Oracle® Database

Security Assessment Tool User Guide

Release 2.0.2

E72220-05

July 2018

About the Oracle Database Security Assessment Tool

The Oracle Database Security Assessment Tool (DBSAT) analyzes database configurations, users, their entitlements, security policies and identifies where sensitive data resides to uncover security risks and improve the security posture of Oracle Databases within your organization.

You can use DBSAT report findings to:

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

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 and CIS benchmark recommendations.
- 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 light weight utility that will not impair system performance in a measurable way.

Database Security Assessment Tool Components

The Database Security Assessment Tool (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.

- **Reporter:**

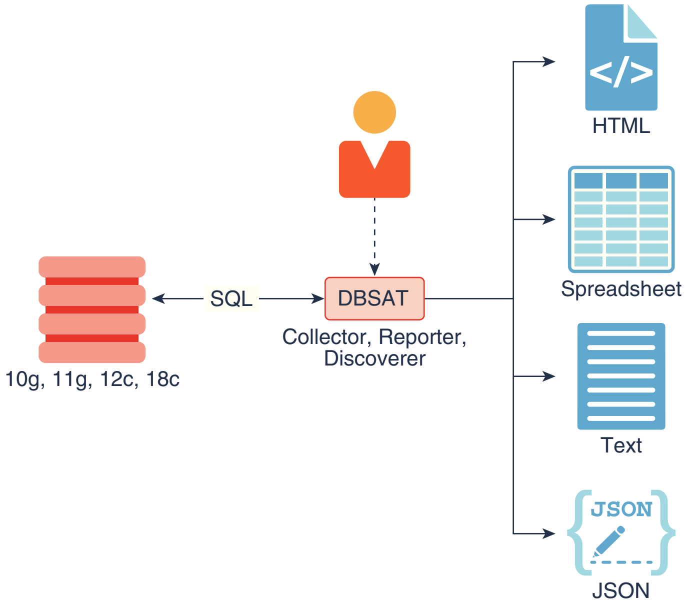
  The **Reporter** analyzes the collected data and generates a Database Security Assessment Report in HTML, Excel, JSON, and Text formats. The Reporter can run on any machine: PC, laptop, or server. You are not limited to running the Reporter on the database server or the same machine as the Collector.

- **Discoverer:**

  The **Discoverer** executes SQL queries and collects data from the system 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 a Database Sensitive Data Assessment Report in HTML and CSV 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 Database Security Assessment Tool.

Figure DBSAT Components, Sources, and Reports



For more information about the Collector, Reporter, and Discoverer, see Using the Database Security Assessment Tool (page 7).

Prerequisites

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

- Supported Operating Systems (page 3)
- Supported Database Versions (page 4)
- Security Requirements (page 4)
- Database Security Assessment Tool Prerequisites (page 4)

Supported Operating Systems

The database configuration collection queries run on most supported Oracle Database platforms. However, currently the OS data collection will be skipped on Windows platforms.

DBSAT runs on:

- Solaris x64 and Solaris SPARC64
- Linux x86-64
- Windows x64

- HP-UX IA (64-bit)
- IBM AIX (64-bit) & Linux on zSeries (64-bit)

Supported Database Versions

You can run the DBSAT tool on Oracle Database 10.2.0.5 and later releases.

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 on a short-term basis and revoke these when no longer necessary.

> **Caution:**
>
> This tool is intended to assist in 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.

Database Security Assessment Tool Prerequisites

DBSAT uses Zip and Unzip to compress or decompress the generated files. DBSAT searches for Zip and Unzip utilities in the default locations shown below. In order to use other Zip and Unzip utilities, update the following lines in the relevant script.

Windows (dbsat.bat script):

```
SET ZIP_CMD=%ORACLE_HOME%\bin\zip.exe
SET UNZIP_CMD=%ORACLE_HOME%\bin\unzip.exe
```

Note:

The Unzip utility is not included in Oracle Database 12.2 and higher. Ensure that you have installed an utility such as WinZip or WinRar, and add the path to the utility in the `SET UNZIP_CMD` parameter.

All other platforms (dbsat script):

```
ZIP=/usr/bin/zip
UNZIP=/usr/bin/unzip
DBZIP=${ORACLE_HOME}/bin/zip
```

The following are the prerequisites for the components of the Database Security Assessment Tool:

- Collector Prerequisites (page 5)
- Reporter Prerequisites (page 6)
- Discoverer Prerequisites (page 6)

Collector Prerequisites

In order to collect complete data, the DBSAT Collector must be run on the server that contains the database, because it executes some operating system commands to collect process and file system information that cannot be obtained from the database. In addition, the DBSAT Collector must be run as an OS user with read permissions on files and directories under `ORACLE_HOME` in order to collect and process file system data using OS commands.

The 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. You can grant the DBSAT user the individual privileges in the following list, or you can grant this user the DBA role plus the `DV_SECANALYST` role if needed.

If you plan to run only the Discoverer component, you can use just the privileges marked with an asterisk (*) below.

Required privileges and roles:

- `CREATE SESSION`*
- `READ` or `SELECT` on `SYS.REGISTRY$HISTORY`
- Role `SELECT_CATALOG_ROLE`*
- Role `DV_SECANALYST`* (if Database Vault is enabled)
- Role `AUDIT_VIEWER` (12*c* and later)
- Role `CAPTURE_ADMIN` (12*c* and later)
- `READ` or `SELECT` on `SYS.DBA_USERS_WITH_DEFPWD` (11*g* and later)
- `READ` or `SELECT` on `AUDSYS.AUD$UNIFIED` (12*c* and later)

Note:

In order to successfully collect Database Vault information in a Database Vault protected environment, you must connect as a non-SYS user with the DV_SECANALYST role.

