transparent Data Encryption automatically encrypts data as it is stored and decrypts it upon retrieval. This protects sensitive data from attacks that bypass the database and read data files directly.	• How TDE tablespace encryption works • About encrypting future tablespaces
Encryption Key Wallet	ENCRYPT.WALLET	Displays wallet information. Wallets are encrypted files used to store encryption keys, passwords, and other sensitive data. Wallet files should not be stored in the same directory with database data files, to avoid accidentally creating backups that include both encrypted data files and the wallet containing the master key protecting those files. For maximum separation of keys and data, consider storing encryption keys in Oracle Key Vault instead of wallet files.	• Introduction to Oracle Key Vault • Managing Oracle AI Database Wallets and Certificates • Migrating Existing TDE Wallets to Oracle Key Vault
FIPS Mode for TDE and DBMS_CRYPTO	ENCRYPT.DBFIPS	Displays information whether TDE and DBMS_CRYPTYO run in a FIPS-compliant mode. Federal Information Processing Standard (140-2) is a U.S. government security standard that specifies security requirements. It is used to approve cryptographic modules. Setting parameter DBFIPS_140 = TRUE enables Transparent Data Encryption (TDE) and DBMS_CRYPTO PL/SQL package program units to run in a FIPS-compliant mode. FIPS mode is mostly used by departments and agencies of the United States federal government looking to meet FIPS and/or STIG compliance. Be aware that this setting and thus using the underlying FIPS-certified library incurs a slight amount of overhead when the library is first loaded. This is due to the verification of the library signature and the execution of the self-test.	• DBFIPS_140 • Configuring FIPS 140-2 for Transparent Data Encryption and DBMS_CRYPTO

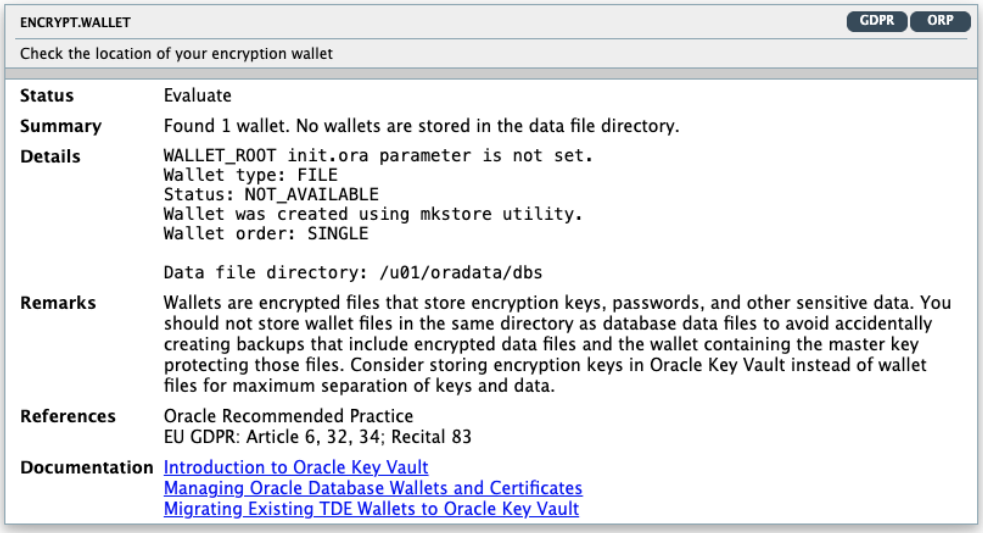
Name	Finding ID	Description	Link(s)
FIPS mode for TLS	ENCRYPT.TLSFIPS	Federal Information Processing Standard (140-2) is a U.S. government security standard that specifies security requirements. The SSLFIPS_140 parameter configures the Transport Layer Security (TLS) adapter to run in FIPS mode. SSLFIPS_LIB sets the location of the FIPS library.	• TLS Configuration for FIPS • Oracle Database FIPS 140-2 settings

The following figure displays an example of the Oracle Database Security Assessment Report — Encryption section.

Figure 1-8 Oracle Database Security Assessment Report — Encryption and Encryption Key Wallets



Encryption Key Wallet



ENCRYPT.WALLET GDPR ORP

Check the location of your encryption wallet

Status	Evaluate
Summary	Found 1 wallet. No wallets are stored in the data file directory.
Details	WALLET_ROOT init.ora parameter is not set. Wallet type: FILE Status: NOT_AVAILABLE Wallet was created using mkstore utility. Wallet order: SINGLE Data file directory: /u01/oradata/dbs
Remarks	Wallets are encrypted files that store encryption keys, passwords, and other sensitive data. You should not store wallet files in the same directory as database data files to avoid accidentally creating backups that include encrypted data files and the wallet containing the master key protecting those files. Consider storing encryption keys in Oracle Key Vault instead of wallet files for maximum separation of keys and data.
References	Oracle Recommended Practice EU GDPR: Article 6, 32, 34; Recital 83
Documentation	Introduction to Oracle Key Vault Managing Oracle Database Wallets and Certificates Migrating Existing TDE Wallets to Oracle Key Vault

The Encryption section is followed by the Authorization Control section.

Oracle Database Security Assessment Report — Authorization Control

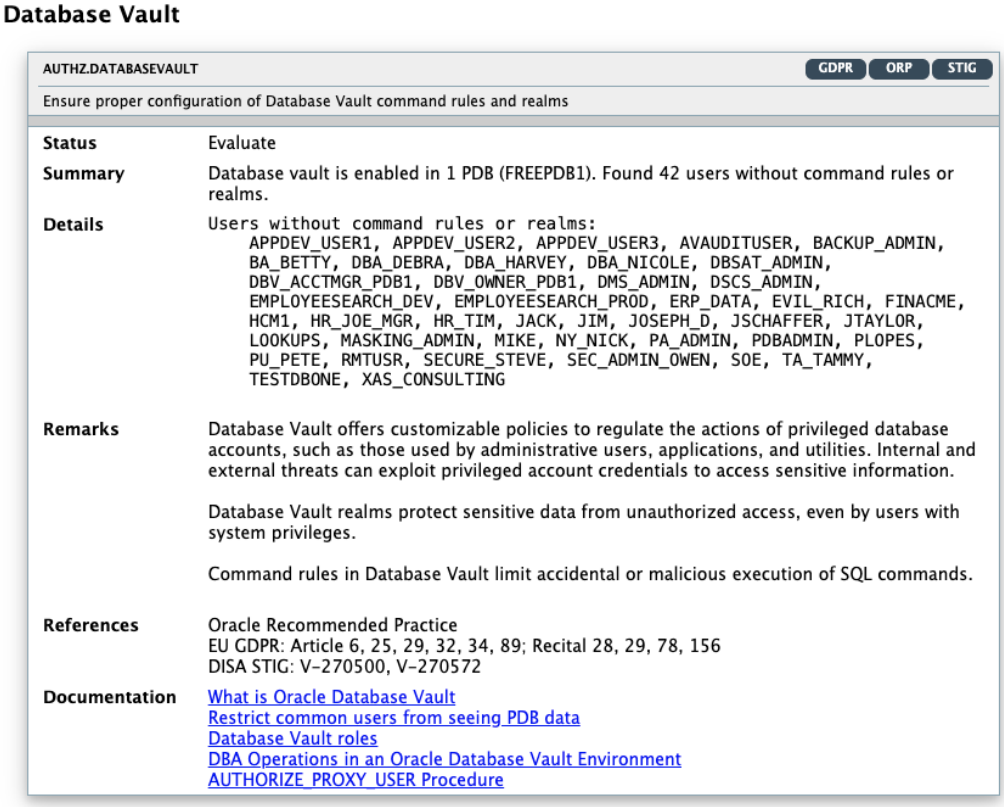
The Oracle Database Security Assessment Report — Authorization Control section displays the following information:

Name	Finding ID	Description	Link(s)
Database Vault	AUTHZ.DATABASEVAULT	Displays whether Oracle Database Vault is enabled, details realms, command rules, their status, and protected objects. Database Vault provides for configurable policies to control the actions of database accounts with elevated privileges such as those accounts used by administrative users, applications and utilities. Attacks (originating from external as well as internal sources) leverage privileged account credentials to access sensitive information. Database Vault realms prevent unauthorized access to sensitive data objects, even by user accounts with system privileges. Database Vault Command rules limit the accidental or malicious execution of SQL commands. Also it provides trusted paths to further restrict access to sensitive data using system factors such as IP address, program name, time of day and user name. Database Vault operations control can be used to restrict common users from accessing pluggable database (PDB) local data in autonomous, regular Cloud, or on-premises environments.	• What is Oracle Database Vault • Restrict common users from seeing PDB data • Database Vault roles • DBA Operations in an Oracle Database Vault Environment • AUTHORIZE_PROXY_USER Procedure

Name	Finding ID	Description	Link(s)
Database Vault Separation of Duty	AUTHZ.DATABASEVAULTSOD	Displays information about users with Database Vault-specific roles, including DV_OWER, DV_ACCTMGR, DV_PATCH_ADMIN, and others. It also verifies if users have been properly authorized for specific operations (e.g., Data Pump export/ import requires roles and a specific Database Vault authorization) and checks if Database Vault operation control is enabled.	• Performing Privilege Analysis to Identify Privilege Use • Who Can Perform Privilege Analysis • AUTHORIZE_PROXY_USER Procedure
Privilege Analysis	AUTHZ.PRIVANALYSIS	Displays Privilege Analysis policies and users with privileges to start the capture proces. Privilege Analysis records the privileges used during a real or simulated workload. After collecting data about the privileges that are actually used, this information can be used to revoke privilege grants that are no longer needed or to create roles with only the privileges that are used by the user or role. This helps implement Least Privilege Model and minimizes risk from intentional or accidental abuse of privileges.	• Performing Privilege Analysis to Identify Privilege Use • Who Can Perform Privilege Analysis • Use Database Vault with ADB-S
Authentication for Client Scripts	AUTHZ.PASSWORDSCRIPTS	Lists password-authenticated users whose passwords can potentially be embedded in client scripts, jobs, and application source code to connect to the database server.	• Managing Secrets and Credentials for SQL*Plus • Managing the Secure External Password Store for Password Credentials
Data Masking	AUTHZ.DATAMASKING	Lists tables with sensitive data that should be masked when transferred to non-production systems. This check lists tables marked sensitive by TSDP or in `DBA_TABLES` and users that can transfer data via `DATAPUMP_EXP_FULL_DATABASE` or `DATAPUMP_IMP_FULL_DATABASE`.	• Why Data Masking and Subsetting?

The following figure displays an example of the Oracle Database Security Assessment Report — Authorization Control section.

Figure 1-9 Oracle Database Security Assessment Report — Authorization Control



The Authorization Control section is followed by the Fine-Grained Access Control section.

Oracle Database Security Assessment Report — Fine-Grained Access Control

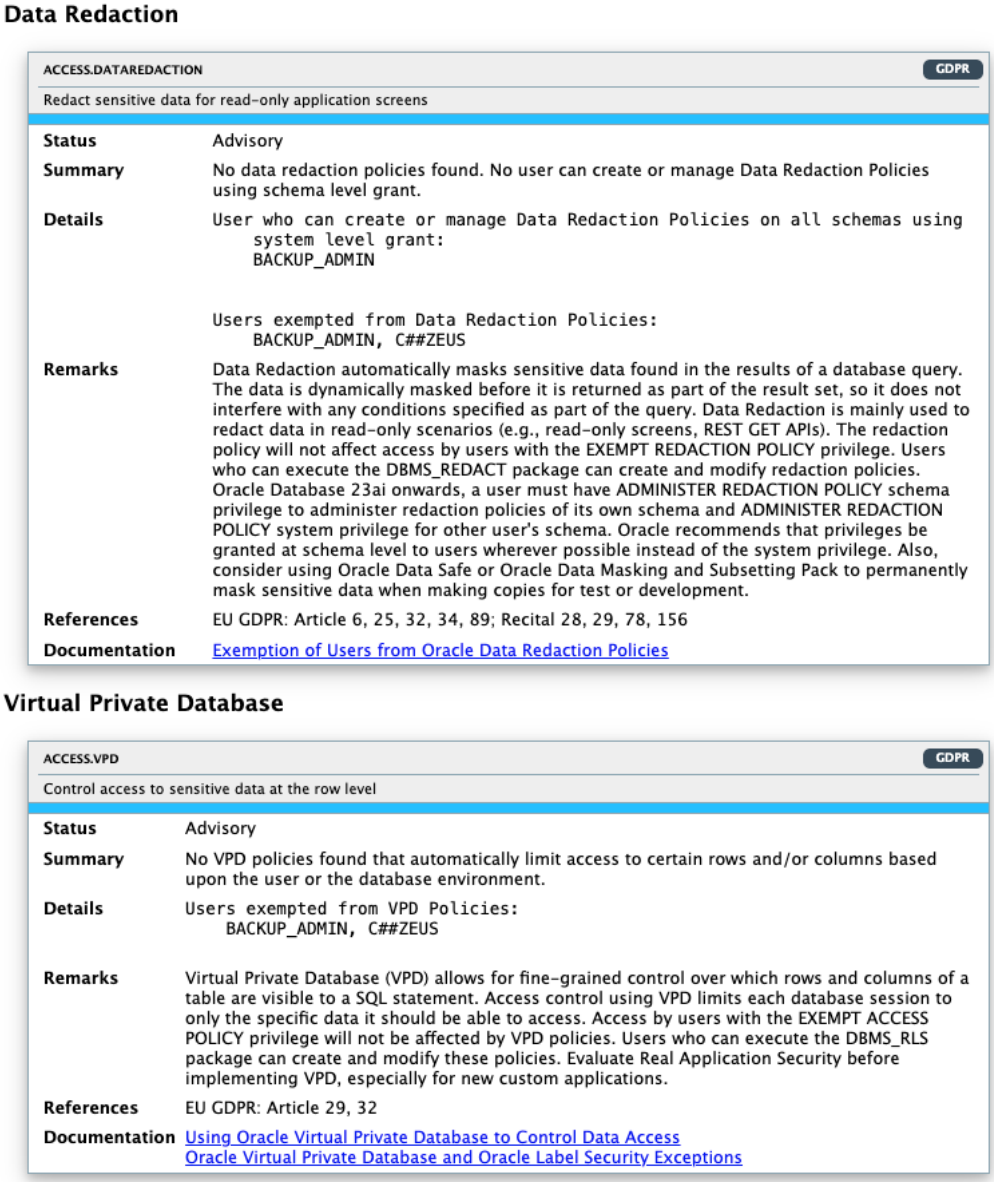
The Oracle Database Security Assessment Report — Fine-Grained Access Control section displays the following information:

Name	Finding ID	Description	Link(s)
Data Redaction	ACCESS.DATAREDACTION	Displays information on Data Redaction policies, exempted users, and execute grants on the DBMS_REDACT package. Data Redaction automatically masks sensitive data found in the results of a database query.	• What is Data Redaction • Oracle Data Redaction • Exemption of Users from Oracle Data Redaction Policies

Name	Finding ID	Description	Link(s)
Virtual Private Database	ACCESS.VPD	Displays information on Virtual Private Database policies, exempted users, and execute grants on the DBMS_RLS package. VPD allows for fine-grained control over the rows and columns of a table are visible to a SQL statement.	• Using Oracle Virtual Private Database to Control Data Access • Oracle Virtual Private Database and Oracle Label Security Exceptions
Real Application Security	ACCESS.RAS	Displays information on Real Application Security policies, exempted users, and users granted ADMIN_SEC_POLICY and APPLY_SEC_POLICY. Real Application Security (RAS) is a more modern, advanced version of Virtual Private Database and provides fine-grained control over the rows and columns of a table that are visible to a SQL statement.	• What is Real Application Security • About schema level RAS administration • Auditing RAS Events
Label Security	ACCESS.LABELSECURITY	Displays whether Oracle Label Security is enabled. Oracle Label Security provides the ability to tag data with a data label or a data classification. Access to sensitive data is controlled by comparing the data label with the requesting user's label or security clearance.	• About Oracle Label Security • Oracle Label Security • Exemptions from Oracle Label Security Enforcement
Transparent Sensitive Data Protection	ACCESS.TSDP	Displays information on Transparent Sensitive Data policies and the users that can manage it. TSDP was introduced in Oracle Database 12c Release 1 (12.1), and allows a data type to be associated with each column that contains sensitive data. TSDP can then apply various data security features to all instances of a particular type so that protection is uniform and consistent.	• Transparent Sensitive Data Protection

The following figure displays an example of the OracleDatabase Security Assessment Report — Fine-Grained Access Control section.

