

# Oracle Database Security Assessment Tool FAQ

Protecting business-sensitive and regulated data is mission-critical. However, it is challenging for most organizations to know whether their databases are securely configured, who can access them, and where sensitive data resides. As part of Oracle's defense-in-depth capabilities, Oracle Database Security Assessment Tool (DBSAT) helps identify areas where your database configuration, operation, or implementation introduces risks and recommends changes and controls to mitigate those risks.

## General

### What are the primary use cases for Oracle Database Security Assessment Tool (DBSAT)?

There are three core use cases. Assessing how securely the database is configured, determining who the users and their entitlements are, and identifying where sensitive data resides within the database.

### How does DBSAT work?

DBSAT has three components: Collector, Reporter, and Discoverer. The Collector collects all relevant data from the database that the Reporter then analyzes and generates a *Security Assessment* report. The Discoverer is a stand-alone module that identifies different types of sensitive data in the database and generates a *Sensitive Data Assessment Report*.

### What type of data is collected and analyzed?

DBSAT collects and reports on the following categories of data:

- User accounts, privileges, and roles
- Authorization Control
- Fine-grained Access Control
- Auditing Policies
- Data Encryption
- Database Configuration
- Listener Configuration
- Related Operating System Configuration

To discover the type and quantity of sensitive data in the database, DBSAT Discoverer does pattern matching on column names and column comments. It categorizes sensitive data as follows:

- Identification Information
- Biographic Information
- IT Information
- Financial Information
- Health Information
- Job Information
- Academic Information

The sensitive data categories can be customized to meet different requirements.

### What is the performance impact of running DBSAT?

The performance impact on the database is negligible. DBSAT Collector and Discoverer gather data only from the database configuration files and Oracle data dictionary views. It does not look at the application data.

**How much time does it take to learn how to run DBSAT and analyze the data?**

DBSAT itself is a straightforward command-line tool to use. It takes a few minutes to learn how to run the tool. You could go from Install to Reports in as little as 10 minutes. Databases that contain thousands of database users can take longer to analyze.

**Can I run DBSAT on my databases that are deployed in the Cloud?**

DBSAT can be used whether your database runs on-premises, in Autonomous Databases, customer-managed Database Cloud Services (DBCS), or IaaS-deployed databases. Other prerequisites apply. Please refer to the documentation. If you would like to run an assessment as a service for multiple databases and leverage enterprise features like baselining, drifts, comparisons, history, and alerting, please look at Data Safe. Oracle Data Safe provides Security and User Assessment capabilities.

**Can I run it on Autonomous Databases?**

Yes. DBSAT is certified for Autonomous Data Warehouse Cloud (ADW) and Autonomous Transaction Processing (ATP) databases in serverless, dedicated, or cloud at customer deployment models. Autonomous JSON Database is also certified (AJD).

**Will DBSAT provide me with different recommendations depending on the database type?**

Yes. DBSAT identifies the target type and performs specific checks on whether your databases run on-premises or in-cloud. DBSAT differentiates between on-premises databases, the different Autonomous Databases, and Base Database Service. For these target types, and when applicable, DBSAT provides specific recommendations.

## DBSAT Collector and Reporter

**How do I run the DBSAT Collector?**

The Collector is invoked against an Oracle Database:

```
$ dbsat collect <connect_string> <dest-file>
```

`connect_string` is the connection string for the target database.

`dest-file` is the name of the output file created by the Collector, without the extension suffix.

Here is an example of the command:

```
$ dbsat collect dbsatusr@orcl dbdata
```

As the DBSAT Collector analyzes both database and operating system configuration, it is recommended that you run the DBSAT Collector from the same host where the database server is running.

To get the reports, you need to run the DBSAT reporter (described below).

**How do I run the DBSAT Reporter?**

The DBSAT Reporter can run on any system, including a desktop/laptop with Java Runtime Environment (JRE) 1.8 (jdk8-u172) or later.

```
$ dbsat report <dest-file>
```

The `dest-file` is the JSON/zip file name the Collector produces (without the file extension). The same pathname is used as the base for all report files created by the DBSAT Reporter, with appropriate suffixes added for the Text, HTML, JSON, and XLS report formats. For example,

```
$ dbsat report dbdata
```

**What is a Finding?**

The output of the DBSAT Reporter creates a *Database Security Assessment Report* composed of multiple Findings. Each finding includes suggestions to improve the database security posture or provide information for further analysis. When appropriate, findings also include a reference to the applicable portion of the Oracle Database STIG rules, CIS benchmark recommendations, or EU GDPR articles/recitals. DBSAT also marks findings as Oracle Best Practice (OBP) if the finding is a best practice that all customers should follow no matter you are looking into CIS, STIG or GDPR compliance.