Reporter Prerequisites

The Reporter is a platform-independent Python program and requires Python 2.6 or later to run.

Discoverer Prerequisites

The Discoverer is a Java program and requires the Java Runtime Environment (JRE) 1.8 (jdk8-u172) or later to run.

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 (page 5).

Note:

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 Database Security Assessment Tool

To install the Database Security Assessment Tool (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.

The Database Security Assessment Tool (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 Database Security Assessment Tool

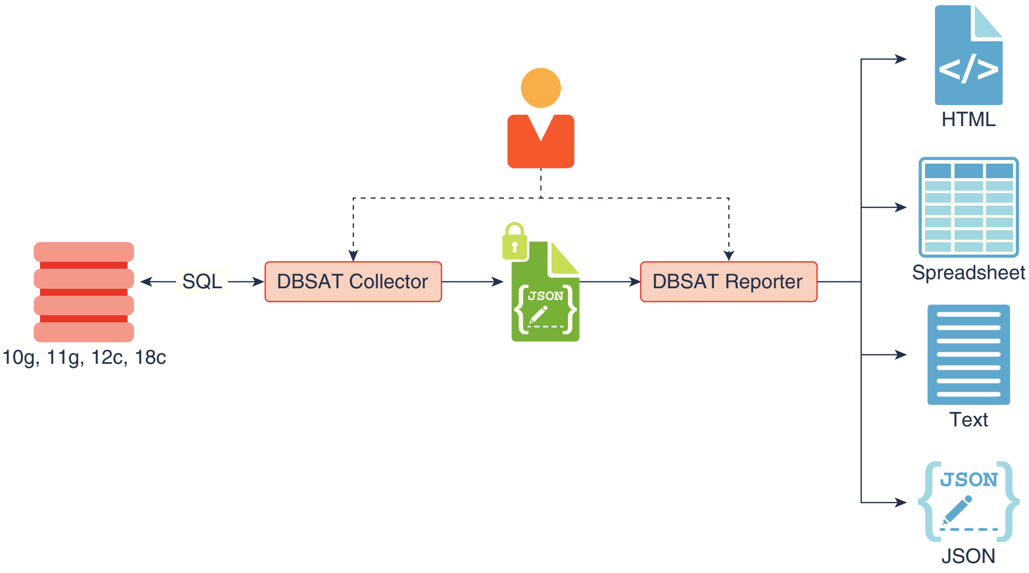
You can generate the following reports with the Collector, Reporter, and Discoverer components:

Database Security Assessment Report

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

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

Figure Collector and Reporter Components and Architecture

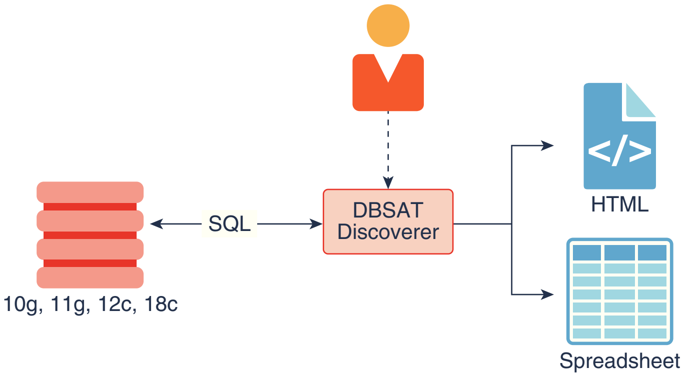


Database Sensitive Data Assessment Report

The Discoverer component is used to generate a Database Sensitive Data Assessment Report.

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

Figure   Discoverer Components and Architecture



The following sections describe how to run these components:

- Running the Collector (page 8)
- Running the Reporter (page 9)
- Using the Discoverer (page 11)

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 <connect_string> <destination>
   ```

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

   - *`connect_string`*

     Specifies the connection string to connect to the database.

     Example: `dbsat@orcl`

   - *`destination`*

     Specifies the location and file name for the Database Security Assessment report.

     Example: `/home/oracle/dbsat/db04`

2. Run the Collector.

   ```
   $ ./dbsat collect dbsat@orcl db04
   ```

   The following output is displayed:

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

   Enter password:

   SQL*Plus: Release 12.2.0.1.0 Production on Mon Jan 15 08:06:53 2018

   Copyright (c) 1982, 2016, Oracle.  All rights reserved.

   Last Successful login time: Tue Jan 09 2018 07:08:47 -05:00

   Connected to:
   Oracle Database 12c Enterprise Edition Release 12.2.0.1.0 - 64bit Production
   Setup complete.
   SQL queries complete.
   OS commands complete.
   Disconnected from Oracle Database 12c Enterprise Edition Release 12.2.0.1.0 -
   64bit Production
   DBSAT Collector completed successfully.

   Calling /u01/app/oracle/product/12.2/db_1/bin/zip to encrypt db04.json...
   Enter password:
   Verify password:
     adding: db04.json (deflated 87%)
   zip completed successfully.
   [oracle@db04 201]$
   ```

   > **Note:**
   >
   > If you do not want to encrypt the file invoke the `dbsat collect` script with the `-n` option. This is not recommended.
   >
   > 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.