Figure 1-10 Oracle Database Security Assessment Report — Fine-Grained Access Control



Data Redaction

ACCESS.DATAREDACTION — GDPR

Redact sensitive data for read-only application screens

Status	Advisory
Summary	No data redaction policies found. No user can create or manage Data Redaction Policies using schema level grant.
Details	User who can create or manage Data Redaction Policies on all schemas using system level grant: BACKUP_ADMIN Users exempted from Data Redaction Policies: BACKUP_ADMIN, C##ZEUS
Remarks	Data Redaction automatically masks sensitive data found in the results of a database query. The data is dynamically masked before it is returned as part of the result set, so it does not interfere with any conditions specified as part of the query. Data Redaction is mainly used to redact data in read-only scenarios (e.g., read-only screens, REST GET APIs). The redaction policy will not affect access by users with the EXEMPT REDACTION POLICY privilege. Users who can execute the DBMS_REDACT package can create and modify redaction policies. Oracle Database 23ai onwards, a user must have ADMINISTER REDACTION POLICY schema privilege to administer redaction policies of its own schema and ADMINISTER REDACTION POLICY system privilege for other user's schema. Oracle recommends that privileges be granted at schema level to users wherever possible instead of the system privilege. Also, consider using Oracle Data Safe or Oracle Data Masking and Subsetting Pack to permanently mask sensitive data when making copies for test or development.
References	EU GDPR: Article 6, 25, 32, 34, 89; Recital 28, 29, 78, 156
Documentation	Exemption of Users from Oracle Data Redaction Policies

Virtual Private Database

ACCESS.VPD — GDPR

Control access to sensitive data at the row level

Status	Advisory
Summary	No VPD policies found that automatically limit access to certain rows and/or columns based upon the user or the database environment.
Details	Users exempted from VPD Policies: BACKUP_ADMIN, C##ZEUS
Remarks	Virtual Private Database (VPD) allows for fine-grained control over which rows and columns of a table are visible to a SQL statement. Access control using VPD limits each database session to only the specific data it should be able to access. Access by users with the EXEMPT ACCESS POLICY privilege will not be affected by VPD policies. Users who can execute the DBMS_RLS package can create and modify these policies. Evaluate Real Application Security before implementing VPD, especially for new custom applications.
References	EU GDPR: Article 29, 32
Documentation	Using Oracle Virtual Private Database to Control Data Access Oracle Virtual Private Database and Oracle Label Security Exceptions

The Fine-Grained Access Control section is followed by the Database Configuration section.

Oracle Database Security Assessment Report — Database Configuration

The Oracle Database Security Assessment Report — Database Configuration section displays the following information:

Name	Finding ID	Description	Link(s)
Initialization Parameters for Security	-	Displays security related Database initialization parameters and their values.	-
Pre-Authenticated Request URL	CONF.PREAUTHREQUESTURL	Displays pre-authenticated URL information for Oracle Autonomous AI Database Serverless databases including who can manage them via the DBMS_DATA_ACCESS package.	-
Authentication Configuration	CONF.AUTHN	Displays information about the user account initialization parameters. SEC_MAX_FAILED_LOGIN_ATTEMPTS configures the maximum number of failed login attempts in a single session before the connection is closed. This is independent of the user profile parameter FAILED_LOGIN_ATTEMPTS, which controls locking the user account after multiple failed login attempts. RESOURCE_LIMIT should be set to TRUE to enable enforcement of any resource constraints set in user profiles.	• SEC_MAX_FAILED_LOGIN_ATTEMPTS • Configuration of the Maximum Number of Authentication Attempts
Lockdown Profiles	CONF.LOCKDOWNPROFILES	Checks whether a PDB lockdown profile is configured for the current PDB. If a profile is set, it lists the restricted functionalities along with their current status. Also verifies if the PDB_LOCKDOWN parameter is set and, if so, displays its value.	• Restricting Operations on PDBs Using PDB Lockdown Profiles • PDB_LOCKDOWN
PDB OS User	CONF.DEFAULTPDBOSUSER	Checks if the highly privileged Oracle OS user is set for the PDB_OS_CREDENTIAL parameter.	-
Control Files	CONF.CONTROLFILES	Checks if control files are multiplexed and lists all the control file locations. The REMOTE_LOGIN_PASSWORDFILE set to EXCLUSIVE, allows passwords to be updated using the ALTER USER command.	• Managing Control Files • CONTROL_FILES

Name	Finding ID	Description	Link(s)
Redo Log Files	CONF.REDOLOGS	Checks if the defined redo log files follow best practices and lists their location. Redo logs should be multiplexed and stored on different physical disks.	• Managing the Redo Log
Archive Log Mode	CONF.ARCHIVELOG	Checks if the database is in `ARCHIVELOG` or `NOARCHIVELOG` mode. If set, also displays the `archive_log_destination` or the `recovery_file_destination`. Also displays the `archive_log_destination` or the `recovery_file_destination` for the standalone databases.	• Choosing Between NOARCHIVELOG and ARCHIVELOG Mode
Database Backup	CONF.BACKUP	Displays information about Database backup records. Database should be backed up regularly to prevent loss of data in the event of a system failure. Oracle Recovery Manager (RMAN) allows performing backup and recovery tasks on your databases. Unencrypted backup data should not be transported on tape or disk to offsite storage for safekeeping.	• RMAN Backup concepts • Ransomware and Cybersecurity-ZDLRA
Instance Name Check	CONF.INSTANCENAME	Displays whether the instance name contains the Database version number. Instance names should not contain Oracle version numbers. Service names may be discovered by unauthenticated users. If the service name includes version numbers or other database product information, a malicious user may use that information to develop a targeted attack.	-
SQL Firewall	CONF.SQLFIREWALL	Checks if SQL Firewall is enabled and displays the users that are affected by the policy and whether the policy is in observing, blocking, or enforcing mode. Also, details if the SQL and context allow-lists are in enforcement mode or not. Only applicable to Oracle Database >= 23ai.	• Using SQL Firewall • Configuring Oracle SQL Firewall

Name	Finding ID	Description	Link(s)
Read-only ORACLE_HOME	CONF.READONLYHOME	Checks if the ORACLE_HOME is read-only. Only applicable to Oracle Database versions >=18c.	• About Read-Only Oracle Homes • Enabling a Read-Only Oracle Home
Access to Dictionary Objects	CONF.SYSTEMOBJ	Displays whether access to dictionary objects is properly limited. When O7_DICTIONARY_ACCESSIBILITY is set to FALSE, tables owned by SYS are not affected by the ANY TABLE system privileges. This parameter should always be set to FALSE because tables owned by SYS control the overall state of the database and should not be subject to manipulation by users with ANY TABLE privileges.	-
Inference of Table Data	CONF.SQL92SECURITY	Displays whether data inference attacks are properly blocked. When SQL92_SECURITY is set to TRUE, UPDATE and DELETE statements that refer to a column in their WHERE clauses will succeed only when the user has the privilege to SELECT from the same column. This parameter should be set to TRUE so that this requirement is enforced in order to prevent users from inferring the value of a column which they do not have the privilege to view.	• SQL92_SECURITY
Access to Password File	CONF.PASSWORDFILE	Displays whether the password file is configured correctly. The REMOTE_LOGIN_PASSWORDFILE set to EXCLUSIVE allows the password file to contain distinct entries for each administrative user allowing them to be individually audited and tracked for their actions. It also allows passwords to be updated using the ALTER USER command.	• REMOTE_LOGIN_PASSWORDFILE

Name	Finding ID	Description	Link(s)
Network Communication	CONF.NETWORK	Displays information about initialization parameters that determine the database server response to malformed packets. Also, includes details on usage of a remote listener and if database server version information is hidden from unauthenticated client requests. REMOTE_LISTENER allows a network listener running on another system to be used. This parameter should normally be unset to ensure that the local listener is used. The SEC_PROTOCOL_ERROR parameters control the database server's response when it receives malformed network packets from a client. Because these malformed packets may indicate an attempted attack by a malicious client, the parameters should be set to log the incident and terminate the connection. SEC_RETURN_SERVER_RELEASE_BANNER should be set to FALSE to limit the information that is returned to an unauthenticated client, which could be used to help determine the server's vulnerability to a remote attack.	• Parameters for Enhanced Security of Database Communication
External OS Authentication	CONF.EXTERNALOSAUTH	Displays whether the Oracle Database roles are defined and managed by the database itself or by the host operating system (for local and remote authentication). The OS_ROLES parameter determines whether roles granted to users are controlled by GRANT statements in the database or by the database server's operating system. REMOTE_OS_AUTHENT and REMOTE_OS_ROLES allow the client operating system to set the database user and roles. All of these parameters should be set to FALSE so that the authorizations of database users are managed by the database itself.	• Specifying the Type of Role Authorization • Role Grants and Revokes When OS_ROLES Is Set to TRUE • Users of Database Links

Name	Finding ID	Description	Link(s)
Unused Components	CONF.DB COMPONENTS	Checks to see if components like XOQ, CONTEXT, SDO, DV, OLS are installed/enabled and not being used.	-
Job Details	CONF.JOBS	Checks the scheduled database jobs and users who can administer them. Checks include: • Users who can create database jobs • Jobs that can use privileges of DBA/PDB_DBA	-
Triggers	CONF.TRIGGERS	Displays information about logon triggers. A trigger is code that executes whenever a specific event occurs, such as inserting data in a table or connecting to the database. Disabled triggers are a potential cause for concern because whatever protection or monitoring they may be expected to provide is not active.	• Enabling and Disabling triggers • Trigger Enabling and Disabling
Disabled Constraints	CONF.CONSTRAINTS	Displays information about disabled constraints. Constraints are used to enforce and guarantee specific relationships between data items stored in the database. Disabled constraints are a potential cause for concern because the conditions they ensure are not enforced.	• Maintaining Data Integrity in Database Applications • Managing Integrity Constraints

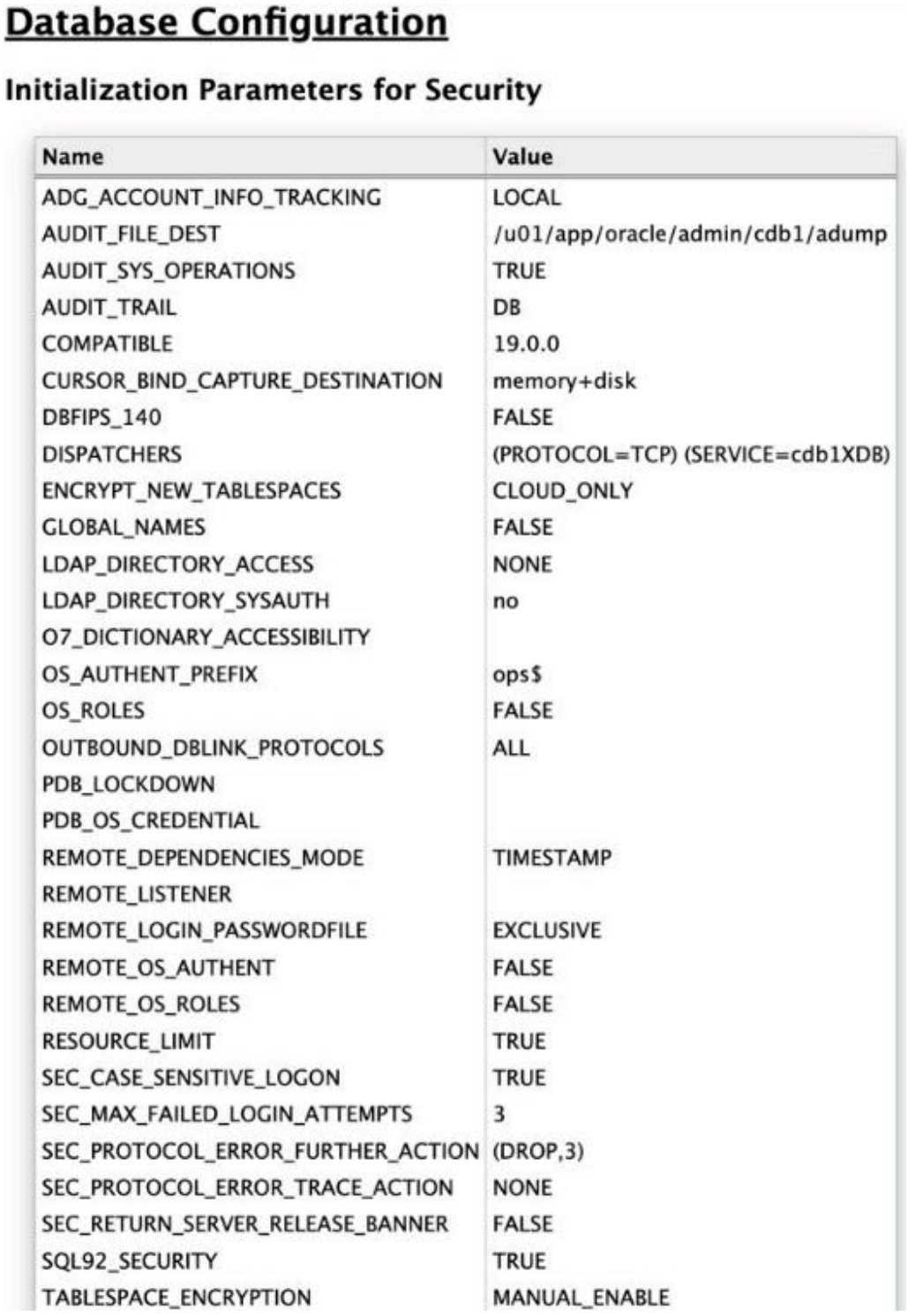
Name	Finding ID	Description	Link(s)
External Procedures	CONF.EXTERNALPROCS	Displays information about external procedures and services. External procedures allow code written in other languages to be executed from PL/SQL. Note that modifications to external code cannot be controlled by the database. Be careful to ensure that only trusted code libraries are available to be executed. Although the database can spawn its own process to execute the external procedure, it is advisable to configure a listener service for this purpose so that the external code can run as a less-privileged OS user. The listener configuration should set `EXTPROC_DLLS` to identify the specific shared library code that can be executed rather than using the default value `ANY`.	• Default Configuration for External Procedures
Source Code Analysis	CONF.SOURCEANALYSIS	Checks `DBA_SOURCE` for non-oracle maintained procedures and functions using `RAISE_APPLICATION_ERROR` and `DBMS_OUTPUT.PUT_LINE.`	• DBMS_OUTPUT package • PL/SQL Error Handling
Directory Objects	CONF.DIRECTORYOBJ	Displays information about directory objects. Directory objects allow access to the server's file system from PL/SQL code within the database. Access to files that are used by the database kernel itself should not be permitted, as this may alter the operation of the database and bypass its access controls.	• Directory Objects • On never granting WRITE and EXECUTE
Directory Separation for Multi-applications	CONF.DIRECTORYSEPARATION	Displays information about the file paths for data files, redo log files, and audit files (AUDIT_FILE_DEST).	-

Name	Finding ID	Description	Link(s)
Database Links	CONF.DATABASELINKS	Displays information about database links. Database links allow users to execute SQL statements that access tables in other databases. This allows for both querying and storing data on the remote database. It is advisable to set `GLOBAL_NAMES` to `TRUE` in order to ensure that link names match the databases they access.	• Database Links • Use Database Links with Autonomous AI Database
Network Access Control	CONF.NETWORKACL	Displays information about Network Access Control Lists (ACLs). Network ACLs control the external servers that database users can access using network packages such as UTL_TCP and UTL_HTTP. Specifically, a database user needs the connect privilege to an external network host computer if he or she is connecting using the `UTL_TCP`, `UTL_HTTP`, `UTL_SMTP`, and `UTL_MAIL` utility packages. To convert between a host name and its IP address using the `UTL_INADDR` package, the `Resolve` privilege is required. Make sure that these permissions are limited to the minimum required by each user.	• Managing Fine-Grained Access in PL/SQL Packages and Types • Syntax for Configuring Access Control for External Network Services • DBA_NETWORK_ACL_PRIVILEGE
XML Database Access Control	CONF.XMLACL	Displays information about XML Database Access Control Lists (ACLs). XML ACLs control access to database resources using the XML DB feature. Every resource in the Oracle XML DB Repository hierarchy has an associated ACL. The ACL mechanism specifies a privilege-based access control for resources to principals, which are database users or roles. Whenever a resource is accessed, a security check is performed, and the ACL determines if the requesting user has sufficient privileges to access the resource. Make sure that these privileges are limited to the minimum required by each user.	• Repository Access Control • Privileges

Name	Finding ID	Description	Link(s)
File System Access	CONF.FILESYS	Checks for UTL_FILE_DIR for older database versions where the parameter is not deprecated.	-
Trace Files	CONF.TRACEFILELIMIT	Displays information about the initialization parameters for trace files. The hidden parameter _TRACE_FILES_PUBLIC determines whether trace files generated by the database should be accessible to all OS users. Since these files may contain sensitive information, access should be limited by setting this parameter to FALSE.	-
Database Resource Plans	CONF.RESOURCEMANAGER	Check for users with EXECUTE on DBMS_RESOURCE_MANAGER package and with ADMINISTER RESOURCE MANAGER system privilege. Also lists the existing resource plans.	• ALLOW_GROUP_ACCESS_TO_SGA • About Resource Manager Administration Privileges • DBMS_RESOURCE_MANAGER
Database Shared Memory	CONF.SGA	Checks if only the Oracle software installation owner can have read and write access to the SGA. Checks for ALLOW_GROUP_ACCESS_TO_SGA.	• ALLOW_GROUP_ACCESS_TO_SGA
Database Vault Configuration	CONF.DATABASEVAULT	Checks for Database Vault integrity. Validates the presence of both the DVSYS and DVF schemas, checks for invalid Database Vault objects, identifies rules that are not associated with any rule sets, and flags any empty rule sets.	-
Security Assessment	CONF.ASSESSMENT	Displays a count of findings in each section that should be reviewed.	-

The following figure displays an example of the Oracle Database Security Assessment Report — Database Configuration section.