**Can I extract certain Findings, compare different reports, or create an aggregated report for multiple databases?**

DBSAT Reporter provides the report in JSON format to make further processing of Findings possible.

You can also download and leverage DBSAT utils for further processing. DBSAT utils are two sample Python programs that can extract a finding and help you compare two JSON reports. You can download DBSAT utils from My Oracle Support.

Alternatively, you may also want to consider Oracle Data Safe. Data Safe is a database security cloud service that provides a comprehensive set of security capabilities, including user and security assessments. Oracle Data Safe provides enterprise-grade assessment capabilities that allow you to run assessments on a schedule, on multiple databases, establish a security baseline, and get comparison reports highlighting the drift between the baseline and the current assessment run. Leveraging Oracle Data Safe events and OCI events and notifications, you can get alerted on a drift and integrate these alerts into other systems. To learn more about Oracle Data Safe, please visit <https://www.oracle.com/security/database-security/data-safe/>.

Audit Vault and Database Firewall (AVDF) 20.9 introduced Database Security Posture Management. Besides collecting audit records and allowing for the provisioning of audit policies, reports, and alerts, AVDF now provides enterprises with a centralized security assessment solution by integrating DBSAT for Oracle Databases. The full-featured assessment with compliance mappings and recommendations will help organizations understand their security posture for all their Oracle Databases in one central place. To learn more about Audit Vault and Database Firewall, please visit <https://www.oracle.com/security/database-security/audit-vault-database-firewall/>.

### Can I run DBSAT Collector on a multitenant pluggable database?

Yes, however, DBSAT needs to be executed for the root container and each PDB separately.

### Can I add my custom security assessment rules?

No, DBSAT was built to be a quick and easy-to-use tool that provides immediate value for our customers. DBSAT ships with Oracle Database Security best practices rules and, where applicable, highlights Oracle Database STIG Rules, CIS Benchmark recommendations, and related EU GDPR articles/recitals. We encourage you to file an Enhancement Request on My Oracle Support. We review and evaluate all enhancement requests for new rules inclusion. DBSAT does support customers creating or modifying Discovery rules/config.

## DBSAT Discoverer

### How does DBSAT Discoverer work?

DBSAT Discoverer uses a configuration file, one or more pattern files describing sensitive data types, and regular expressions to search column names and column comments. DBSAT Discoverer does not query the data, only the metadata associated with the column names and column comments.

e.g., To search for "First Name", you could use:

```
[FIRST NAME]
COL_NAME_PATTERN = (^|[_-])(FNAME|(FIRST|GIVEN).*(NAME|NM)|FORE.?(NAME|NM))($|[_-])
COL_COMMENT_PATTERN = (FIRST|GIVEN) NAME|FORENAME
SENSITIVE_CATEGORY = Identification Info - Public IDs
```

DBSAT comes with the initial configuration and pattern file, but customers can add custom sensitive types and categories/subcategories.

For a more thorough approach to identifying sensitive data, you might want to check out Oracle Data Safe Sensitive Data Discovery. In addition to analyzing column names and comments, Data Safe also validates the data itself, allowing it to identify sensitive information more accurately.

### What types of Regular expressions are used?

DBSAT Discoverer supports Extended Regular Expressions (ERE). This syntax is standardized by IEEE and is commonly used in Java.

For example, `(^JOB.*(TITLE|PROFILE|POSITION)$|^POSITION` matches a string that starts with JOB (^JOB), followed by zero or more occurrences (\*) of any character (.), and ends in (\$) TITLE or PROFILE or POSITION. Or `(|)`, it matches a string that starts (^) with POSITION.

### How accurate are the pattern-matching rules? How does one deal with false positives?

The rules provided with DBSAT were created to reduce false positives. However, as DBSAT examines only the column names and column comments, it might generate false positives. One way to reduce false positives is to edit the pattern file and tune the regular expression for your specific data model; another is to exclude schemas, tables, and columns from the search using an exclusion list file. As the CSV report includes a fully qualified name for the column (Schema.Table.Column), you easily exclude false positives by copying/pasting from the CSV report to the exclusion list file.

### Can DBSAT find sensitive data if my data model is in other languages besides English?

Along with a pattern file that searches English-based column names and comments, DBSAT also includes additional sample pattern files for Dutch, French, German, Greek, Italian, Portuguese, and Spanish that can help you quickly get started to discover

sensitive data in non-English-based data models. You can create your own pattern files from scratch or copy an existing one and adapt it to your requirements.

### How do I run the DBSAT Discoverer?

DBSAT Discoverer can run on any machine, including a laptop with Java Runtime Environment (JRE) 1.8 (jdk8-u172) or later. There is no need to run Discoverer on the same server as the database server.

```
$ dbsat discover -c <config file> <dest-file>
```

e.g.,

```
$ dbsat discover -c Discoverer/conf/dbsat.config dbdata
```

### Do I need to run the DBSAT Collector before running DBSAT Discoverer?

No. DBSAT Discoverer is a standalone component. There is no dependency on the DBSAT Collector or the Reporter. You can choose to run it or skip it.