Running the Reporter

The Reporter analyses 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 Python version is 2.6 or later is installed.

```
[oracle@db04 sat]$ python -V
```

A similar output is displayed:

```
Python 2.7.11rc1
```

2. Specify the arguments to run the Reporter.

   ```
   $ dbsat report [-a] [-n] [-x <section>] <pathname>
   ```

   Where the argument *`pathname`* stands for the full or relative path name to the data file `db04` 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` means: include all the database user accounts in the analysis. (Locked Oracle-supplied accounts are excluded by default as they cannot be used to connect to the database.)
   - `-n` means: do not encrypt the reports generated by the analysis.
   - `-x` means: exclude a section from the report. Valid sections are:
     - `USER` : **User Accounts**
     - `PRIV` : **Privileges and Roles**
     - `AUTH` : **Authorization Control**
     - `CRYPT` : **Data 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 db04
   ```

   The following output appears:

   ```
   Archive:  db04.zip
   [db04.zip] db04.json password:
     inflating: db04.json
   DBSAT Reporter ran successfully.
   ```

```
Calling /usr/bin/zip to encrypt the generated reports...
Enter password:
Verify password:
    zip warning: db04_report.zip not found or empty
  adding: db04_report.txt (deflated 82%)
  adding: db04_report.html (deflated 86%)
  adding: db04_report.xlsx (deflated 3%)
  adding: db04_report.json (deflated 85%)
zip completed successfully.
```

4. Specify a password for the `.zip` file.

   The `.zip` file is created.

   > **Note:**
   >
   > The `.zip` file is used for Reporter and Discoverer output. To avoid confusion, it is recommended that you use the same password while creating both outputs.

5. Extract the contents of the `.zip` file to access the Database Security Assessment Report. When prompted, enter the password for the `.zip` file specified in Step *4*.

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

Using the Discoverer

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.

Topics:

- Configuring the Discoverer (page 11)
- Running the Discoverer (page 22)

Configuring the Discoverer

Before running the Discoverer, perform the following steps:

- Configure dbsat.config (page 11)
- Configure the Pattern file (page 16)
- Configure the Exclusion List file (page 20)
- Configure Certificates and Wallets (page 21)

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–specifc requirements. For example, you can rename the file `custom_dbsat.config`.

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

3. Open `dbsat.config`.

   The following are the contents of the configuration file:

   ```
   [Database]
       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_en.ini
       schemas_scope = ALL
       minrows = 1
       exclusion_list_file =

   [Sensitive Category]
       PII = High Risk
       PII - Address = High Risk
       PII - IDs = High Risk
       PII - IT Data = High Risk
       PII-Linked = Medium Risk
       PII-Linked - Birth Details = Medium Risk
       Job Data = Medium Risk
       Financial Data - PCI = High Risk
       Financial Data - Banking = Medium Risk
       Health Data = Medium Risk
   ```

4. Configure the settings. For more information about the configuration settings, see Configuration Settings (page 13).
5. Save and close the configuration file.

The following table describes the configuration settings in the `dbsat.config` file:

Section	Key	Value	Description
[Database]	`DB_HOSTNAME`	`<hostname> | <ip_address>`	Hostname or IP Address of the target database server
	`DB_PORT`	`<port number>` 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`.
	`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 a 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 a 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.
`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`.	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 (page 16).
	`SCHEMAS_SCOPE`	`ALL | <schema1>,<schema2>` The default is `ALL`.	Specifies the schemas to be scanned. Multiple schemas can be specified as a comma-separated list.
	`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 (page 20).
[Sensitive_Category]			The **[Sensitive_Category]** section defines which Sensitive Categories are used. The default 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 (page 16).

Pattern File Configuration

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

Topics:

- About Sensitive Types (page 16)
- Customizing the Pattern File (page 17)
- About Regular Expressions (page 18)

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 = ^(PERSON|FULL).*NAME$
COL_COMMENT_PATTERN = (Full|Person).*Name
SENSITIVE_CATEGORY = PII
```

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 Database Sensitive Data Assessment Report (page 26).

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 (page 13).

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_en.ini file and rename the file my_sensitive_en.ini.

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 (page 16) and Configuration Settings (page 13).

5. Save and close my_sensitive_en.ini.

   The Pattern file is configured.

6. Include my_sensitive_en in the Discoverer scan by adding a reference to the file in the mydbsat.config file.

   ```
   sensitive_pattern_files = my_sensitive_en.ini
   ```

For more information about referencing the Pattern file in the mydbsat.config file, see Configuring dbsat.config (page 11).

About Regular Expressions

The search parameters are defined using Regular Expressions such as Character Classes, Quantifiers, and Boundary Matchers. Regular Expressions are used to specify COL_NAME_PATTERN and COL_COMMENT_PATTERN parameters.

Commonly used Regular Expressions are:

Boundary Matchers

Boundary Matchers are used to make pattern matches more precise by specifying the location in the string to search for the pattern match.

Table Boundary Matchers

Boundary Matchers

Boundary Construct	Description
^	Searches for the specified text at the beginning of a string (starts with search). **Example:** ^VISA searches for database column names and column comments beginning with VISA.
$	Searches for the specified text at the end of a string (ends with search). **Example:** DATUM$ searches for database column names and column comments ending with DATUM.

Table (Cont.) Boundary Matchers

`\b`	Marks a word boundary. Searches for an exact match of the specified text anywhere within a string (`exact match` search). **Example:** `\bAGE\b` searches for database column names and column comments containing `AGE`. The search identifies occurrences such as `EMPLOYEE_AGE` and `AGE_EMPLOYEE`. Occurrences such as `AGEING` and `EMPLOYEEAGE` are ignored.

If no Boundary Matchers are specified, a `contains` search is performed.

Example: `ELECTORAL` searches for database column names and column comments containing `ELECTORAL`. The search identifies occurrences such as `ELECTORAL_ID`, `ID_ELECTORAL`, and `ELECTORALID`.

An `exact match` search can also be performed by using `^` and `$` together.

Example: `^ADDRESS$` searches for database column names and column comments containing `ADDRESS`. The search identifies occurrences such as `PRIMARY_ADDRESS` and `ADDRESS_HOME`. Occurrences such as `ADDRESSES` and `EMPLOYEEADDRESS` are ignored.