Figure 1-11 Oracle Database Security Assessment Report — Database Configuration



Database Configuration

Initialization Parameters for Security

Name	Value
ADG_ACCOUNT_INFO_TRACKING	LOCAL
AUDIT_FILE_DEST	/u01/app/oracle/admin/cdb1/adump
AUDIT_SYS_OPERATIONS	TRUE
AUDIT_TRAIL	DB
COMPATIBLE	19.0.0
CURSOR_BIND_CAPTURE_DESTINATION	memory+disk
DBFIPS_140	FALSE
DISPATCHERS	(PROTOCOL=TCP) (SERVICE=cdb1XDB)
ENCRYPT_NEW_TABLESPACES	CLOUD_ONLY
GLOBAL_NAMES	FALSE
LDAP_DIRECTORY_ACCESS	NONE
LDAP_DIRECTORY_SYSAUTH	no
O7_DICTIONARY_ACCESSIBILITY	
OS_AUTHENT_PREFIX	ops$
OS_ROLES	FALSE
OUTBOUND_DBLINK_PROTOCOLS	ALL
PDB_LOCKDOWN	
PDB_OS_CREDENTIAL	
REMOTE_DEPENDENCIES_MODE	TIMESTAMP
REMOTE_LISTENER	
REMOTE_LOGIN_PASSWORDFILE	EXCLUSIVE
REMOTE_OS_AUTHENT	FALSE
REMOTE_OS_ROLES	FALSE
RESOURCE_LIMIT	TRUE
SEC_CASE_SENSITIVE_LOGON	TRUE
SEC_MAX_FAILED_LOGIN_ATTEMPTS	3
SEC_PROTOCOL_ERROR_FURTHER_ACTION	(DROP,3)
SEC_PROTOCOL_ERROR_TRACE_ACTION	NONE
SEC_RETURN_SERVER_RELEASE_BANNER	FALSE
SQL92_SECURITY	TRUE
TABLESPACE_ENCRYPTION	MANUAL_ENABLE

The Database Configuration section is followed by the Network Configuration section.

Oracle Database Security Assessment Report — Network Configuration

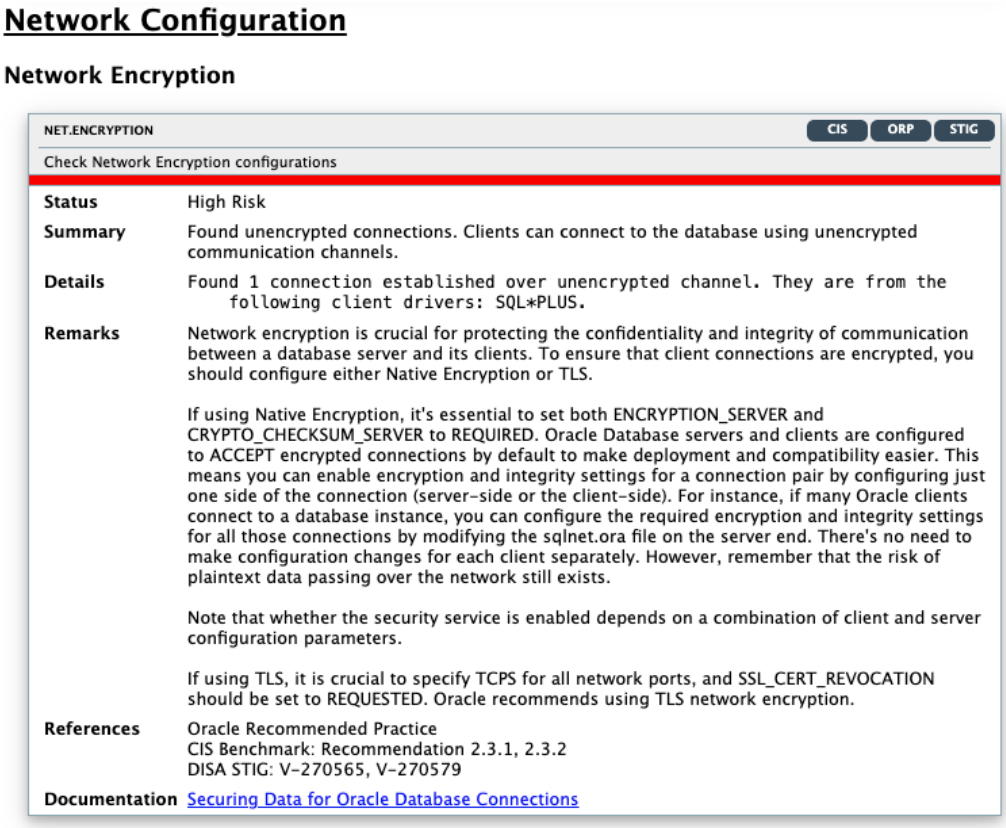
The Oracle Database Security Assessment Report — Network Configuration section displays the following information:

Name	Finding ID	Description	Link(s)
Security Related SQLNET Parameters	-	Displays the security-related SQLNET parameters: • Parameter — Displays the parameter name. • Value — Displays the value set for the parameter.	-
Network Encryption	NET.ENCRYPTION	Displays information about network encryption. Network encryption protects the confidentiality and integrity of communication between the database server and its clients. Either Native Encryption or TLS should be enabled. For Native Encryption, both `ENCRYPTION_SERVER` and `CRYPTO_CHECKSUM_SERVER` should be set to `REQUIRED`. If TLS is used, TCPS should be specified for all network ports and `SSL_CERT_REVOCATION` should be set to `REQUIRED`.	• Securing Data for Oracle Database Connections • Data Encryption
Client Nodes	NET.INVITEDNODES	Displays whether the database accepts connections from any client. `TCP.VALIDNODE_CHECKING` should be enabled to control which client nodes can connect to the database server. Either an allowlist of client nodes allowed to connect (`TCP.INVITED_NODES`) or a blocklist of nodes that are not allowed (`TCP.EXCLUDED_NODES`) may be specified. Configuring both lists is an error; only the invited node list will be used in this case.	• TCP.VALIDNODE_CHECKING • TCP.INVITED_NODES • TCP.EXCLUDED_NODES
Connection Limits Configuration	NET.CONNECTIONLIMITS	Check value of parameters governing termination of unauthenticated connections: • SQLNET.INBOUND_CONNECT_TIMEOUT • INBOUND_CONNECT_TIMEOUT_LISTENER • SQLNET.EXPIRE_TIME	• SQLNET.INBOUND_CONNECT_TIMEOUT • INBOUND_CONNECT_TIMEOUT_listener_name • SQLNET.EXPIRE_TIME

Name	Finding ID	Description	Link(s)
Network Listener Configuration	NET.LISTENERCONFIG	Displays information about network listener configuration. These parameters are used to limit changes to the network listener configuration. ADMIN_RESTRICTIONS should be enabled to prevent parameter changes to the running listener. One of the following restrictions on service registration should be implemented: • Prevent changes by disabling DYNAMIC_REGISTRATION • Limit the nodes that can make changes by enabling VALID_NODE_CHECKING_REGISTRATION • Limit the network sources for changes using the COST parameters SECURE_PROTOCOL, SECURE_CONTROL, and SECURE_REGISTER. CONNECTION_RATE determines rate enforced across all the endpoints that are rate limited	-
Listener Logging Control	NET.LISTENERLOG	Displays information about network listener logging configuration. The LOGGING_LISTENER parameter enables logging of listener activity. Log information can be useful for troubleshooting and to provide early warning of attempted attacks.	• Net Listener Parameters in the listener.ora File - LOGGING_listener_name

The following figure displays an example of the Oracle Database Security Assessment Report — Network Configuration section.

Figure 1-12 Oracle Database Security Assessment Report — Network Configuration



Network Configuration

Network Encryption

NET.ENCRYPTION — CIS ORP STIG

Check Network Encryption configurations

Status	High Risk
Summary	Found unencrypted connections. Clients can connect to the database using unencrypted communication channels.
Details	`Found 1 connection established over unencrypted channel. They are from the following client drivers: SQL*PLUS.`
Remarks	Network encryption is crucial for protecting the confidentiality and integrity of communication between a database server and its clients. To ensure that client connections are encrypted, you should configure either Native Encryption or TLS. If using Native Encryption, it's essential to set both ENCRYPTION_SERVER and CRYPTO_CHECKSUM_SERVER to REQUIRED. Oracle Database servers and clients are configured to ACCEPT encrypted connections by default to make deployment and compatibility easier. This means you can enable encryption and integrity settings for a connection pair by configuring just one side of the connection (server-side or the client-side). For instance, if many Oracle clients connect to a database instance, you can configure the required encryption and integrity settings for all those connections by modifying the sqlnet.ora file on the server end. There's no need to make configuration changes for each client separately. However, remember that the risk of plaintext data passing over the network still exists. Note that whether the security service is enabled depends on a combination of client and server configuration parameters. If using TLS, it is crucial to specify TCPS for all network ports, and SSL_CERT_REVOCATION should be set to REQUESTED. Oracle recommends using TLS network encryption.
References	Oracle Recommended Practice CIS Benchmark: Recommendation 2.3.1, 2.3.2 DISA STIG: V-270565, V-270579
Documentation	Securing Data for Oracle Database Connections

The Network Configuration section is followed by the Operating System section.

Oracle Database Security Assessment Report — Operating System

The Oracle Database Security Assessment Report — Operating System section displays the following information:

Name	Finding ID	Description	Link(s)
Installation Account	OS.INSTALLATION USER	This check specifies the Oracle installation owner.	-

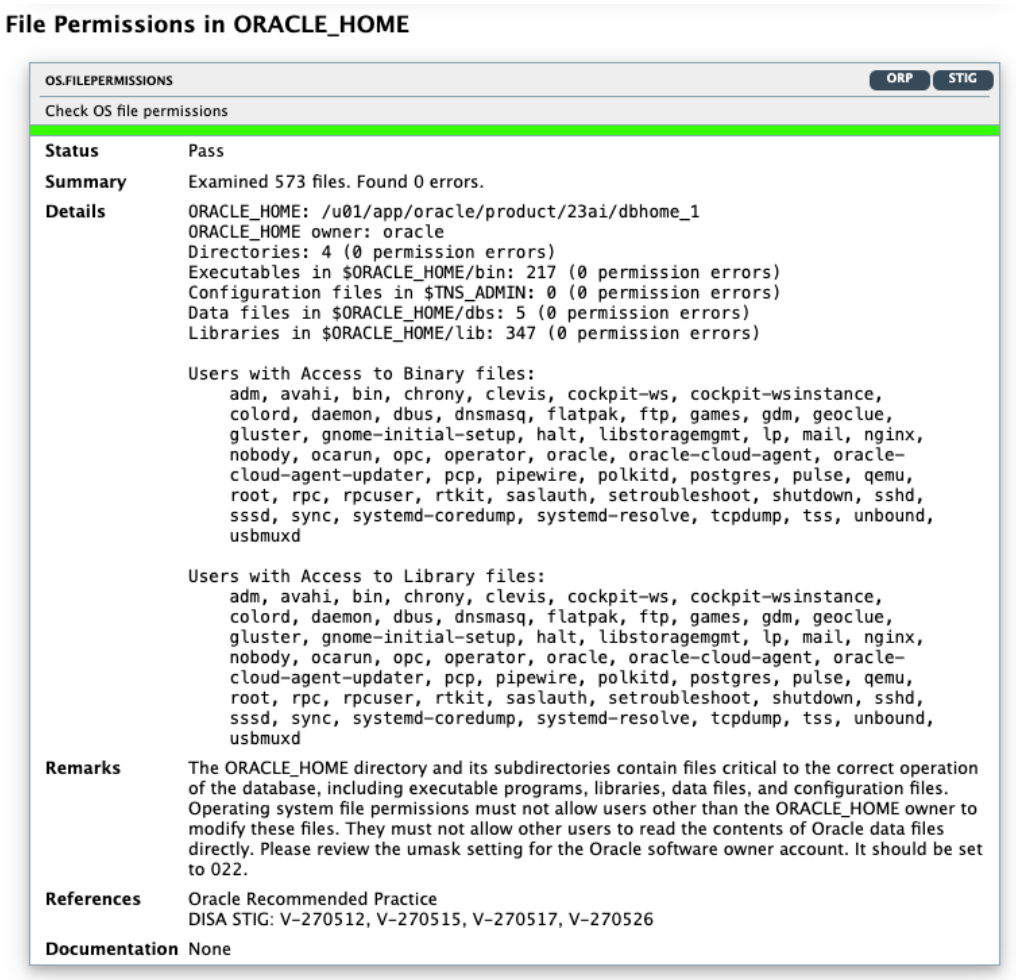
Name	Finding ID	Description	Link(s)
OS Authentication	OS.AUTH	Displays information about operating system group names and users that can exercise administrative privileges. OS authentication allows operating system users within the specified user group to connect to the database with administrative privileges. This shows the OS group names and users that can exercise each administrative privilege. OS users with administrative privileges should be reviewed to prevent any unauthorized, malicious or unintentional access to the database.	-
Segregation of Production and Development Databases	OS.MULTIDB	Checks for databases/instances running on the same server. If there are multiple databases/instances running on the same server ensure that it is not hosting production and test/development databases.	• Deploying an Oracle Database Application
Process Monitor Processes	OS.PMON	Displays whether Process Monitor (PMON) processes are running under the `ORACLE_HOME` owner account. The PMON process monitors user processes and frees resources when they terminate. This process should run with the user ID of the `ORACLE_HOME` owner.	-
Agent Processes	OS.AGENT	Displays whether Agent processes owners overlap with Listener or Process Monitor (PMON) process owners. Agent processes should run with a user ID separate from the database and listener processes. These processes should run under a user ID separate from the database and listener processes.	-
Listener Processes	OS.LISTENER	Displays whether Listener process owners overlap with Agent or Process Monitor (PMON) process owners. Listener processes accept incoming network connections and connect them to the appropriate database server process. These processes should run with a user ID separate from the database and agent processes. These processes should be administered only through local OS authentication.	• Managing Oracle Net Listener Security
Listener Ports	OS.LISTENERPORTS	Displays listener ports.	-

Name	Finding ID	Description	Link(s)
CMAN Remote Admin	OS.CMANLOCAL	Checks if Oracle Connection Manager is installed in the server and if yes, if CMAN remote administration is configured.	• Configuring and Administering Oracle Connection Manager
Diagnostic Destination	OS.DIAGNOSTICDEST	Checks permissions of DIAGONSTIC_DEST: • Checks file permissions if DIAGNOSTIC_DEST is set and is either ORACLE_HOME/rdbms/log or ORACLE_BASE <= 750 • Checks file permissions if DIAGNOSTIC_DEST is set and is either ORACLE_HOME/rdbms/log or ORACLE_BASE > 750 • Checks if the value of DIAGNOSTIC_DEST is not equal to ORACLE_HOME/rdbms/log nor ORACLE_BASE	• DIAGNOSTIC_DEST
File Permissions in ORACLE_HOME	OS.FILEPERMISSIONS	Displays information about file permissions errors in the ORACLE_HOME. The ORACLE_HOME directory and its subdirectories contain files that are critical to the correct operation of the database, including executable programs, libraries, data files, and configuration files. Operating system file permissions must not allow these files to be modified by users other than the ORACLE_HOME owner and must not allow other users to directly read the contents of Oracle data files.	-

> **Note**
>
> On Windows, the DBSAT Collector collects data only from SQL queries. Since the data from the operating system commands is missing, the DBSAT Reporter runs a subset of rules on this data. Operating System findings are not available for databases running on Windows platform.

The following figure displays an example of the Oracle Database Security Assessment Report — Operating System section.

Figure 1-13 Oracle Database Security Assessment Report — Operating System



File Permissions in ORACLE_HOME

OS.FILEPERMISSIONS ORP STIG

Check OS file permissions

Status	Pass
Summary	Examined 573 files. Found 0 errors.
Details	ORACLE_HOME: /u01/app/oracle/product/23ai/dbhome_1 ORACLE_HOME owner: oracle Directories: 4 (0 permission errors) Executables in $ORACLE_HOME/bin: 217 (0 permission errors) Configuration files in $TNS_ADMIN: 0 (0 permission errors) Data files in $ORACLE_HOME/dbs: 5 (0 permission errors) Libraries in $ORACLE_HOME/lib: 347 (0 permission errors) Users with Access to Binary files: adm, avahi, bin, chrony, clevis, cockpit-ws, cockpit-wsinstance, colord, daemon, dbus, dnsmasq, flatpak, ftp, games, gdm, geoclue, gluster, gnome-initial-setup, halt, libstoragemgmt, lp, mail, nginx, nobody, ocarun, opc, operator, oracle, oracle-cloud-agent, oracle-cloud-agent-updater, pcp, pipewire, polkitd, postgres, pulse, qemu, root, rpc, rpcuser, rtkit, saslauth, setroubleshoot, shutdown, sshd, sssd, sync, systemd-coredump, systemd-resolve, tcpdump, tss, unbound, usbmuxd Users with Access to Library files: adm, avahi, bin, chrony, clevis, cockpit-ws, cockpit-wsinstance, colord, daemon, dbus, dnsmasq, flatpak, ftp, games, gdm, geoclue, gluster, gnome-initial-setup, halt, libstoragemgmt, lp, mail, nginx, nobody, ocarun, opc, operator, oracle, oracle-cloud-agent, oracle-cloud-agent-updater, pcp, pipewire, polkitd, postgres, pulse, qemu, root, rpc, rpcuser, rtkit, saslauth, setroubleshoot, shutdown, sshd, sssd, sync, systemd-coredump, systemd-resolve, tcpdump, tss, unbound, usbmuxd
Remarks	The ORACLE_HOME directory and its subdirectories contain files critical to the correct operation of the database, including executable programs, libraries, data files, and configuration files. Operating system file permissions must not allow users other than the ORACLE_HOME owner to modify these files. They must not allow other users to read the contents of Oracle data files directly. Please review the umask setting for the Oracle software owner account. It should be set to 022.
References	Oracle Recommended Practice DISA STIG: V-270512, V-270515, V-270517, V-270526
Documentation	None

The Operating System section is followed by the Diagnostics section.

Oracle Database Security Assessment Report — Diagnostics

The Diagnostics section displays the checks which could not be executed.

Note

This report provides information and recommendations that may be helpful in securing your Oracle database system. These recommendations reflect best practices for database security and should be part of any strategy for Data Protection by Design and by Default. These practices may help in addressing Articles 25 and 32 of the EU General Data Protection Regulation as well as other data privacy regulations. Technical controls alone are not sufficient for compliance. Passing all findings does not guarantee compliance.

Apart from Oracle Recommended Practices, findings in this report map to DISA Oracle Database 19c STIG V1R1 Group IDs, CIS Benchmark for Oracle Database 19c v1.2.0 recommendations, and EU GDPR 2016/679 articles and recitals.

Oracle Database Vault, Oracle Advanced Security, Oracle Label Security, Oracle Data Masking and Subsetting Pack are database licensed options. Oracle Key Vault and Oracle Audit Vault and Database Firewall require separate licensing as well.

The report provides a view on the current status. The results shown are provided for informational purposes only and should not be used as a substitute for a thorough analysis or interpreted to contain any legal or regulatory advice or guidance.

You are solely responsible for your system, and the data and information gathered during the production of this report. You are also solely responsible for the execution of software to produce this report, and for the effect and results of the execution of any mitigating actions identified herein.

Oracle provides this analysis on an "as is" basis without warranty of any kind and Oracle hereby disclaims all warranties and conditions whether express, implied or statutory.

Using the Discoverer

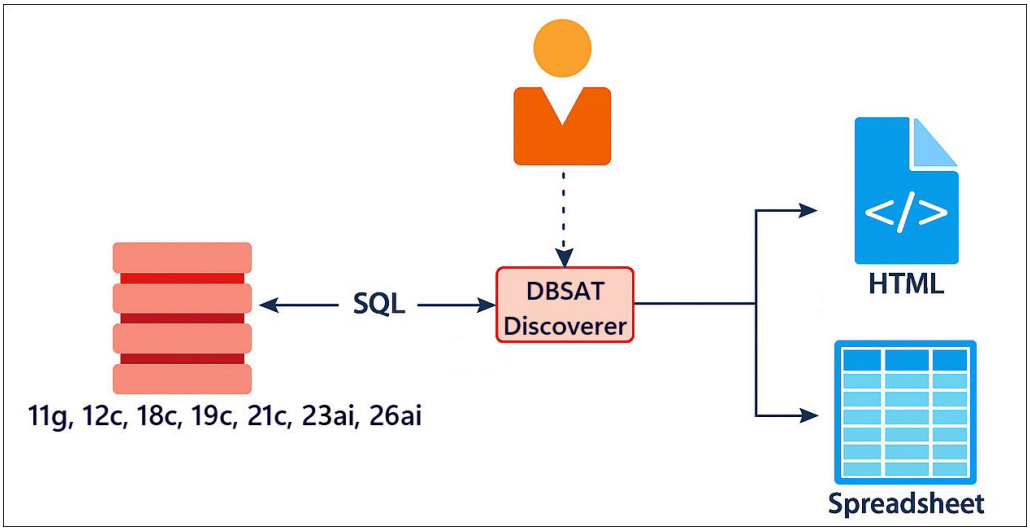
You can generate the Oracle Database Sensitive Data Assessment Report with the Discoverer component.

Oracle Database Sensitive Data Assessment Report

The Discoverer component is used to generate the Oracle Database Sensitive Data Assessment Report. The Discoverer executes SQL queries and collects data from the system to be assessed, based on the settings specified in the configuration and pattern files.

The following figure shows the components and architecture of the Discoverer.

Figure 1-14 Discoverer Components and Architecture



Configuring the Discoverer

Configuring dbsat.config

The settings in the configuration file determine the behavior of the Discoverer.

To configure the Discoverer, do the following:

1. Access the directory where DBSAT is installed.
2. Navigate to the `Discover/conf` directory. Make a copy of the `sample_dbsat.config` file and rename the file to match your site–specific requirements. For example, you can rename the file to `custom_dbsat.config`.

> **Note**
>
> Creating a duplicate file ensures that your custom settings are not overwritten during reinstallation.

3. Open `custom_dbsat.config`.

   The following are the contents of the configuration file:

```
[Database]
        TNS_ADMIN =
        NET_SERVICE_NAME =
        WALLET_LOCATION =

        DB_HOSTNAME = localhost
        DB_PORT = 1521
        DB_SERVICE_NAME =
```

```
        SSL_ENABLED = FALSE
        SSL_TRUSTSTORE =
        SSL_TRUSTSTORE_TYPE =
        SSL_KEYSTORE =
        SSL_KEYSTORE_TYPE =
        SSL_DN =
        SSL_VERSION =
        SSL_CIPHER_SUITES =

[Discovery Parameters]
        sensitive_pattern_files = sensitive.ini
        schema_scope = ALL
        minrows = 1
        exclusion_list_file =

[Sensitive Categories]
        Identification Info - National IDs = High Risk
        Identification Info - Personal IDs = High Risk
        Identification Info - Public IDs = High Risk
        Biographic Info - Address = High Risk
        Biographic Info - Family Data = High Risk
        Biographic Info - Extended PII = High Risk
        Biographic Info - Restricted Data = High Risk
        IT Info - User IT Data = High Risk
        IT Info - Device Data = Medium Risk
        Financial Info - Card Data = High Risk
        Financial Info - Bank Data = High Risk
        Health Info - Insurance Data = High Risk
        Health Info - Provider Data = Medium Risk
        Health Info - Medical Data = Medium Risk
        Job Info - Employee Data = High Risk
        Job Info - Org Data = Low Risk
        Job Info - Compensation Data = High Risk
        Academic Info - Student Data = High Risk
        Academic Info - Institution Data = Medium Risk
        Academic Info - Performance Data = Low Risk
```

> **Note**
>
> Keep the `[Database]`, `[Discovery Parameters]`, and `[Sensitive Categories]` entries for the sections. If you remove these lines, DBSAT discoverer will fail to execute.

4. Configure the settings. For more information about the configuration settings, see Configuration Settings.
5. Save and close the configuration file.

Configuration Settings

Section	Key	Value	Description
[Database]	TNS_ADMIN	<network service name location>	Location from where network service names needs to be read
-	NET_SERVICE_NAME	<net_service_name>	Network Service name to be used to make connection
-	WALLET_LOCATION	<SSL wallet location> | <SEPS wallet location>	Location of wallets for secured connections via SSL or SEPS (Secure External Password Store)
-	DB_HOSTNAME	<hostname> | <ip_address>	Hostname or IP Address of the target database server
-	DB_PORT	<portnumber> The default is 1521.	Listener port number for the target database. If a port number is not specified, the default port 1521 is used.
-	DB_SERVICE_NAME	<service_name>	Service name for the target database
-	SSL_ENABLED	TRUE | FALSE The default is FALSE.	Specifies if SSL is enabled or disabled when connecting to the Database Server. This is an optional argument. It is recommended that the SSL_ENABLED value is set to TRUE. Retain the default FALSE value if you do not require an SSL connection to the Database Server. If SSL_ENABLED = TRUE, then SSL_TRUSTSTORE is mandatory.
-	SSL_TRUSTSTORE	<Absolute path to the TrustStore/ TrustStore filename> **Example:** /opt/ oracle/wallets/ truststore.jks	Specifies the absolute path to the TrustStore, and the TrustStore file name. Mandatory if SSL_ENABLED = TRUE.

Section	Key	Value	Description
-	SSL_TRUSTSTORE_TYPE	PKCS12 | JKS | SSO	Specifies the type of TrustStore. Use PKCS12 if the Truststore is a Wallet. Use JKS if the Truststore is an Oracle Java KeyStore. Use SSO if the Truststore is an auto-login SSO Wallet.
-	SSL_KEYSTORE	<Absolute path to the KeyStore/ KeyStore filename> **Example:** /opt/oracle/wallets/keystore.jks	Specifies the absolute path to the KeyStore, and the KeyStore file name. If SSL_KEYSTORE is not specified, the value specified in SSL_TRUSTSTORE is used. Mandatory if the Database server requires client authentication.
-	SSL_KEYSTORE_TYPE	PKCS12 | JKS | SSO	Specifies the type of KeyStore. Use PKCS12 if the KeyStore is a Wallet. Use JKS if the KeyStore is an Oracle Java KeyStore. Use SSO if the KeyStore is an auto-login SSO Wallet.
-	SSL_DN	<distinguished_name>	Distinguished Name (DN) of the target Database server. Specify the DN if the server's DN needs to be checked. This is an optional argument.

Section	Key	Value	Description
-	SSL_VERSION	1.0 | 1.1 | 1.2 The default is 1.2.	Specifies the version of the SSL protocol to use when connecting to the Database Server. This is an optional argument. Use 1.0 for SSL version TLSv1.0. Use 1.1 for SSL version TLSv1.1. Use 1.2 for SSL version TLSv1.2.
-	SSL_CIPHER_SUITES	<cipher_suite1>,<cipher_suite2> **Example:** TLS_RSA_WITH_AES_256_CBC_SHA256 , SSL_RSA_WITH_RC4_128_MD5	Specifies the Cryptographic Algorithms to be used. Multiple entries can be specified as a comma-separated list. This is an optional argument. For information about supported cryptographic suites, see https://docs.oracle.com/javase/8/docs/technotes/guides/security/SunProviders.html.
[Discovery Parameters]	SENSITIVE_PATTERN_FILES	<file_name> | <file_name1>, <file_name2> The default is sensitive_en.ini.	Specifies the pattern files to be used. Multiple files can be specified as a comma-separated list. The limit is 10 files. For more information about configuring the Sensitive Data Type pattern file, see Pattern File Configuration (Optional).
-	SCHEMA_SCOPE	ALL | <schema1>,<schema2> The default is ALL.	Specifies the schemas to be scanned. Multiple schemas can be specified as a comma-separated list.

Section	Key	Value	Description
-	MINROWS	<numerical value> The default is 1.	Specifies the minimum number of rows in a table for that table to be scanned. Tables with a number of rows less than what is specified in the minrows parameter are excluded from the scan.
-	EXCLUSION_LIST_FILE	<exclusion_list_filename>.ini	Specifies the file to be used to exclude schemas, tables, or columns from the scan. For more information about configuring the Exclusion List file, see Configuring the Exclusion List File (Optional).
[Sensitive Categories]			The **[Sensitive Categories]** section defines which Sensitive Categories are used. Valid risk levels are: • Low Risk • Medium Risk • High Risk The types of sensitive data are defined in the Sensitive Data Type pattern file. For more information about configuring the Sensitive Data Type pattern file, see Pattern File Configuration (Optional).

Pattern File Configuration (Optional)

The Oracle Database Security Assessment Tool searches for the types of sensitive data defined in the Pattern file(s).

About Sensitive Types

Pattern files contain the patterns to search for. A Pattern file is grouped into sections, defined by the section heading format `[SENSITIVE_TYPE_NAME]`. Each section constitutes a Sensitive Type.

The following example shows a sample Sensitive Type section for `FULL NAME`.

```
[FULL NAME]
COL_NAME_PATTERN = ^(?!.*(ITEM|TAX|BALANCE)).*(FULL.*NAME)|(^|[_-])
(CUSTOMER|CUST|CLIENT|PATIENT|PERSON).?(NAME|NM)($|[_-])
COL_COMMENT_PATTERN = ^(?!.*(ITEM|TAX|BALANCE)).*(FULL.?NAME)|(CUSTOMER|
CUST|CLIENT|PATIENT|PERSON).?NAME
SENSITIVE_CATEGORY = Identification Info - Public IDs
```

The Sensitive Type name `[SENSITIVE_TYPE_NAME]` is displayed in the Sensitive Type column of the Database Sensitive Data Assessment Report — Sensitive Column Details section. For more information about the Database Sensitive Data Assessment Report, see Oracle Database Sensitive Data Assessment Report.

Each Sensitive Type is defined by the following three parameters: `COL_NAME_PATTERN`, `COL_COMMENT_PATTERN`, and `SENSITIVE_CATEGORY`.

COL_NAME_PATTERN

The `COL_NAME_PATTERN` parameter specifies the text to search for in the Regular Expression (`RegExp`) patterns of the database column names.

```
(^LNAME$)|((LAST|FAMILY|SUR|PATERNAL).*NAME$)
```

In the example above, the following text will be searched for in the `RegExp` patterns of the database column names:

- `(^LNAME$)` — Searches for a column titled `LNAME`.
- `((LAST|FAMILY|SUR|PATERNAL).*NAME$)` — Searches for column names that contain `LAST`, `FAMILY`, `SUR`, or `PATERNAL`, followed by any characters and ending with `NAME`. For example, `LAST_NAME` or `CUSTOMER_SURNAME`.

COL_COMMENT_PATTERN

The `COL_COMMENT_PATTERN` parameter specifies the text to search for in the Regular Expression (`RegExp`) patterns of the database column comments.

SENSITIVE_CATEGORY

The `SENSITIVE_CATEGORY` parameter specifies the type of sensitive data. The risk levels associated with exposing types of sensitive data are specified in the `sample_dbsat.config` file. The risk levels are:

- `Low Risk`
- `Medium Risk`

- `High Risk`

For more information about configuring the `sample_dbsat.config` file, see Configuration Settings.

Customizing the Pattern File

To customize the Pattern file, do the following:

1. Access the directory where DBSAT is installed.
2. Navigate to the `Discover/conf` directory. Make a copy of the `sensitive.ini` file and rename the file `my_sensitive.ini`.

> **Note**
>
> The `Discover/conf` directory also contains the following language-specific `.ini` files to help discover sensitive data in data dictionaries in major European languages (filename - country, language):
>
> - `sensitive_en.ini` - English, U.S.
> - `sensitive_de.ini` - German, Germany.
> - `sensitive_el.ini` - Greek, Greece.
> - `sensitive_es.ini` - Spanish, Spain.
> - `sensitive_fr.ini` - French, France.
> - `sensitive_it.ini` - Italian, Italy.
> - `sensitive_nl.ini` - Dutch, Netherlands.
> - `sensitive_pt.ini` - Portuguese, Portugal.

3. Open `my_sensitive_en.ini`.
4. Customize the settings by adding new Sensitive Types and modifying existing Sensitive Types.

   For more information about adding new Sensitive Types and Sensitive Categories to the Pattern file, see About Sensitive Types and Configuration Settings.
5. Save and close `my_sensitive_en.ini`.

   The Pattern file is configured.
6. Include `my_sensitive_en.ini` in the Discoverer scan by adding a reference to the file in the `custom_dbsat.config` file.

   ```
   sensitive_pattern_files = my_sensitive_en.ini
   ```

For more information about referencing the Pattern file in the `custom_dbsat.config` file, see Configuring dbsat.config.

About Regular Expressions

The search parameters use regular expressions, sets of strings based on common characteristics shared by each string in the set. Regular expressions vary in complexity, but once you understand the basics of how they are constructed, you can decipher or create any regular expression. You can use character classes, capturing groups, quantifiers, boundary matchers, and logical operators to define regular expressions.

String Literals

The most basic form of pattern matching is the match of a string literal. For example, if the regular expression is `EMP` and the input string is `EMP`, the match succeeds because the strings are identical. This regular expression also matches any string containing `EMP`, such as `EMPLOYEE`, `TEMP`, and `TEMPERATURE`.

Metacharacters

You can also use some special characters that affect the way a pattern is matched. One of the most common ones is the dot (`.`) symbol, which matches any character. For example, `EMPLOYEE.ID` matches `EMPLOYEE_ID` and `EMPLOYEE-ID`, but not `EMPLOYEE_VERIFICATION_ID`. Here, the dot is a metacharacter — a character with special meaning interpreted by the matcher.