For more information about Boundary Matchers, see Boundary Matchers.

Logical Operators

Logical operators are used to specify an `AND` or `OR` search.

Example: `NAME DESIGNATION` searches for database column names and column comments containing `NAME` AND `DESIGNATION`. `NAME | DESIGNATION` searches for database column names and column comments containing `NAME` OR `DESIGNATION`.

Character Classes

Character classes are used to specify a character search. DBSAT supports predefined Regex character classes.

The most used one is the dot (.). The dot (.) searches for database column names and column comments containing any character. Used in conjunction with `*`, the search identifies occurrences of any character any number of times.

Example: `JOB.*` searches for database column names and column comments containing `JOB` followed by any other character.

For more information about Character Classes, see Character Classes.

Quantifiers

Quantifiers allow you to specify the number of occurrences to match against.

Table Quantifiers

Quantifiers

Quantifier	Description
X?	Searches for occurrences of specified text X once or not at all. **Example:** ID_?CARD searches for database column names and column comments containing occurrences such as IDCARD and ID_CARD.
X*	Searches for occurrences of specified text X zero or more times. **Example:** TERM.*DATE searches for database column names and column comments containing occurrences such as TERMINAL_DATE and LAST_TERMIN_DATE.

For more information about Quantifiers, see Quantifiers.

Example Regular Expressions — Examples

The following examples show how to use regular expressions to specify COL_NAME_PATTERN and COL_COMMENT_PATTERN parameters:

```
(^JOB.*(TITLE|PROFILE|POSITION)$)|^POSITION
```

In the example above, the search will identify database column names and column comments beginning with JOB, followed by zero or more occurrences of any character, and ending with TITLE, PROFILE, or POSITION. The search will also identify database column names and column comments beginning with POSITION.

Note:

Use a backslash (“\”) to escape meta characters in regular expressions.

For more information about Regular Expressions, see Regular Expressions.

Configuring the Exclusion List file

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 a file <ignore_list_filename>.ini, and save it in the Discover/conf directory.
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.

The Exclusion List file is configured. You can include the file in the Discoverer scan by adding a reference to the file in the configuration file. For more information about referencing the Exclusion List file, see Configuring dbsat.config (page 11).