Some other metacharacters are: `^ $ ? + * \ - [ ] ( ) { }`.

If you want a metacharacter to be treated literally (as an ordinary character), you can use a backslash (\) to escape it. For example, the regular expression `9\+9` matches `9+9`.

Character Classes

A character class is a set of characters enclosed within square brackets. It specifies the characters that successfully match a single character from a given input string.

The following table describes some common regular expression constructs.

Construct	Description
`[abc]`	Matches one of the characters mentioned within square brackets. Example: `EMPLOYE[ER]` matches `EMPLOYEE` and `EMPLOYER`.
`[^abc]`	Matches any character except the ones mentioned within square brackets. Example: `[^BC]AT` matches `RAT` and `HAT`, but does not match `BAT` and `CAT`.
`[A-Z0-9]`	Matches any character in the range mentioned within square brackets. To specify a range, simply insert the dash metacharacter "`-`" between the first and last character to be matched; for example, `[1-5]` or `[A-M]`. You can also place different ranges beside each other within the class to further expand the match possibilities. Example: `[B-F]AT` matches `BAT`, `CAT`, `DAT`, `EAT`, and `FAT`, but does not match `AAT` and `GAT`.

> **See Also**
>
> - Character Classes
> - Predefined Character Classes

Capturing Groups

You can use capturing groups to treat multiple characters as a single unit. A capturing group is created by placing the characters to be grouped inside a set of parentheses. For example, the regular expression `(SSN)` creates a single group containing the letters `S`, `S`, and `N`.

> **See Also**
>
> Capturing Groups

Quantifiers

You can use quantifiers to specify the number of occurrences to match against.

The following table describes some common quantifiers.

Quantifier	Description
`X?`	Matches zero or one occurrence of the specified character or group of characters. Example: `SSN_NUMBERS?` matches strings `SSN_NUMBER` and `SSN_NUMBERS`.
`X*`	Matches zero or more occurrences of the specified character or group of characters. Example: `TERM.*DATE` matches strings like `TERMDATE`, `TERM_DATE` and `LAST_TERMINATION_DATE`.
`X+`	Matches one or more occurrences of the specified character or group of characters. Example: `TERM.+DATE` matches strings like `TERM_DATE` and `TERMINATION_DATE`, but not `TERMDATE`.
`X{n}`	Matches the specified character or group of characters exactly `n` times. Example: `9{3}` matches `999`, but not `99`.
`X{n,}`	Matches the specified character or group of characters at least `n` times. Example: `9{3,}` matches `999`, `9999`, and `99999`, but not `99`.
`X{n,m}`	Matches the specified character or group of characters at least `n` times but not more than `m` times. Example: `9{3,4}` matches `999` and `9999`, but not `99`.

An example of regular expression using character class is `SSN[0-9]+`, which matches strings like `SSN0`, `SSN1`, and `SSN12`. Here, `[0-9]` is a character class and is allowed one or more times. The regular expression however, does not match `SSN`.

> **See Also**
>
> Quantifiers

Boundary Matchers

You can use boundary matchers to make pattern matching more precise by specifying where in the string the match should take place. For example, you might be interested in finding a particular word, but only if it appears at the beginning or end of an input string.

The following table describes common boundary matchers.

Boundary Construct	Description
`^`	Matches the specified character or group of characters at the beginning of a string (starts with search). Example: `^VISA` matches strings beginning with `VISA`.
`$`	Matches the specified character or group of characters at the end of a string (ends with search). Example: `NUMBER$` matches strings ending with `NUMBER`.
`\b`	Marks a word boundary. Matches the character or group of characters specified between a pair of `\b` only if it is a separate word (as opposed to substring within a longer string). Example: `\bAGE\b` matches strings like `EMPLOYEE AGE` and `PATIENT AGE INFORMATION`, but does not match strings like `AGEING` and `EMPLOYEEAGE`.

If no boundary matcher is specified, a contains search is performed. For example, `ELECTORAL` matches strings containing `ELECTORAL`, such as `ELECTORAL_ID`, `ID_ELECTORAL`, and `ELECTORALID`.

An exact match search can be performed by using `^` and `$` together. For example, `^ADDRESS$` searches for the exact string `ADDRESS`. It matches the string `ADDRESS`, but does not match strings like `PRIMARY_ADDRESS` and `ADDRESS_HOME`.

> **See Also**
>
> Boundary Matchers

Logical Operators

You can use the pipe or vertical bar character (|) if you want to match any one of the characters (or group of characters) separated by pipe. For example, `EMPLOY(EE|ER)_ID` matches `EMPLOYEE_ID` and `EMPLOYER_ID`.

Examples

`^JOB.*(TITLE|PROFILE|POSITION)$` matches strings beginning with `JOB`, followed by zero or more occurrences of any character, and ending with `TITLE`, `PROFILE`, or `POSITION`.

`^[A-Z]{3}[0-9]{2}[A-Z0-9]$` matches strings beginning with three letters, followed by two digits, and ending with a letter or digit.

`BIRTH.?(COUNTRY|PLACE)|(COUNTRY|PLACE).*BIRTH` matches strings such as `BIRTH COUNTRY`, `PATIENT_BIRTH_PLACE`, `PLACE_OF_BIRTH`, and `EMPLOYEE'S COUNTRY OF BIRTH`.

> **See Also**
>
> Regular Expressions

Configuring the Exclusion List File (Optional)

You can specify schemas, tables, or columns to exclude from the scan in the Exclusion List file.

This is an optional step but often required to fine tune the Discoverer to exclude false positives.

To create an Exclusion List file, do the following:

1. Create an Exclusion List file, and save it in the `Discover/conf` directory as `myexclusion_list`.
2. Specify the schemas, tables, or columns to exclude from the Discoverer scan.

   The following is a sample of the contents of the Exclusion List file.

   ```
   PAYROLL
   IT.ENTITLEMENTS
   HR.EMPLOYEE.MARITAL_STATUS
   HR.JOB.CANDIDATE
   ```

   Specify the schemas, tables, or columns to exclude using the format `SchemaName.TableName.ColumnName`. Type each exclusion entry on a new line.

   In the example above, PAYROLL excludes the `PAYROLL` schema from the discovery scan; IT.ENTITLEMENTS excludes the `ENTITLEMENTS` table in `IT` schema; HR.EMPLOYEE.MARITAL_STATUS excludes column `MARITAL_STATUS` from the `HR.EMPLOYEE` table. Similarly, HR.JOB.CANDIDATE excludes column `CANDIDATE` from `HR.JOB` table.

> **Tip**
>
> The Discoverer CSV report includes a column with the fully qualified column names (FULLY_QUALIFIED_COLUMN_NAME). This column can be used to create the exclusion list file contents and speed up the removal of unwanted columns or false positives from the report in a subsequent run.

3. Save and close the Exclusion List file.
4. Update the `exclusion_list_file` entry in your `custom_dbsat.config` file to `exclusion_list_file = myexclusion_list`

For more information about referencing the Exclusion List file, see Configuring dbsat.config.

Configuring Certificates and Wallets (Optional)

The Discoverer allows usage of Secure External Password Store to retrieve login credentials stored a wallet while connecting. Secure External Password Store can be used to connect to Database without entering the username and password. Secure External Password Store improves the security and allows automation of the execution of the Discoverer.

For increased security, Oracle Database provides Secure Sockets Layer (SSL) support to encrypt the connection between clients and the server. If SSL (TLS) encryption is configured on the Database Server, the Discoverer needs to be configured in order to connect and discover data. Configuration parameters for SSL can be found in the `dbsat.config` file.

To establish an SSL connection with the Discoverer, the Database Server sends its certificate, which is stored in its wallet. The client may or may not need a certificate or wallet, depending on the server configuration.

> **Note**
>
> Configuring certificates and wallets is an optional step and needs to be performed only when using SSL to connect to the Oracle Database server.

For more information about configuring certificates and wallets, see Support for SSL in the *Oracle Database JDBC Developer's Guide*.

Running the Discoverer

To run the Discoverer, do the following:

1. Specify the arguments to run the Discoverer:

```
$ dbsat discover [-n] -c <config_file> <output_file>
```

The `dbsat discover` command has the following options and arguments:

- *`-n`*

  Specifies that there is no encryption for output.

- *`-c`*

  Specifies the name of the configuration file used for discoverer. For more information about the *`config_file`* file, see Configuring dbsat.config.

- *`output_file`*

  Specifies the full or relative path name to create the `.dbsat` file. Do not add an extension.

  Example: `/home/oracle/dbsat/PDB1`

2. Run the Discoverer.

   ```
   $ ./dbsat discover -c Discover/conf/custom_dbsat.config PDB1
   ```

   The following output is displayed:

   ```
   Enter username: dbsat_admin
   Enter password:
   DBSAT Discover ran successfully.
   Encrypting the generated reports...
   Enter an encryption key:
   Re-enter the encryption key:
   Encryption completed successfully.
   $
   ```

3. Specify a password to encrypt the `.dbsat` file.

   An encrypted file named <*`destination`*>`_report.dbsat` is created.

4. Extract the contents of the .dbsat file with dbsat extract to access the Database Sensitive Data Assessment Report. When prompted, enter the password to decrypt the `.dbsat` file specified in Step 3.

   The contents of the `.dbsat` file are extracted.

5. Use the appropriate tools to read the Database Sensitive Data Assessment Report.

   Example: Use a browser to display the `.html` file.

   Example: Use a spreadsheet reader like `OpenOffice Calc` or `Excel` to open the `.csv` file.

Oracle Database Sensitive Data Assessment Report

The Discoverer component is used to generate the Oracle Database Sensitive Data Assessment Report in HTML, CSV, and JSON formats.

The HTML report is the main report and contains the discovered sensitive data and its categories along with target database information and Discoverer parameters.

The CSV report can be loaded into Oracle Audit Vault and Database Firewall to add sensitive data context to the new Data Privacy reports. For more information about this functionality, see Importing Sensitive Data Into AVDF Repository in the *Oracle Audit Vault and Database Firewall Auditor's Guide*. The JSON format can be used for integration with other tools.

Oracle Database Sensitive Data Assessment Report — High-Level Summary

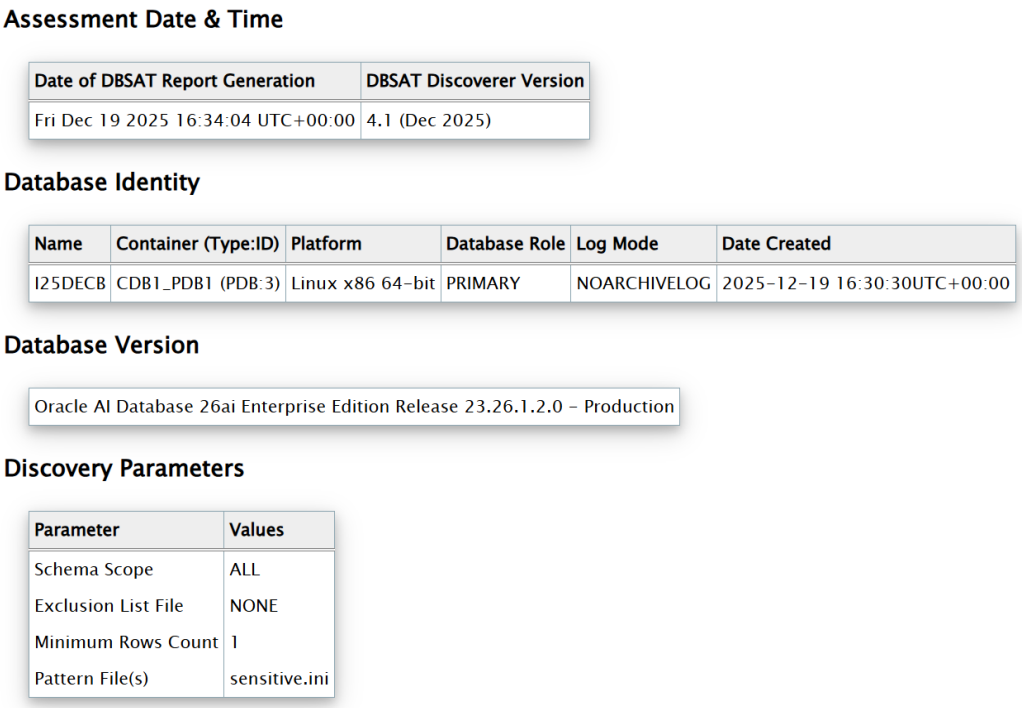
The Oracle Database Sensitive Data Assessment Report — High-Level Summary section contains the following information:

Table 1-1 Oracle Database Sensitive Data Assessment Report — High-Level Summary

Section	Description
Assessment Time & Date	Displays when the Sensitive Data Assessment report was generated. The DBSAT Discoverer version is also displayed.
Database Identity	Displays the details of the database assessed by the Discoverer.
Database Version	Displays the version of the database assessed by the Discoverer.
Discovery Parameters	Displays the Discovery Parameters specified in the configuration file. For more information about Discovery Parameters, see Configuration Settings.

The following figure displays the first four tables of the Oracle Database Sensitive Data Assessment Report — High-Level Summary section.

Figure 1-15 Oracle Database Sensitive Data Assessment Report — High-Level Summary



Assessment Date & Time

Date of DBSAT Report Generation	DBSAT Discoverer Version
Fri Dec 19 2025 16:34:04 UTC+00:00	4.1 (Dec 2025)

Database Identity

Name	Container (Type:ID)	Platform	Database Role	Log Mode	Date Created
I25DECB	CDB1_PDB1 (PDB:3)	Linux x86 64-bit	PRIMARY	NOARCHIVELOG	2025-12-19 16:30:30UTC+00:00

Database Version

Oracle AI Database 26ai Enterprise Edition Release 23.26.1.2.0 - Production

Discovery Parameters

Parameter	Values
Schema Scope	ALL
Exclusion List File	NONE
Minimum Rows Count	1
Pattern File(s)	sensitive.ini

The High-Level Summary section is followed by the Summary section.

Oracle Database Sensitive Data Assessment Report — Summary

The Oracle Database Sensitive Data Assessment Report — Summary section displays information about the number of tables, columns, and rows identified as sensitive data, grouped by Sensitive Category.

The Database Sensitive Data Assessment Report — Summary section contains the following columns:

Table 1-2 Oracle Database Sensitive Data Assessment Report — Summary

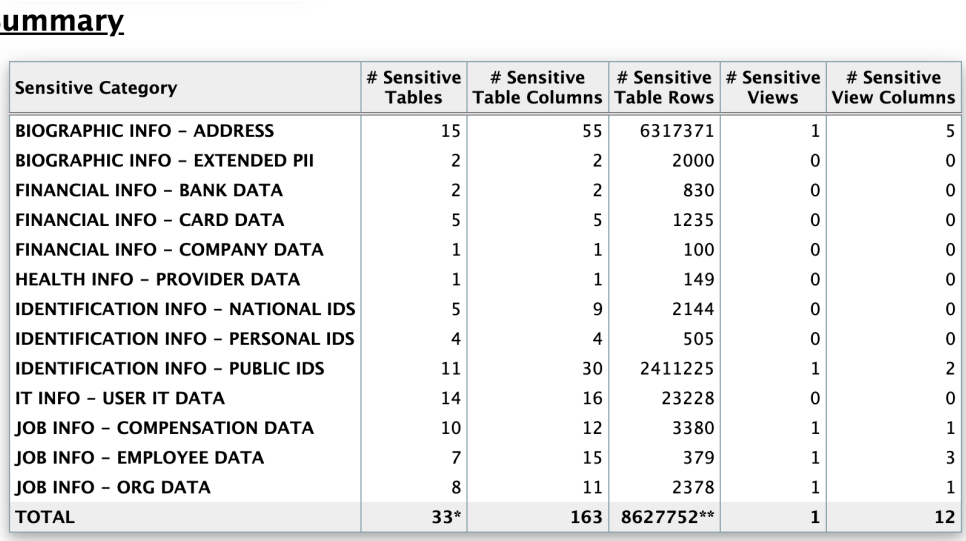
Column Name	Description
Sensitive Category	Displays the name of the Sensitive Category
# Sensitive Tables	Displays the number of tables detected that contain sensitive data
# Sensitive Table Columns	Displays the number of columns detected in the tables that contain sensitive data
# Sensitive Table Rows	Displays the number of table rows containing data classified under a specific sensitive category

Table 1-2 (Cont.) Oracle Database Sensitive Data Assessment Report — Summary

Column Name	Description
# Sensitive Views	Displays the number of views detected that contain sensitive data
# Sensitive View Columns	Displays the number of columns detected in views that contain sensitive data

The following figure displays the information displayed in the Oracle Database Sensitive Data Assessment Report — Summary section:

Figure 1-16 Oracle Database Sensitive Data Assessment Report — Summary



Summary

Sensitive Category	# Sensitive Tables	# Sensitive Table Columns	# Sensitive Table Rows	# Sensitive Views	# Sensitive View Columns
BIOGRAPHIC INFO - ADDRESS	15	55	6317371	1	5
BIOGRAPHIC INFO - EXTENDED PII	2	2	2000	0	0
FINANCIAL INFO - BANK DATA	2	2	830	0	0
FINANCIAL INFO - CARD DATA	5	5	1235	0	0
FINANCIAL INFO - COMPANY DATA	1	1	100	0	0
HEALTH INFO - PROVIDER DATA	1	1	149	0	0
IDENTIFICATION INFO - NATIONAL IDS	5	9	2144	0	0
IDENTIFICATION INFO - PERSONAL IDS	4	4	505	0	0
IDENTIFICATION INFO - PUBLIC IDS	11	30	2411225	1	2
IT INFO - USER IT DATA	14	16	23228	0	0
JOB INFO - COMPENSATION DATA	10	12	3380	1	1
JOB INFO - EMPLOYEE DATA	7	15	379	1	3
JOB INFO - ORG DATA	8	11	2378	1	1
TOTAL	33*	163	8627752**	1	12

> **Note**
>
> A single database table could contain columns or column comments that match more than one Sensitive Category, causing a higher number to be displayed in the `# Sensitive Tables` and `# Sensitive Rows` columns. However, the `Total` row displays the unique number of tables and rows identified as sensitive data.

For more information about configuring Sensitive Categories, see Pattern File Configuration (Optional).

The Summary section is followed by the Sensitive Data section.

Oracle Database Sensitive Data Assessment Report — Sensitive Data

The Oracle Database Sensitive Data Assessment Report — Sensitive Data section displays information about the schemas containing sensitive data.

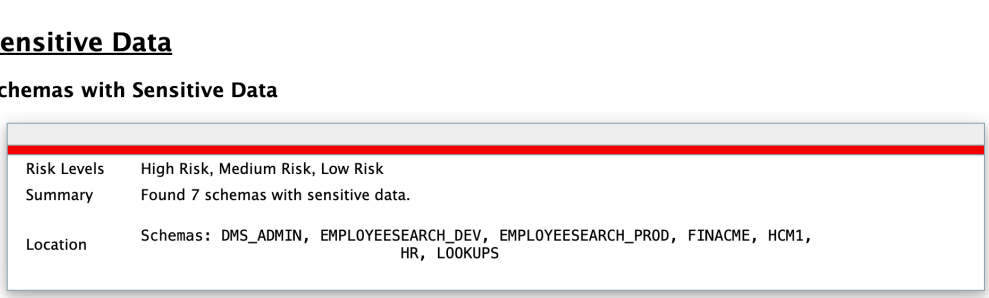
The Oracle Database Sensitive Data Assessment Report — Sensitive Data section contains the following information:

Table 1-3 Oracle Database Sensitive Data Assessment Report — Sensitive Data

Section	Description
Risk Level(s)	Displays the Risk Level(s) of the sensitive data identified in the schema of the database assessed by the Discoverer.
Summary	Displays a summary of the occurrence of sensitive data in the schema.
Location	Displays the names of the schemas containing sensitive data.

The following figure shows the information displayed in the Oracle Database Sensitive Data Assessment Report — Sensitive Data section.

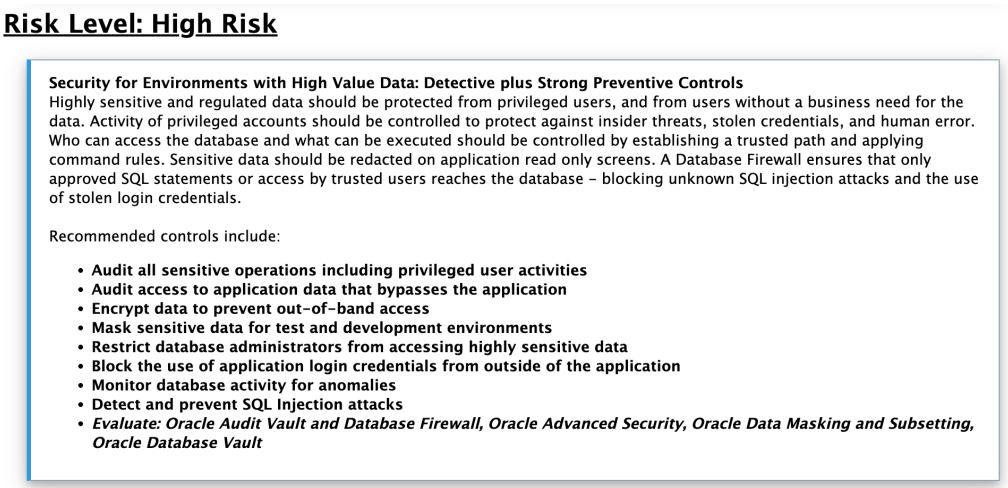
Figure 1-17 Oracle Database Sensitive Data Assessment Report — Sensitive Data



Findings belonging to each risk level are followed by a set of recommendations to secure the sensitive data. These recommendations lists various controls based on the Risk Levels, namely HIGH, MEDIUM, and LOW.

The following figure shows the information displayed in the Risk Level: High Risk section.

Figure 1-18 Sensitive categories grouped by Risk Level



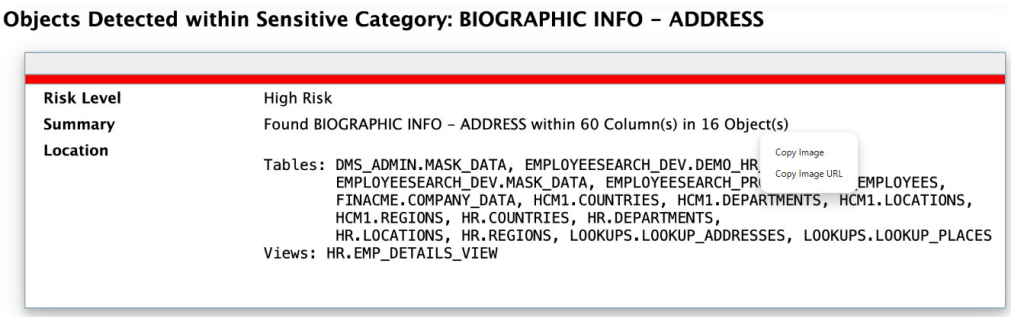
Each Risk Level section is followed by a list of the tables detected that contain sensitive data. The following information is displayed:

Table 1-4 Objects Detected within Sensitive Category: <Sensitive Category Name>

Name	Description
Risk Level	Displays the Risk Level
Summary	Displays a summary of the sensitive category data detected
Location	Displays the names of the tables and views that contain sensitive data

The following figure shows the information displayed in the Objects Detected within each Sensitive Category: <Sensitive Category Name> subsection.

Figure 1-19 Objects Detected within Sensitive Category: <Sensitive Category Name>



The Sensitive Data section is followed by the Schema View section.

Oracle Database Sensitive Data Assessment Report — Schema View

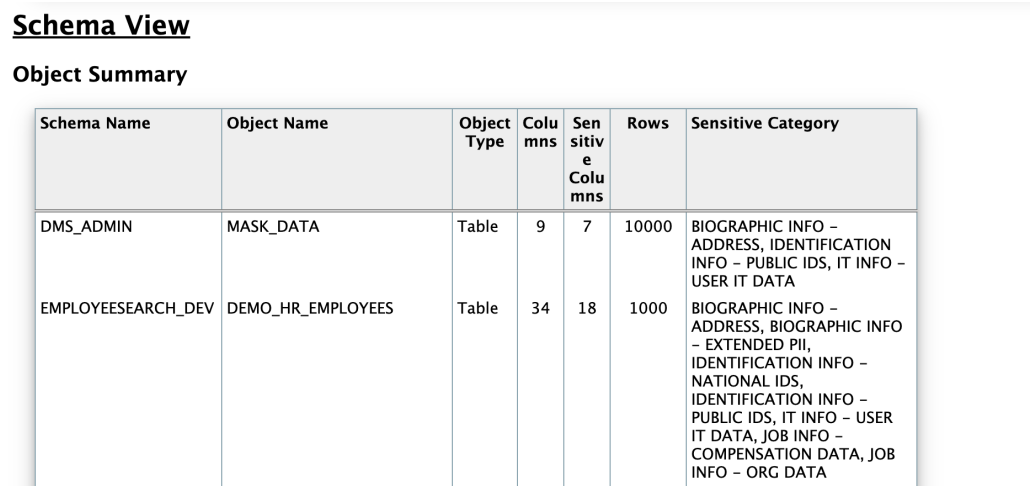
The Oracle Database Sensitive Data Assessment Report — Schema View section displays information about the schemas, tables, columns, and rows containing sensitive data. The Sensitive Category is also displayed.

The Oracle Database Sensitive Data Assessment Report — Summary section contains the following columns:

Column Name	Description
Schema Name	Displays the name of the schema
Object Name	Displays the object name
Object Type	Displays the object type - Table/View
Columns	Displays the number of columns in the table
Sensitive Columns	Displays the number of columns detected that contain sensitive data
Rows	Displays the number of rows in the table
Sensitive Category	Displays the category of sensitive data detected in each column

The following figure highlights the information displayed in the Oracle Database Sensitive Data Assessment Report — Schema View section:

Figure 1-20 Oracle Database Sensitive Data Assessment Report — Schema View



Schema View

Object Summary

Schema Name	Object Name	Object Type	Columns	Sensitive Columns	Rows	Sensitive Category
DMS_ADMIN	MASK_DATA	Table	9	7	10000	BIOGRAPHIC INFO – ADDRESS, IDENTIFICATION INFO – PUBLIC IDS, IT INFO – USER IT DATA
EMPLOYEESEARCH_DEV	DEMO_HR_EMPLOYEES	Table	34	18	1000	BIOGRAPHIC INFO – ADDRESS, BIOGRAPHIC INFO – EXTENDED PII, IDENTIFICATION INFO – NATIONAL IDS, IDENTIFICATION INFO – PUBLIC IDS, IT INFO – USER IT DATA, JOB INFO – COMPENSATION DATA, JOB INFO – ORG DATA

The Schema View section is followed by the Sensitive Column Details section.

Oracle Database Sensitive Data Assessment Report — Sensitive Column Details

The Oracle Database Sensitive Data Assessment Report — Sensitive Column Details section displays information about the columns containing sensitive data. The Sensitive Category and Type are also displayed.

Column Name	Description
Schema Name	Displays the name of the schema
Object Name	Displays the object name
Object Type	Displays the object type - Table/View
Column Name	Displays the name of the column
Column Comment	Displays the column comment
Sensitive Category	Displays the category of sensitive data detected in each column
Sensitive Type	Displays the type of sensitive data detected in each column
Risk Level	Displays the risk level

The following figure displays the information displayed in the Oracle Database Sensitive Data Assessment Report — Sensitive Column Details section.

Figure 1-21 Oracle Database Sensitive Data Assessment Report — Sensitive Column Details

Sensitive Column Details

Schema Name	Object Name	Object Type	Column Name	Column Comment	Sensitive Category	Sensitive Type	Risk Level
DMS_ADMIN	MASK_DATA	Table	CITY	--	BIOGRAPHIC INFO – ADDRESS	CITY	High Risk
DMS_ADMIN	MASK_DATA	Table	GIVENNAME	--	IDENTIFICATION INFO – PUBLIC IDS	FIRST NAME	High Risk
DMS_ADMIN	MASK_DATA	Table	STREETADDRESS	--	BIOGRAPHIC INFO – ADDRESS	STREET	High Risk
DMS_ADMIN	MASK_DATA	Table	SURNAME	--	IDENTIFICATION INFO – PUBLIC IDS	LAST NAME	High Risk
DMS_ADMIN	MASK_DATA	Table	TELEPHONENUMBER	--	IDENTIFICATION INFO – PUBLIC IDS	PHONE NUMBER	High Risk
DMS_ADMIN	MASK_DATA	Table	USERNAME	--	IT INFO – USER IT DATA	USER ID	High Risk
DMS_ADMIN	MASK_DATA	Table	ZIPCODE	--	BIOGRAPHIC INFO – ADDRESS	POSTAL CODE	High Risk
EMPLOYEESEARCH_DEV	DEMO_HR_EMPLOYEES	Table	ADDRESS_1	--	BIOGRAPHIC INFO – ADDRESS	FULL ADDRESS	High Risk

Best Practices

Collector - OS Commands

As a general best practice, you should not put username/password credentials in cleartext in an application or file. When you provide the password on the command line while executing `dbsat collect`, someone can retrieve credentials, either using history or executing the `ps` Unix command or any similar Windows command. Therefore, Oracle recommends that you enter the password when prompted.

Collector - Database User Account

It's advisable that you run DBSAT collect and discoverer with a user that has the minimum set of privileges required to execute the assessments. The user shall also have a strong password. This will help reduce the attack surface and the potential impact of stolen DBSAT user account credentials, account misuse, and human error.

You can create a user with the required minimum privileges to run the Oracle Database Security Assessment Tool with the script provided in the pre-requisites section.

Securing DBSAT Output Files

By default, DBSAT produces encrypted output files.

Excluding Sensitive User Accounts

DBSAT allows you to exclude users from the security assessment report. If there are critical users that you do not want to show in the report, you can exclude them by using the -u option in dbsat report execution.

Appendix A

Improved DBSAT Target Specific Checks and Recommendations

DBSAT can be run against on-premises databases, Oracle Autonomous AI Databases (Serverless and Dedicated) and Oracle Cloud DBCS (DBSystems EE/HP/EP). Some findings will execute different checks and provide specific recommendations for these databases. The table below highlights which findings were improved.

Figure 1-22 DBSAT Target Specific Checks and Recommendations

	New Rule ID (4.0)	Old Rule ID (as in 3.1)	Finding Title	On-premises		Oracle Autonomous AI Database		Oracle Base Database EE/EP/HP (5)	References
				Check (1)	Remarks (2)	Serverless (3)	Dedicated (4)		
1	INFO.PATCH	INFO.PATCH	Patch Check	Yes	No	Yes	Yes	No	ORP, CIS, STIG
2	USER.DEFAULTPROFILE	USER.DEFAULTPROFILE	Users with DEFAULT Profile	No	Yes	No	No	No	CIS
3	USER.DEFPASSWORD	USER.DEFPASSWORD	Users with Default Passwords	No	No	No	No	No	ORP, CIS, STIG
4	USER.EXPIRED	USER.EXPIRED	Users with Expired Passwords	No	Yes	Yes	Yes	No	ORP
5	USER.INACTIVE	USER.INACTIVE	Inactive Users	No	Yes	Yes	Yes	No	ORP, CIS, STIG
6	USER.SAMPLE	USER.SAMPLE	Sample Schemas	No	Yes	Yes	Yes	No	ORP, CIS, STIG
7	USER.APPOWNER	USER.APPOWNER	Application Owner Account	Yes	No	No	No	No	ORP
8	USER.SHARED	USER.SHARED	Shared Accounts	Yes	Yes	No	No	No	ORP, STIG
9	USER.OBJOWNER	USER.OBJOWNER	Users with Objects	No	Yes	No	No	No	STIG
10	USER.OBJAUTHZ	USER.OBJAUTHZ	Users Authorized for Object Ownership	Yes	Yes	No	No	No	STIG
11	USER.SECURITYOBJS	USER.SECURITYOBJS	Users with Security Objects	No	No	No	No	No	STIG
12	USER.GRANTOPTION	USER.GRANTOPTION	Users with Grant Option	No	No	No	No	No	ORP, STIG
13	USER.SENSITIVEDATA	USER.SENSITIVEDATA	Users with Sensitive Data	No	No	No	No	No	ORP
14	USER.TABLESPACE	USER.TBLSPACE	User Schemas in SYSTEM or SYSAUX Tablespace	Yes	No	No	No	No	ORP, STIG
15	USER.PASSWORDCASE	USER.PASSWORDCASE	Case-Sensitive Passwords	Yes	Yes	Yes	Yes	No	ORP, CIS
16	USER.AUTHLEGACY	USER.AUTHLEGACY	Legacy Password Versions	Yes	Yes	No	No	No	ORP
17	USER.PASSWORDFUNCTION	USER.PASSWORDFUNCTION	Users with no Password Complexity Requirements	Yes	Yes	No	No	No	ORP, CIS, STIG
18	USER.NOLOCK	USER.NOLOCK	Account Locking after Failed Login Attempts	No	Yes	No	No	No	ORP, CIS, STIG
19	USER.TOEXPIRE	-	Users with Passwords About to Expire	**New**	**New**	**New**	**New**	**New**	ORP
20	USER.NOEXPIRE	USER.NOEXPIRE	Users with Unlimited Password Lifetime	Yes	No	No	No	No	ORP, CIS, STIG
21	USER.SESSIONS	USER.SESSIONS	Users with Unlimited Concurrent Sessions	Yes	Yes	No	No	No	ORP, CIS, STIG

Figure 1-23 DBSAT Target Specific Checks and Recommendations (continued)