Configuring Certificates and Wallets

For increased security, Oracle Database provides Secure Sockets Layer (SSL) support to encrypt the connection between clients and 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 <dbsat.config>] <destination>
   ```

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

   - `-n`

     Specifies that the generated reports are not encrypted.

   - `–c`

     Specifies the name of the configuration file to be used. For more information about the `dbsat.config` file, see Configuring dbsat.config (page 11).

   - `destination`

     Specifies the full or relative path name to create the `.zip` file.

     Example:

     ```
     /home/oracle/dbsat/discover1
     ```

2. Run the Discoverer.

   ```
   $ ./dbsat discover -c Discover/conf/dbsat.config db04
   ```

   The following output is displayed:

   ```
   DBSAT Discover ran successfully.
   Calling /usr/bin/zip to encrypt the generated reports...
   Enter password:
   Verify password:
     adding: db04_discover.html (deflated 86%)
     adding: db04_discover.csv (deflated 86%)
   Zip completed successfully.
   [oracle@db04 201]$
   ```

3. Specify a password for the `.zip` file.

   A zip file named `<destination>_report.zip` is created. If the file `<destination>_report.zip` exists, the discovery results are added to the existing zip file.

   > **Note:**
   >
   > The `.zip` file is used for Reporter and Discoverer output. To avoid confusion, it is recommended that you use the same password while creating both outputs.

4. Extract the contents of the `.zip` file to access the Database Sensitive Data Assessment Report. When prompted, enter the password for the `.zip` file specified in Step *3*.

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

DBSAT Reports

DBSAT produces output in multiple formats for various audiences and purposes.

Topics:

- Database Security Assessment Reports (page 23)
- Database Sensitive Data Assessment Report (page 26)

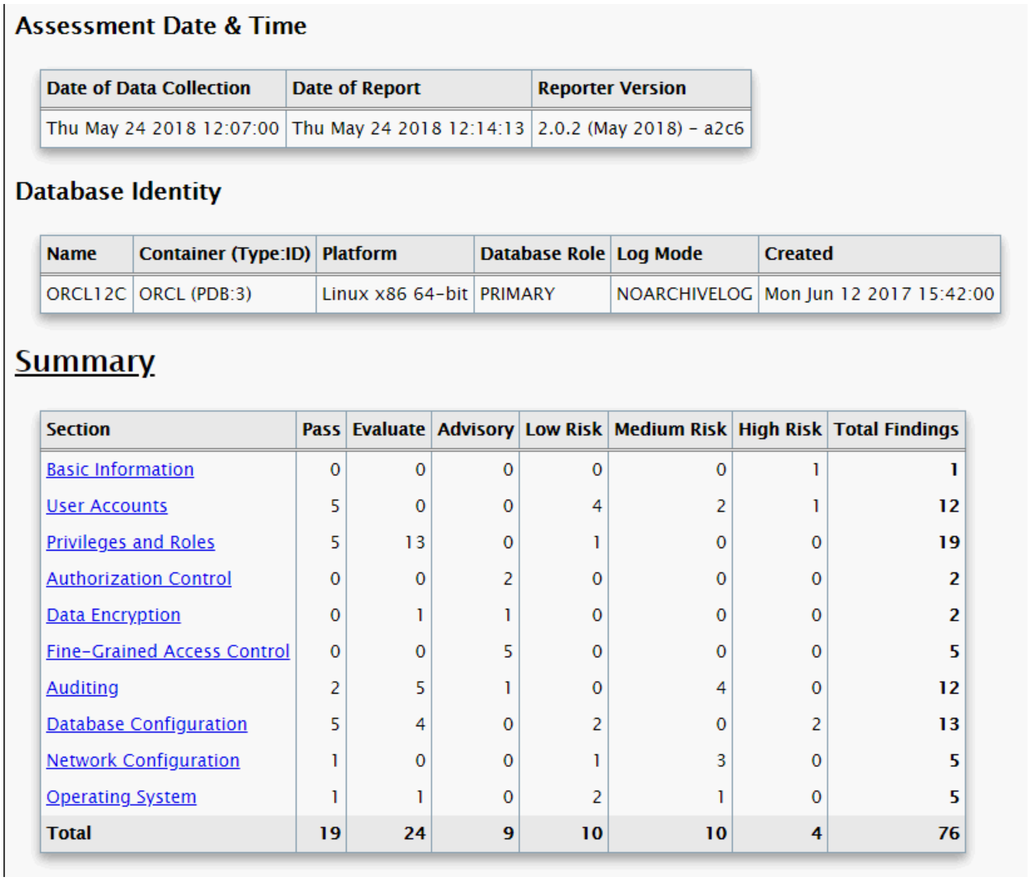
Database Security Assessment Reports

The Collector and Reporter components are used to generate a Database Security Assessment Report in HTML, Excel, JSON, and Text formats.

The HTML report provides detailed results of the assessment 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 usage. Finally, a JSON document containing the report contents is provided for easier filtering, comparison, aggregation, and integration with other tools.

The following figure displays the first three tables of the Database Security Assessment Report — Summary.

Figure Database Security Assessment Report — Summary



Assessment Date & Time

Date of Data Collection	Date of Report	Reporter Version
Thu May 24 2018 12:07:00	Thu May 24 2018 12:14:13	2.0.2 (May 2018) - a2c6

Database Identity

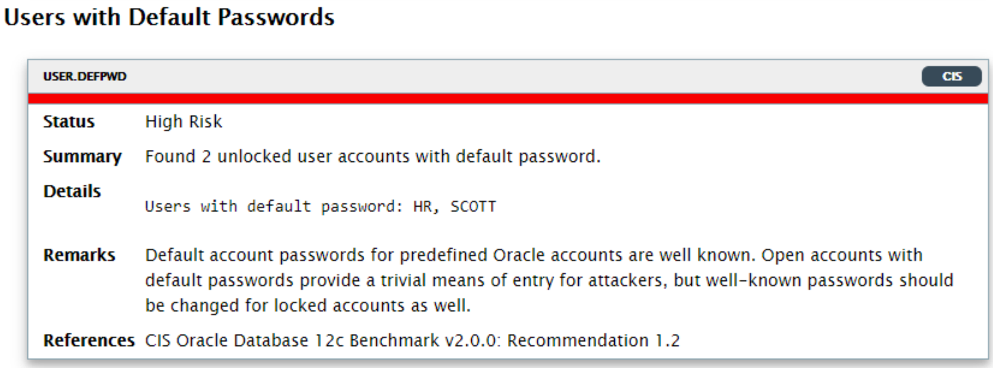
Name	Container (Type:ID)	Platform	Database Role	Log Mode	Created
ORCL12C	ORCL (PDB:3)	Linux x86 64-bit	PRIMARY	NOARCHIVELOG	Mon Jun 12 2017 15:42:00

Summary

Section	Pass	Evaluate	Advisory	Low Risk	Medium Risk	High Risk	Total Findings
Basic Information	0	0	0	0	0	1	**1**
User Accounts	5	0	0	4	2	1	**12**
Privileges and Roles	5	13	0	1	0	0	**19**
Authorization Control	0	0	2	0	0	0	**2**
Data Encryption	0	1	1	0	0	0	**2**
Fine-Grained Access Control	0	0	5	0	0	0	**5**
Auditing	2	5	1	0	4	0	**12**
Database Configuration	5	4	0	2	0	2	**13**
Network Configuration	1	0	0	1	3	0	**5**
Operating System	1	1	0	2	1	0	**5**
Total	**19**	**24**	**9**	**10**	**10**	**4**	**76**

The resulting analysis is reported in units called Findings. An example follows:

Figure Database Security Assessment Report — Users with Default Password



Users with Default Passwords

USER.DEFPWD

Status High Risk

Summary Found 2 unlocked user accounts with default password.

Details