22	USER.IDLETIME	USER.IDLETIME	Users with Unlimited Session Idle Time	Yes	Yes	No	No	No	ORP, STIG
23	USER.PASSWORDROLLOVER	USER.GPR	Users with Gradual Password Rollover	No	No	No	No	No	ORP
24	USER.TEMP	USER.TEMP	Temporary Users	No	No	No	No	No	ORP, CIS, STIG
25	USER.DEV	USER.DEV	Development Users in Production Databases	No	No	No	No	No	ORP, STIG
26	USER.REPCAT	USER.REPCAT	Advanced Replication Users	No	No	No	No	No	STIG
27	USER.AUTHVERSION	USER.AUTHVERSION	Minimum Client Authentication Version	No	Yes	No	No	No	ORP, STIG
28	USER.NEW	-	New Users Who Need to Reset Password	**New**	**New**	**New**	**New**	**New**	ORP, STIG
29	USER.LOCALAUTH	-	Locally Managed Accounts	**New**	**New**	**New**	**New**	**New**	STIG
30	USER.EXTERNALAUTH	AUTHZ.PKI	PKI-based Authentication	Yes	Yes	No	No	No	CIS, STIG
31	PRIV.ACCESSVERIFIERS	PRIV.ACCESSVERIFIERS	Access to Password Verifier Tables	Yes	Yes	No	No	No	ORP, CIS
32	PRIV.SYSADMIN	PRIV.ADMIN	Users with Administrative SYS* Privileges	Yes	No	No	No	No	ORP, STIG
33	PRIV.DBA	PRIV.DBA	Users with DBA Role	Yes	No	No	No	No	ORP, CIS
34	PRIV.BIGROLES	PRIV.BIGROLES	Users with Powerful Roles	Yes	Yes	No	No	No	ORP, CIS, STIG
35	PRIV.SYSTEM	PRIV.SYSTEM	System Privilege Grants	No	Yes	No	No	No	ORP, CIS, STIG
36	PRIV.SCHEMA	-	Schema Privilege Grants	**New**	**New**	**New**	**New**	**New**	ORP
37	PRIV.SYSPUBLIC	PRIV.SYSPUBLIC	System Privileges Granted to PUBLIC	No	No	No	No	No	ORP, STIG
38	PRIV.ROLEPUBLIC	PRIV.ROLEPUBLIC	Roles Granted to PUBLIC	No	No	No	No	No	ORP, STIG
39	PRIV.COLPUBLIC	PRIV.COLPUB	Column Privileges Granted to PUBLIC	No	No	No	No	No	ORP
40	PRIV.OBJPUBLIC	PRIV.OBJPUBLIC	Objects accessible by PUBLIC	No	No	No	No	No	ORP, STIG
41	PRIV.ENCRYPTPACKAGEPUBLIC	PRIV.ENCRYPTPACKAGEPUBLIC	Encryption Packages Granted to PUBLIC	No	No	No	No	No	CIS
42	PRIV.JOBSCHPACKAGEPUBLIC	PRIV.JOBSCHPACKAGEPUBLIC	Scheduler Job Packages Granted to PUBLIC	No	No	No	No	No	ORP, CIS
43	PRIV.CREDPACKAGEPUBLIC	PRIV.CREDPACKAGEPUBLIC	Credential Package Granted to PUBLIC	No	No	No	No	No	CIS

Figure 1-24 DBSAT Target Specific Checks and Recommendations (continued)

45	PRIV.NETPACKAGEPUBLIC	PRIV.NETPACKAGEPUBLIC	Network Packages Granted to PUBLIC	No	No	No	No	No	CIS
46	PRIV.JAVAPACKAGEPUBLIC	PRIV.JAVAPACKAGEPUBLIC	JAVA Permissions Granted to PUBLIC	No	No	No	No	No	CIS
47	PRIV.QUERYPACKAGEPUBLIC	PRIV.QUERYPACKAGEPUBLIC	SQL Packages Granted to PUBLIC	No	No	No	No	No	CIS
48	PRIV.ANYSYSTEM	PRIV.ANYSYSTEM	Broad Data Access Privileges	No	No	No	No	No	ORP, CIS
49	PRIV.CONTAINERACCESS	-	Container Access Privilege Grants	**New**	**New**	**New**	**New**	**New**	ORP
50	PRIV.ALLROLES	PRIV.ALLROLES	All Roles	No	No	No	No	No	ORP
51	PRIV.ACCOUNTMGMT	PRIV.ACCOUNTMGMT	Account Management Privileges	Yes	Yes	No	No	No	ORP, STIG
52	PRIV.ROLEPRIVMGMT	PRIV.ROLEPRIVMGMT	Role and Privilege Management Privileges	No	No	No	No	No	ORP, CIS
53	PRIV.DBMGMT	PRIV.DBMGMT	Database Management Privileges	No	No	Yes	No	No	ORP, CIS
54	PRIV.AUDITMGMTPKG	PRIV.AUDITMGMTPKG	Audit Management Package	No	No	No	No	No	ORP, STIG
55	PRIV.AUDITMGMT	PRIV.AUDITMGMT	Audit Management Privileges	No	Yes	No	No	No	ORP, CIS, STIG
56	PRIV.ACCESSAUDITOBJ	PRIV.ACCESSAUDITOBJ	Access to Audit Objects	Yes	Yes	No	No	No	ORP, CIS, STIG
57	PRIV.ACCESSEXEMPT	PRIV.ACCESSEXEMPT	Access Control Exemption Privileges	No	No	No	No	No	ORP, CIS
58	PRIV.RESTRICTEDOBJ	PRIV.RESTRICTEDOBJ	Write Access to Restricted Objects	No	No	No	No	No	ORP, CIS, STIG
59	PRIV.IMPERSONATEUSER	PRIV.IMPERSONATEUSER	Users who can Impersonate other users	No	No	No	No	No	ORP, CIS
60	PRIV.EXFILTRATION	PRIV.EXFILTRATION	Privilege for Data Exfiltration in Bulk	No	No	Yes	Yes	No	ORP, CIS
61	PRIV.CBAC	PRIV.CBAC	Code Based Access Control	No	Yes	No	No	No	ORP
62	PRIV.JAVAPERMISSIONS	PRIV.JAVAPERMISSIONS	Java Permissions	No	Yes	No	No	No	ORP
63	AUTHZ.DATABASEVAULT	AUTHZ.DATABASEVAULT	Database Vault	Yes	Yes	Yes	Yes	No	ORP, STIG, GDPR
64	AUTHZ.DATABASEVAULTSOD	-	Database Vault Separation of Duty	**New**	**New**	**New**	**New**	**New**	ORP, STIG, GDPR
65	AUTHZ.PRIVANALYSIS	AUTHZ.PRIVANALYSIS	Privilege Analysis	Yes	No	No	No	No	ORP

Figure 1-25 DBSAT Target Specific Checks and Recommendations (continued)

66	AUTHZ.PASSWORDSCRIPTS	AUTHZ.PASSWORDSCRIPTS	Authentication for Client Scripts	No	No	No	No	No	ORP, STIG
67	AUTHZ.DATAMASKING	AUTHZ.DATAMASKING	Data Masking	Yes	Yes	No	No	No	ORP, STIG, GDPR
68	ACCESS.DATAREDACTION	ACCESS.DATAREDACTION	Data Redaction	Yes	No	No	No	No	GDPR
69	ACCESS.VPD	ACCESS.VPD	Virtual Private Database	Yes	No	No	No	No	GDPR
70	ACCESS.RAS	ACCESS.RAS	Real Application Security	No	No	No	No	No	GDPR
71	ACCESS.LABELSECURITY	ACCESS.OLS	Label Security	Yes	Yes	No	No	No	STIG, GDPR
72	ACCESS.TSDP	ACCESS.TSDP	Transparent Sensitive Data Protection (TSDP)	No	No	No	No	No	ORP
73	AUDIT.ENABLED	AUDIT.ENABLED	Audit Records	Yes	Yes	Yes	Yes	Yes	ORP, CIS, STIG, GDPR
74	AUDIT.UNIFIEDPOLICIES	AUDIT.UNIFIEDPOLICIES	Unified Audit Policies	Yes	Yes	Yes	Yes	Yes	ORP, STIG, GDPR
75	AUDIT.CONDITION	AUDIT.CONDITION	Audit Conditions	No	No	No	No	No	ORP
76	AUDIT.FGA	AUDIT.FGA	Fine Grained Audit	No	No	No	No	No	ORP, STIG
77	AUDIT.ADMINACTIONS	AUDIT.ADMIN	Audit Administrative (SYS*) Users	No	No	No	No	No	ORP, CIS, STIG
78	AUDIT.CONNECTIONS	AUDIT.CONN	Audit User Logon and Logoff	No	No	Yes	Yes	No	ORP, CIS
79	AUDIT.DBMGMT	AUDIT.DBMGMT	Audit Database Management Activities	No	No	Yes	Yes	No	ORP, CIS, STIG
80	AUDIT.ACCOUNTMGMT	AUDIT.ACCOUNTMGMT	Audit Account Management Activities	No	No	No	No	No	ORP, CIS, STIG
81	AUDIT.SYSTEMPRIVS	AUDIT.SYSTEMPRIVS	Audit System Privileges	No	No	No	No	No	ORP, CIS
82	AUDIT.ROLESYSTEMPRIVS	AUDIT.ROLESYSTEMPRIVS	Audit Roles with System Privileges	No	No	No	No	No	ORP
83	AUDIT.PRIVMGMT	AUDIT.PRIVMGMT	Audit Privilege Management	Yes	Yes	No	No	No	ORP, CIS
84	AUDIT.STATEMENT	AUDIT.STATEMENT	Audit SQL Statements	Yes	Yes	No	No	No	ORP
85	AUDIT.SENSITIVEOBJS	AUDIT.SENSITIVEOBJS	Audit Object Actions	Yes	Yes	No	No	No	ORP, CIS
86	AUDIT.SYNONYMS	AUDIT.SYNONYMS	Audit Synonym Management Activities	Yes	Yes	No	No	No	CIS
87	AUDIT.SHAREDPROXY	AUDIT.SHAREDPROXY	Audit Shared Accounts	No	Yes	No	No	No	ORP, STIG
88	AUDIT.TABLESPACE	AUDIT.TABLESPACE	Audit Storage	Yes	Yes	No	No	No	ORP, STIG
89	AUDIT.CLEANUPJOBS	AUDIT.CLEANUPJOBS	Audit Trail Cleanup	Yes	Yes	No	No	No	ORP

Figure 1-26 DBSAT Target Specific Checks and Recommendations (continued)

90	AUDIT.DATAPUMP	AUDIT.DATAPUMP	Audit Data Pump	No	No	No	No	No	ORP
91	AUDIT.STIGPOLICY	AUDIT.STIGPOLICY	Audit STIG Actions	Yes	Yes	No	No	No	STIG
92	AUDIT.DATABASEVAULT	AUDIT.DATABASEVAULT	Audit Database Vault	Yes	Yes	No	No	No	ORP
93	AUDIT.LABELSECURITY	AUDIT.LABELSECURITY	Audit Label Security	Yes	No	No	No	No	ORP
94	ENCRYPT.TDE	ENCRYPT.TDE	Transparent Data Encryption	Yes	Yes	Yes	Yes	Yes	ORP, STIG, GDPR
95	ENCRYPT.WALLET	ENCRYPT.WALLET	Encryption Key Wallet	No	No	No	Yes	Yes	ORP, GDPR
96	ENCRYPT.DBFIPS	ENCRYPT.DBFIPS	FIPS Mode for TDE and DBMS_CRYPTO	No	Yes	No	No	No	STIG
97	ENCRYPT.TLSFIPS	ENCRYPT.TLSFIPS	FIPS mode for TLS	No	No	No	No	No	STIG
98	CONF.PREAUTHREQUESTURL	CONF.PREAUTHREQUESTURL	Pre-Authenticated Request URLs	No	No	Yes	No	No	ORP
99	CONF.AUTHN	CONF.AUTHN	Authentication Configuration	No	No	No	No	No	ORP, CIS
100	CONF.LOCKDOWNPROFILES	-	Lockdown Profiles	New	New	New	New	New	ORP
101	CONF.DEFAULTPDBOSUSER	CONF.DEFAULTPDBOSUSER	PDB OS User	Yes	No	No	No	No	ORP, CIS
102	CONF.CONTROLFILES	CONF.CONTROLFILES	Control files	No	No	Yes	Yes	Yes	ORP, STIG
103	CONF.REDOLOGS	CONF.REDOLOGS	Redo Log Files	No	No	Yes	Yes	Yes	ORP, STIG
104	CONF.ARCHIVELOG	CONF.ARCHIVELOG	Archive Log Mode	No	No	Yes	Yes	Yes	ORP, STIG
105	CONF.BACKUP	CONF.BACKUP	Database Backup	YES	No	Yes	Yes	No	ORP, STIG
106	CONF.INSTANCENAME	CONF.INSTANCENAME	Instance Name Check	No	No	No	No	No	ORP, STIG
107	CONF.SQLFIREWALL	CONF.SQLFIREWALL	SQL Firewall	No	No	No	No	No	ORP
108	CONF.SYSTEMOBJ	CONF.SYSOBJ	Access to Dictionary Objects	No	No	No	No	No	ORP, CIS, STIG
109	CONF.READONLYHOME	CONF.READONLYHOME	Read-only ORACLE_HOME	No	No	No	No	No	ORP, STIG
110	CONF.SQL92SECURITY	CONF.INFER	Inference of Table Data	No	No	Yes	Yes	No	ORP, CIS, STIG
111	CONF.PASSWORDFILE	CONF.PASSWORDFILE	Access to Password File	No	No	No	No	No	ORP, CIS, STIG
112	CONF.NETWORK	CONF.NETWORK	Network Communication	No	No	No	No	No	ORP, CIS
113	CONF.EXTERNALOSAUTH	CONF.EXTERNALOSAUTH	External OS Authentication	Yes	No	Yes	Yes	No	ORP, CIS, STIG
114	CONF.DBCOMPONENTS	CONF.DBCOMPONENTS	Unused components	Yes	No	No	No	No	STIG

Figure 1-27 DBSAT Target Specific Checks and Recommendations (continued)

115	CONF.JOB	CONF.JOB	Job Details	No	No	No	No	No	ORP, CIS, STIG
116	CONF.TRIGGERS	CONF.TRIGGERS	Triggers	Yes	No	No	No	No	ORP
117	CONF.CONSTRAINTS	CONF.CONSTRAINTS	Disabled Constraints	Yes	No	Yes	Yes	No	ORP, STIG
118	CONF.EXTERNALPROCS	CONF.EXTERNALPROCS	External Procedures	No	No	No	No	No	ORP, CIS, STIG
119	CONF.SOURCEANALYSIS	CONF.SOURCEANALYSIS	Source Code Analysis	No	Yes	No	No	No	ORP, STIG
120	CONF.DIRECTORYOBJ	CONF.DIRECTORYOBJ	Directory Objects	No	No	Yes	Yes	No	ORP, STIG
121	CONF.DIRECTORYSEPARATION	-	Directory Separation for Multi-applications	**New**	**New**	**New**	**New**	**New**	ORP, STIG
122	CONF.DATABASELINKS	CONF.DATABASELINKS	Database Links	Yes	No	Yes	Yes	No	ORP, CIS, STIG
123	CONF.NETWORKACL	CONF.NETACL	Network Access Control	No	No	Yes	Yes	No	ORP
124	CONF.XMLACL	CONF.XMLACL	XML Database Access Control	Yes	No	No	No	No	ORP
125	CONF.TRACEFILEACCESS	CONF.TRACEFILELIMIT	Trace Files	No	Yes	No	No	No	ORP, CIS, STIG
126	CONF.RESOURCEMANAGER	-	Database Resource Plans	**New**	**New**	**New**	**New**	**New**	ORP
127	CONF.FILESYS	CONF.FILESYS	File System Access	No	No	No	No	No	ORP, CIS
128	CONF.SGA	-	Database Shared Memory	**New**	**New**	**New**	**New**	**New**	ORP
129	CONF.DATABASEVAULT	-	Database Vault Configuration	**New**	**New**	**New**	**New**	**New**	ORP
130	CONF.ASSESSMENT	-	Security Assessment	**New**	**New**	**New**	**New**	**New**	ORP, STIG
131	NET.ENCRYPTION	NET.ENCRYPTION	Network Encryption	Yes	Yes	No	No	No	ORP, CIS, STIG
132	NET.INVITEDNODES	NET.INVITEDNODES	Client Nodes	No	No	No	No	No	ORP, STIG
133	NET.CONNECTIONLIMITS	NET.CONNECTIONLIMITS	Connection Limits Configuration	No	No	No	No	No	STIG
134	NET.LISTENERCONFIG	NET.LISTENERCONFIG	Network Listener Configuration	No	No	No	No	No	ORP, CIS, STIG
135	NET.LISTENERLOG	NET.LISTENERLOG	Listener Logging Control	No	No	No	No	No	ORP
136	OS.INSTALLATIONUSER	OS.INSTALLATIONUSER	Installation Account	No	No	No	No	No	ORP, STIG
137	OS.AUTH	OS.AUTH	OS Authentication	No	No	No	No	No	ORP, STIG
138	OS.MULTIDB	OS.MULTIDB	Segregation of Production and Development Databases	No	No	No	No	No	STIG
139	OS.PMON	OS.PMON	Process Monitor Processes	No	No	No	No	No	ORP
140	OS.AGENT	OS.AGENT	Agent Processes	No	No	No	No	No	ORP

Figure 1-28 DBSAT Target Specific Checks and Recommendations (continued)

141	OS.LISTENER	OS.LISTENER	Listener Processes	No	Yes	No	No	No	STIG
142	OS.LISTENERPORTS	-	Listener Ports	**New**	**New**	**New**	**New**	**New**	STIG
143	OS.CMANLOCAL	OS.CMANLOCAL	CMAN Remote Admin	No	No	No	No	No	ORP, STIG
144	OS.DIAGNOSTICDEST	OS.DIAGNOSTICDEST	Diagnostic Destination	No	No	No	No	No	ORP, STIG
145	OS.FILEPERMISSIONS	OS.FILEPERMISSIONS	File Permissions in ORACLE_HOME	Yes	Yes	No	No	No	ORP, STIG

(1) - Improved the finding logic.