```
Users with default password: HR, SCOTT
```

Remarks Default account passwords for predefined Oracle accounts are well known. Open accounts with default passwords provide a trivial means of entry for attackers, but well-known passwords should be changed for locked accounts as well.

References CIS Oracle Database 12c Benchmark v2.0.0: Recommendation 1.2

Each Finding consists of the following components:

- **Title and Unique ID for the Rule**

  The ID has two parts: the prefix identifies the report section, and the suffix identifies the specific rule.

- **Status**

  You can use the status values as guidelines to implementing DBSAT recommendations. They can be used to prioritize and schedule changes based on the level of risk, and what it might mean to your organization. High risk might require immediate remedial action, whereas other risks might be fixed during a scheduled downtime, or bundled together with other maintenance activities.

  - Pass: no error found
  - Evaluate: needs manual analysis
  - Low Risk
  - Medium Risk
  - High Risk
  - Advisory: improve security posture by enabling additional security features and technology. Poses an opportunity for improvement.

- **Summary**

  A brief summary of the finding. When the finding is informational, the summary typically reports only the number of data elements that were examined.

- **Details**

  Provides detailed information to explain the finding summary, typically results from the assessed database, followed by any recommendations for changes.

- **Remarks**

  Explains the reason for the rule and recommended actions for remediation. It may also explain the recommended actions for remediation if a risk is reported.

- **References**

  Provides information on whether the finding is related to a CIS Oracle Database Benchmark 12c v2.0.0 recommendation or related to a GDPR Article/Recital.

Note:

> These recommendations reflect best practices for database security and should be part of any strategy for Data Protection by Design and by Default. The tool recommendations 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.
>
> Based on Oracle Database security best practices, DBSAT highlights findings that relate to the CIS Oracle Database 12c Benchmark v2.0.0. In some cases DBSAT rules relate to multiple CIS Benchmark recommendations. DBSAT does not execute all CIS Benchmark checks.

Database Sensitive Data Assessment Report

The Discoverer component is used to generate a Database Sensitive Data Assessment Report in HTML and CSV formats.

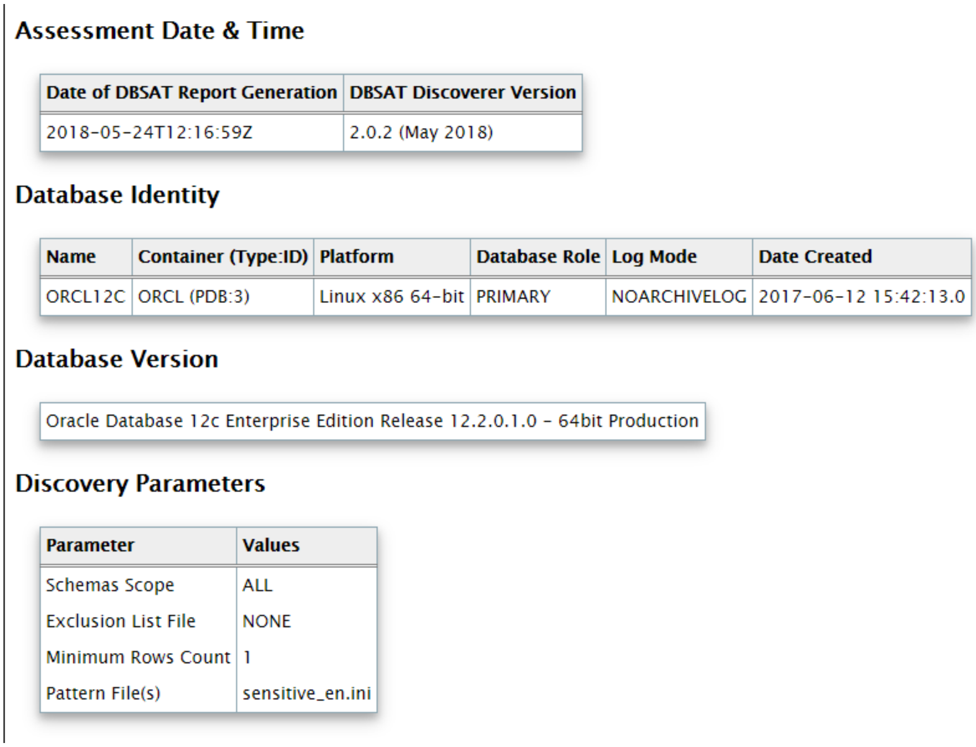
The HTML report is the main report and contains the discovered sensitive data and its categories along with target database information and Discoverer parameters.

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*.

Database Sensitive Data Assessment Report — High-Level Summary

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

Figure Database Sensitive Data Assessment Report — High-Level Summary



Assessment Date & Time

Date of DBSAT Report Generation	DBSAT Discoverer Version
2018-05-24T12:16:59Z	2.0.2 (May 2018)

Database Identity