(2) - Improved the remarks text.

(3) - Improved finding rules and/or remarks to specifically target ADB-S. No - The finding applies but it does not include any change as it was not required. No - Finding is not applicable.

(4) - Improved finding rules and/or remarks to specifically target ADB-D. No - The finding applies but it does not include any change as it was not required. No - Finding is not applicable..

(5) - Improved finding rules and/or remarks to specifically target DBCS EE/HP/EP. No - The finding applies but it does not include any change as it was not required.

Appendix B

You can troubleshoot Oracle Database Security Assessment Tool by using diagnostics and log files.

B.1 Enabling DBSAT Diagnostics to diagnose Oracle Database Security Assessment Tool Errors

Output diagnostics, which the DBSAT generates, capture vital information to help you debug errors.

By default, DBSAT suppresses errors that do not impact the report execution. To find details on errors that might affect your collection or report generation, please run dbsat with the `-d` option.

Example of a dbsat report run with `-d`:

```
$ dbsat report -n -d orcl

Database Security Assessment Tool version 4.1 (Dec 2025)

This tool is intended to assist you in securing your Oracle database
system. You are solely responsible for your system and the effect and
results of the execution of this tool (including, without limitation,
any damage or data loss). Further, the output generated by this tool may
include potentially sensitive system configuration data and information
that could be used by a skilled attacker to penetrate your system. You
are solely responsible for ensuring that the output of this tool,
including any generated reports, is handled in accordance with your
company's policies.

Traceback (most recent call last):
  File "sa", line 18953, in <module>
  File "sa", line 1965, in patch_checks
ValueError: could not convert string to float: '1.2.3'

Oracle AI Database 26ai replaces Oracle Database 23ai starting with RU
23.26.0 (Oct 2025), which followed RU 23.9 (Jul 2025).
DBSAT Reporter ran successfully.
```

Example of a standard run:

```
$ ./dbsat report -n -d orcl

Database Security Assessment Tool version 4.1 (Dec 2025)

This tool is intended to assist you in securing your Oracle database
system. You are solely responsible for your system and the effect and
results of the execution of this tool (including, without limitation,
any damage or data loss). Further, the output generated by this tool may
```

```
include potentially sensitive system configuration data and information
that could be used by a skilled attacker to penetrate your system. You
are solely responsible for ensuring that the output of this tool,
including any generated reports, is handled in accordance with your
company's policies.

Oracle AI Database 26ai replaces Oracle Database 23ai starting with RU
23.26.0 (Oct 2025), which followed RU 23.9 (Jul 2025).
DBSAT Reporter ran successfully.
```

B.2 DBSAT Reporter Fails With "No JSON object could be decoded"

If execute on package `SYS.DBMS_SQL` was revoked from `PUBLIC` you can encounter this issue.

```
$ ./dbsat report -a -n orcl

Database Security Assessment Tool version 4.1 (Dec 2025)

This tool is intended to assist you in securing your Oracle database
system. You are solely responsible for your system and the effect and
results of the execution of this tool (including, without limitation,
any damage or data loss). Further, the output generated by this tool may
include potentially sensitive system configuration data and information
that could be used by a skilled attacker to penetrate your system. You
are solely responsible for ensuring that the output of this tool,
including any generated reports, is handled in accordance with your
company's policies.

... Unable to process input file: orcl.json No JSON object could be
decoded Error:
Unexpected error occurred while running DBSAT Reporter.

Oracle AI Database 26ai replaces Oracle Database 23ai starting with RU
23.26.0 (Oct 2025), which followed RU 23.9 (Jul 2025).
DBSAT Reporter ran successfully.
```

To avoid this error, grant execute privilege on `DBMS_SQL` to the DBSAT database user (and not use PUBLIC privilege) used in `dbsat collect <user>@<service_name> <output-file>`

```
SQL> grant execute on sys.dbms_sql to <user> ;
```

Run `dbsat collect` again to ensure the data is collected appropriately and then run the report.

```
./dbsat collect <user>@<service_name> <output-file>

./dbsat report <output-file>
```

Note: make sure JSON is not invalid or corrupt. Review the json file and/or run the collector.

B.3 DBSAT Reporter Fails – Generic
Occasionally, the source of the issue affecting the DBSAT report's successful execution is present in the collector-generated file. As a troubleshooting step, you can open the file (dbsat extract <*filename*>) generated by DBSAT collect and search the file for errors.

B.4 Issues running DBSAT on AIX platforms
AIX default shell is the Korn shell (`ksh`). DBSAT needs to run under the bash shell. You can either change it to `bash` or install it. DBSAT fails to run under other shells. As an example, if you do not have `bash` shell installed on AIX, and you try to run DBSAT, you can encounter the following:

```
oraprod>./dbsat

ksh: ./dbsat: not found

oraprod>pwd

/home/oraprod/dbsat400
```

At this point, you can install `bash` on AIX or run DBSAT collect remotely. You can execute DBSAT from another server with `bash` (e.g., a linux server), reaching the database running on AIX:

```
./dbsat collect <user>@<service_name> <output-file>
```

When collecting from a remote server, DBSAT will not include Operating System-related findings.

B.5 DBSAT taking too long or not completing
If DBSAT collect is taking too long to complete or not completing at all, you can limit the number of rows collected by using the `-r` option:

```
./dbsat collect -r <row_limit> <user>@<service_name> <output-file>
```

Appendix C

Attribution for Third-Party Licenses

For third party technology that you receive from Oracle in binary form which is licensed under an open source license that gives you the right to receive the source code for that binary, you can obtain a copy of the applicable source code from this page. If the source code for the technology was not provided to you with the binary, you can also receive a copy of the source code on physical media by submitting a written request to:

```
Oracle America, Inc.
Attn: Associate General Counsel
Development and Engineering Legal
500 Oracle Parkway, 10th Floor
Redwood Shores, CA 94065
```

Or, you may send an email to Oracle using this form. Your request should include:

```
The name of the component or binary file(s) for which you are requesting the
source code
The name and version number of the Oracle product
The date you received the Oracle product
Your name
Your company name (if applicable)
Your return mailing address and email
A telephone number in the event we need to reach you
```

We may charge you a fee to cover the cost of physical media and processing. Your request must be sent (i) within three (3) years of the date you received the Oracle product that included the component or binary file(s) that are the subject of your request, or (ii) in the case of code licensed under the GPL v3, for as long as Oracle offers spare parts or customer support for that product model

XlsxWriter, Version: 3.2.9

```
BSD 2-Clause License

Copyright (c) 2013-2025, John McNamara <jmcnamara@cpan.org>
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are
met:

1. Redistributions of source code must retain the above copyright
notice, this list of conditions
and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions
and the following disclaimer in the documentation and/or other
materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS
IS" AND ANY EXPRESS OR
IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
WARRANTIES OF MERCHANTABILITY AND
FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE
COPYRIGHT HOLDER OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE,
```

DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER
IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF
THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Eclipse Public License - v 2.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS ECLIPSE PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. DEFINITIONS

"Contribution" means:

a) in the case of the initial Contributor, the initial content Distributed under this Agreement, and

b) in the case of each subsequent Contributor:
i) changes to the Program, and
ii) additions to the Program;
where such changes and/or additions to the Program originate from and are Distributed by that particular Contributor. A Contribution "originates" from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include changes or additions to the Program that are not Modified Works.

"Contributor" means any person or entity that Distributes the Program.

"Licensed Patents" mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions Distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement or any Secondary License (as applicable), including Contributors.

"Derivative Works" shall mean any work, whether in Source Code or other form, that is based on (or derived from) the Program and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship.

"Modified Works" shall mean any work in Source Code or other form that results from an addition to, deletion from, or modification of the contents of the Program, including, for purposes of clarity any new file

in Source Code form that contains any contents of the Program. Modified Works shall not include works that contain only declarations, interfaces, types, classes, structures, or files of the Program solely in each case in order to link to, bind by name, or subclass the Program or Modified Works thereof.

"Distribute" means the acts of a) distributing or b) making available in any manner that enables the transfer of a copy.

"Source Code" means the form of a Program preferred for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Secondary License" means either the GNU General Public License, Version 2.0, or any later versions of that license, including any exceptions or additional permissions as identified by the initial Contributor.

2. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, Distribute and sublicense the Contribution of such Contributor, if any, and such Derivative Works.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in Source Code or other form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to Distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

e) Notwithstanding the terms of any Secondary License, no Contributor makes additional grants to any Recipient (other than those set forth in this Agreement) as a result of such Recipient's receipt of the Program under the terms of a Secondary License (if permitted under the terms of Section 3).

3. REQUIREMENTS

3.1 If a Contributor Distributes the Program in any form, then:

a) the Program must also be made available as Source Code, in accordance with section 3.2, and the Contributor must accompany the Program with a statement that the Source Code for the Program is available under this Agreement, and informs Recipients how to obtain it in a reasonable manner on or through a medium customarily used for software exchange; and

b) the Contributor may Distribute the Program under a license different than this Agreement, provided that such license:

i) effectively disclaims on behalf of all other Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all other Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) does not attempt to limit or alter the recipients' rights in the Source Code under section 3.2; and

iv) requires any subsequent distribution of the Program by any party to be under a license that satisfies the requirements of this section 3.

3.2 When the Program is Distributed as Source Code:

a) it must be made available under this Agreement, or if the Program (i) is combined with other material in a separate file or files made available under a Secondary License, and (ii) the initial Contributor attached to the Source Code the notice described in Exhibit A of this Agreement, then the Program may be made available under the terms of such Secondary Licenses, and

b) a copy of this Agreement must be included with each copy of the Program.

3.3 Contributors may not remove or alter any copyright, patent, trademark, attribution notices, disclaimers of warranty, or limitations of liability ("notices") contained within the Program from any copy of the Program which they Distribute, provided that Contributors may add their own appropriate notices.

4. COMMERCIAL DISTRIBUTION

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program
in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control,
and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance
claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, AND TO THE EXTENT PERMITTED BY APPLICABLE LAW, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the

appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, AND TO THE EXTENT PERMITTED BY APPLICABLE LAW, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software
or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. The Eclipse Foundation is the initial Agreement Steward. The Eclipse Foundation may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing

version number. The Program (including Contributions) may always be Distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published,
Contributor may elect to Distribute the Program (including its Contributions) under the new version.

Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved. Nothing in this Agreement is intended to be enforceable by any entity that is not a Contributor or Recipient. No third-party beneficiary rights are created under this Agreement.

Exhibit A - Form of Secondary Licenses Notice

"This Source Code may also be made available under the following Secondary Licenses when the conditions for such availability set forth in the Eclipse Public License, v. 2.0 are satisfied: {name license(s), version(s), and exceptions or additional permissions here}."

  Simply including a copy of this Agreement, including this Exhibit A is not sufficient to license the Source Code under Secondary Licenses.

  If it is not possible or desirable to put the notice in a particular file, then You may include the notice in a location (such as a LICENSE file in a relevant directory) where a recipient would be likely to look for such a notice.

  You may add additional accurate notices of copyright ownership.

The GNU General Public License (GPL) Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor
Boston, MA 02110-1335
USA

Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public

License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term

"modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

    a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

    b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

    c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

    a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

    b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

    c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise

to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be

a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

    One line to give the program's name and a brief idea of what it does.
    Copyright (C) <year> <name of author>

    This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

    This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

    You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1335 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

    Gnomovision version 69, Copyright (C) year name of author
    Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'. This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision' (which makes passes at compilers) written by James Hacker.

signature of Ty Coon, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

CLASSPATH EXCEPTION
Linking this library statically or dynamically with other modules is making a combined work based on this library. Thus, the terms and conditions of the GNU General Public License version 2 cover the whole combination.

As a special exception, the copyright holders of this library give you permission to link this library with independent modules to produce an executable, regardless of the license terms of these independent modules, and to copy and distribute the resulting executable under terms of your choice, provided that you also meet, for each linked independent module, the terms and conditions of the license of that module. An independent module is a module which is not derived from or based on this library. If you modify this library, you may extend this exception to your version of the library, but you are not obligated to do so. If you do not wish to do so, delete this exception statement from your version.

Eclipse Public License - v 2.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS ECLIPSE PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. DEFINITIONS

"Contribution" means:

a) in the case of the initial Contributor, the initial content Distributed under this Agreement, and

b) in the case of each subsequent Contributor:
i) changes to the Program, and
ii) additions to the Program;
where such changes and/or additions to the Program originate from and are Distributed by that particular Contributor. A Contribution

"originates" from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include changes or additions to the Program that are not Modified Works.

"Contributor" means any person or entity that Distributes the Program.

"Licensed Patents" mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions Distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement or any Secondary License (as applicable), including Contributors.

"Derivative Works" shall mean any work, whether in Source Code or other form, that is based on (or derived from) the Program and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship.

"Modified Works" shall mean any work in Source Code or other form that results from an addition to, deletion from, or modification of the contents of the Program, including, for purposes of clarity any new file in Source Code form that contains any contents of the Program. Modified Works shall not include works that contain only declarations, interfaces, types, classes, structures, or files of the Program solely in each case in order to link to, bind by name, or subclass the Program or Modified Works thereof.

"Distribute" means the acts of a) distributing or b) making available in any manner that enables the transfer of a copy.

"Source Code" means the form of a Program preferred for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Secondary License" means either the GNU General Public License, Version 2.0, or any later versions of that license, including any exceptions or additional permissions as identified by the initial Contributor.

2. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, Distribute and sublicense the Contribution of such Contributor, if any, and such Derivative Works.

b) Subject to the terms of this Agreement, each Contributor hereby

grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in Source Code or other form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to Distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

e) Notwithstanding the terms of any Secondary License, no Contributor makes additional grants to any Recipient (other than those set forth in this Agreement) as a result of such Recipient's receipt of the Program under the terms of a Secondary License (if permitted under the terms of Section 3).

3. REQUIREMENTS

3.1 If a Contributor Distributes the Program in any form, then:

a) the Program must also be made available as Source Code, in accordance with section 3.2, and the Contributor must accompany the Program with a statement that the Source Code for the Program is available under this Agreement, and informs Recipients how to obtain it in a reasonable manner on or through a medium customarily used for software exchange; and

b) the Contributor may Distribute the Program under a license different than this Agreement, provided that such license:
   i) effectively disclaims on behalf of all other Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness

for a particular purpose;

ii) effectively excludes on behalf of all other Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) does not attempt to limit or alter the recipients' rights in the Source Code under section 3.2; and

iv) requires any subsequent distribution of the Program by any party to be under a license that satisfies the requirements of this section 3.

3.2 When the Program is Distributed as Source Code:

a) it must be made available under this Agreement, or if the Program (i) is combined with other material in a separate file or files made available under a Secondary License, and (ii) the initial Contributor attached to the Source Code the notice described in Exhibit A of this Agreement, then the Program may be made available under the terms of such Secondary Licenses, and

b) a copy of this Agreement must be included with each copy of the Program.

3.3 Contributors may not remove or alter any copyright, patent, trademark, attribution notices, disclaimers of warranty, or limitations of liability ("notices") contained within the Program from any copy of the Program which they Distribute, provided that Contributors may add their own appropriate notices.

4. COMMERCIAL DISTRIBUTION

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program
in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to

control,
and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance
claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, AND TO THE EXTENT PERMITTED BY APPLICABLE LAW, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, AND TO THE EXTENT PERMITTED BY APPLICABLE LAW, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against any entity

(including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software
or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. The Eclipse Foundation is the initial Agreement Steward. The Eclipse Foundation may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be Distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published,
Contributor may elect to Distribute the Program (including its Contributions) under the new version.

Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved. Nothing in this Agreement is intended to be enforceable by any entity that is not a Contributor or Recipient. No third-party beneficiary rights are created under this Agreement.

Exhibit A - Form of Secondary Licenses Notice

"This Source Code may also be made available under the following Secondary Licenses when the conditions for such availability set forth in the Eclipse Public License, v. 2.0 are satisfied: {name license(s), version(s), and exceptions or additional permissions here}."

Simply including a copy of this Agreement, including this Exhibit A is not sufficient to license the Source Code under Secondary Licenses.

If it is not possible or desirable to put the notice in a particular file, then You may include the notice in a location (such as a LICENSE

```
file in a relevant directory) where a recipient would be likely to
look for such a notice.

You may add additional accurate notices of copyright ownership.
```

Licensing Information User Manual Oracle GraalVM for JDK 23

Oracle GraalVM for JDK 23