Name	Container (Type:ID)	Platform	Database Role	Log Mode	Date Created
ORCL12C	ORCL (PDB:3)	Linux x86 64-bit	PRIMARY	NOARCHIVELOG	2017-06-12 15:42:13.0

Database Version

Oracle Database 12c Enterprise Edition Release 12.2.0.1.0 - 64bit Production

Discovery Parameters

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

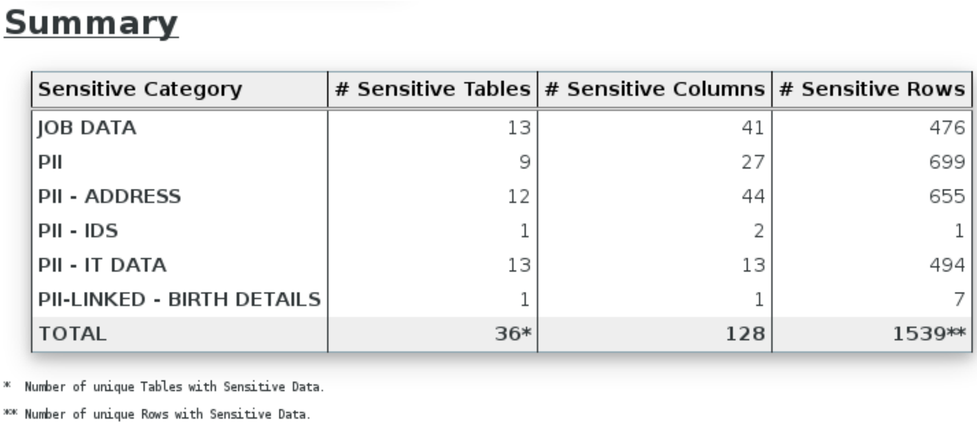
The Database Sensitive Data Assessment Report — High-Level Summary section contains the following information:

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 (page 13).

Database Sensitive Data Assessment Report — Summary

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

Figure Database Sensitive Data Assessment Report — Summary



Summary

Sensitive Category	# Sensitive Tables	# Sensitive Columns	# Sensitive Rows
JOB DATA	13	41	476
PII	9	27	699
PII - ADDRESS	12	44	655
PII - IDS	1	2	1
PII - IT DATA	13	13	494
PII-LINKED - BIRTH DETAILS	1	1	7
TOTAL	36*	128	1539**

* Number of unique Tables with Sensitive Data.

** Number of unique Rows with Sensitive Data.

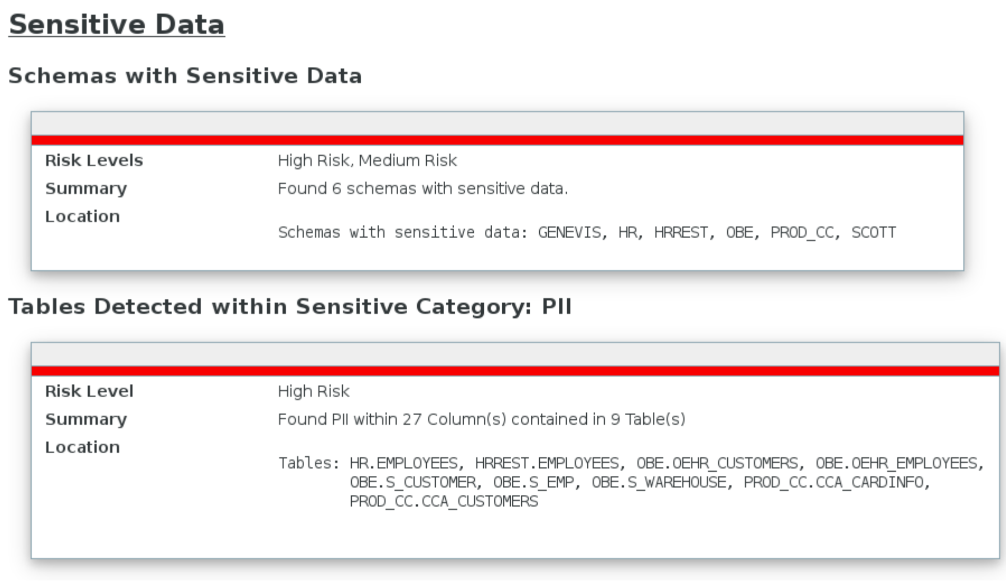
> **Note:**
>
> A single database table could contain columns or column comments that match more than one Sensitive Category, causing a higher number to be displayed in the `# Sensitive Tables` and `# Sensitive Rows` columns. However, the `Total` row displays the unique number of tables and rows identified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

For more information about configuring Sensitive Categories, see Pattern File Configuration (page 16).

Database Sensitive Data Assessment Report — Sensitive Data

The Database Sensitive Data Assessment Report — Sensitive Data section displays information about the schemas and tables containing sensitive data. The following figure displays the information displayed in the Database Sensitive Data Assessment Report — Sensitive Data section.

Figure Database Sensitive Data Assessment Report — Sensitive Data



Sensitive Data

Schemas with Sensitive Data

Risk Levels	High Risk, Medium Risk
Summary	Found 6 schemas with sensitive data.
Location	Schemas with sensitive data: GENEVIS, HR, HRREST, OBE, PROD_CC, SCOTT

Tables Detected within Sensitive Category: PII

Risk Level	High Risk
Summary	Found PII within 27 Column(s) contained in 9 Table(s)
Location	Tables: HR.EMPLOYEES, HRREST.EMPLOYEES, OBE.OEHR_CUSTOMERS, OBE.OEHR_EMPLOYEES, OBE.S_CUSTOMER, OBE.S_EMP, OBE.S_WAREHOUSE, PROD_CC.CCA_CARDINFO, PROD_CC.CCA_CUSTOMERS

Entries for custom sensitive categories will also be present in this report section.

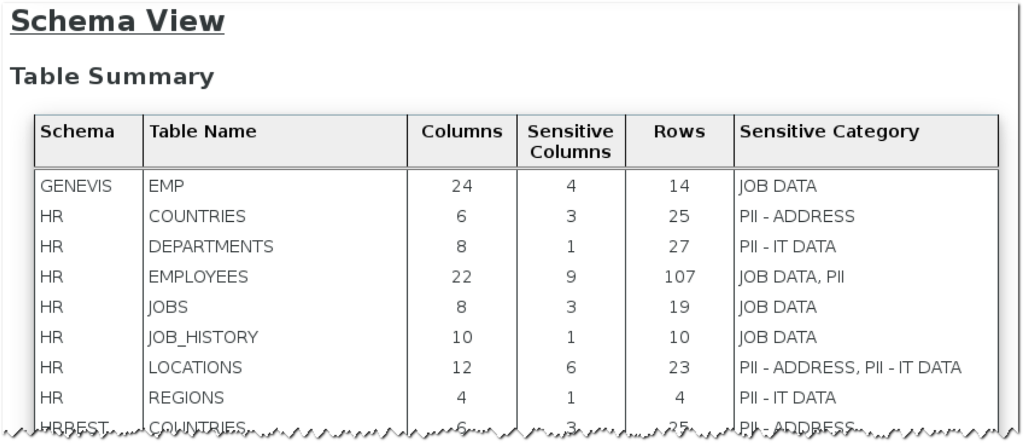
The Database Sensitive Data Assessment Report — Sensitive Data section contains the following information:

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

Database Sensitive Data Assessment Report — Schema View

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

Figure Database Sensitive Data Assessment Report — Schema View



Schema View

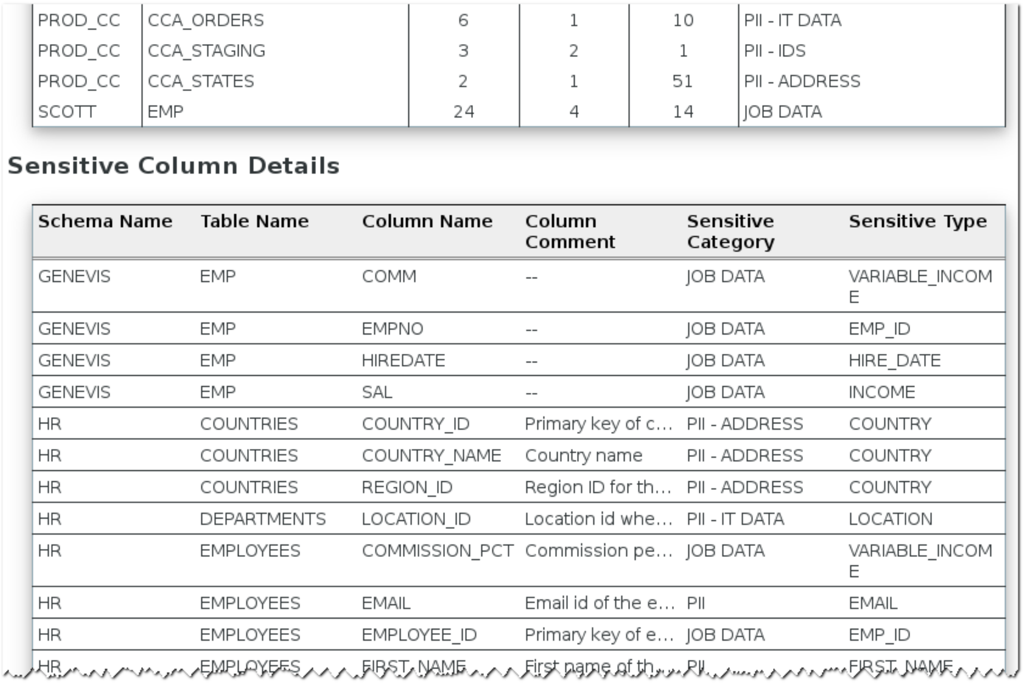
Table Summary

Schema	Table Name	Columns	Sensitive Columns	Rows	Sensitive Category
GENEVIS	EMP	24	4	14	JOB DATA
HR	COUNTRIES	6	3	25	PII - ADDRESS
HR	DEPARTMENTS	8	1	27	PII - IT DATA
HR	EMPLOYEES	22	9	107	JOB DATA, PII
HR	JOBS	8	3	19	JOB DATA
HR	JOB_HISTORY	10	1	10	JOB DATA
HR	LOCATIONS	12	6	23	PII - ADDRESS, PII - IT DATA
HR	REGIONS	4	1	4	PII - IT DATA
HRREST	COUNTRIES	6	3	25	PII - ADDRESS

Database Sensitive Data Assessment Report — Sensitive Column Details

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

Figure Database Sensitive Data Assessment Report — Sensitive Column Details



PROD_CC	CCA_ORDERS	6	1	10	PII - IT DATA
PROD_CC	CCA_STAGING	3	2	1	PII - IDS
PROD_CC	CCA_STATES	2	1	51	PII - ADDRESS
SCOTT	EMP	24	4	14	JOB DATA

Sensitive Column Details

Schema Name	Table Name	Column Name	Column Comment	Sensitive Category	Sensitive Type
GENEVIS	EMP	COMM	--	JOB DATA	VARIABLE_INCOME
GENEVIS	EMP	EMPNO	--	JOB DATA	EMP_ID
GENEVIS	EMP	HIREDATE	--	JOB DATA	HIRE_DATE
GENEVIS	EMP	SAL	--	JOB DATA	INCOME
HR	COUNTRIES	COUNTRY_ID	Primary key of c...	PII - ADDRESS	COUNTRY
HR	COUNTRIES	COUNTRY_NAME	Country name	PII - ADDRESS	COUNTRY
HR	COUNTRIES	REGION_ID	Region ID for th...	PII - ADDRESS	COUNTRY
HR	DEPARTMENTS	LOCATION_ID	Location id whe...	PII - IT DATA	LOCATION
HR	EMPLOYEES	COMMISSION_PCT	Commission pe...	JOB DATA	VARIABLE_INCOME
HR	EMPLOYEES	EMAIL	Email id of the e...	PII	EMAIL
HR	EMPLOYEES	EMPLOYEE_ID	Primary key of e...	JOB DATA	EMP_ID
HR	EMPLOYEES	FIRST_NAME	First name of th...	PII	FIRST_NAME

Sample Script to Create a User with Minimum Privileges

You can create a user with required minimum privileges to run the 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 sys.registry$history to dbsat_user;
grant select on sys.dba_users_with_defpwd to dbsat_user; // 11g and 12c
grant select on audsys.aud$unified to dbsat_user; // 12c only
grant audit_viewer to dbsat_user; // 12c
grant capture_admin to dbsat_user;// 12c covers sys.dba_priv_captures,
sys.priv_capture$, sys.capture_run_log$
```

```
// if Database Vault is enabled, connect as DV_OWNER to run this command
grant DV_SECANALYST to dbsat_user;
```

Known Issues

The following are the Known Issues in Database Security Assessment Tool Release 2.0.2:

- MS Excel Font Size Display (page 32)
- Collector and Reporter - Windows OS Commands (page 32)

MS Excel Font Size Display

Some versions of Microsoft Excel may display text on the screen using a font that is too large to fit in the spreadsheet cells, even though it is sized correctly in printed output. If this happens, you can resize columns to be slightly wider in order to make the text visible.

Collector and Reporter - Windows OS Commands

Data is collected by running SQL queries and operating system commands. 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.

Attribution for Third-Party Licenses

Third-party licenses used in the Database Security Assessment Tool Release 2.0.2.

About 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: 1.0.2

Copyright (c) 2013–2017, 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 OWNER 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.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the FreeBSD Project.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Oracle® Database Security Assessment Tool User Guide, Release 2.0.2
E72220-05