## Security Considerations

### What privileges are required for the user account connecting to the database to collect data?

While a database user account with the Oracle-provided DBA role has the necessary privileges, you should follow the principle of least privileges. Please refer to the documentation for the minimum privileges needed to run DBSAT. In addition, the OS user executing DBSAT Collector must have permission to read the ORACLE\_HOME and TNS\_ADMIN directories and files.

### How does DBSAT protect the collected configuration data and generated reports?

By default, DBSAT output files are compressed and password-protected using installed zip/unzip. We strongly recommend that all output files always be encrypted as they have sensitive information about your database.

### What are the security risks of running DBSAT on production databases?

The risk is minimal as DBSAT only reads configuration and metadata. All database actions performed by DBSAT are read-only.

DBSAT can be run with the least privileges to collect the data it needs for analysis. Customers can run common diagnostic tools to validate what operations DBSAT executes during collector execution. You can also examine the DBSAT Collector output data (in JSON format) to see what data was collected. Access to DBSAT-generated reports should be restricted and the database user account created for DBSAT to run should be dropped or locked after use.

## Download and Installation

### Where can I download the Oracle DBSAT?

DBSAT can be downloaded from My Oracle Support under Doc ID 2138254.1.

### How do I install DBSAT?

DBSAT is provided as a zip file. Just unzip it.

```
$ unzip dbsat.zip -d <directory>
```

### Which Database versions are supported?

DBSAT supports Oracle Database 11.2.0.4 and later releases up to 23c.

### Which platforms are supported?

DBSAT runs on:

- Solaris x64 and Solaris SPARC
- Linux x86-64 and Linux 64-bit Arm
- Windows x64
- HP-UX IA (64-bit)
- IBM AIX (64-bit) and Linux on zSeries (64-bit)

DBSAT runs on most supported Oracle Database platforms. However, currently, DBSAT Collector does not collect OS data from database servers running on the Windows platforms or if executed remotely. In Unix/Linux systems, it must execute under the BASH shell. If BASH shell is unavailable, install it or execute the collector remotely from a server with it.

## Can Oracle Sales Consulting (SC), Oracle Consulting Services (OCS), Oracle Advanced Customer Services (ACS), or Oracle Customer Success Services (OCSS) download DBSAT and run it for me?

We recommend that you download and run DBSAT yourself. Depending on the scope of the assessment, Oracle Sales Consulting, Oracle Consulting Services, or Oracle Advanced Customer Services organizations can help you execute an Oracle Database Security Assessment program, analyze the data, and prioritize remediation steps considering your organization's environment. In addition, they can support you and give better insight into your database security posture through an onsite interview that complements the DBSAT reports. A proper security assessment considers a technical analysis and your organizational specifics, broader IT ecosystem, processes in place, and regulatory compliance requirements.

## Product Licensing and Support

### How is DBSAT distributed?

The tool is available at no additional cost for download by Oracle customers with a My Oracle Support (MOS) account (under an active support contract).

### How can I report bugs or request enhancements for DBSAT?

Please submit a service request (SR) for DBSAT via the MOS portal.

### Where do I go to get the bug fixes for DBSAT?

We plan to make quarterly updates to DBSAT that would include enhancements as well as bug fixes. Therefore, we strongly recommend that you always check for the latest release on My Oracle Support.

## DBSAT and Data Safe

### How does DBSAT relate to Data Safe?

Data Safe is a database security cloud service that provides a comprehensive suite of security capabilities. These capabilities include Security Assessment, User Assessment, Activity Auditing, SQL Firewall, Sensitive Data Discovery, and Data Masking and work for databases running in-cloud or on-premises.

DBSAT is excellent for assessing the current security state of a few databases. Data Safe addresses enterprise-level requirements. With Data Safe, you'll be able to:

- Execute periodic scheduled assessments
- Set a database security baseline
- See a comparison report with the drift against the baseline
- Get alerts
- See the history of all assessment runs
- Get insight into user risks via the User Assessment feature
- Address your company or regulatory requirements that require anonymizing data in non-production environments, monitor database activity, assess your database security posture, and discover sensitive data in a single unified console

To learn more about Oracle Data Safe, please visit <https://www.oracle.com/security/database-security/data-safe/>.

## DBSAT and Audit Vault and Database Firewall

Oracle Audit Vault and Database Firewall (AVDF) is a software appliance you can deploy on-premises or Oracle Cloud Infrastructure using a marketplace image. AVDF 20.9 introduced Database Security Posture Management, and it now provides a centralized security assessment solution for enterprises by integrating the popular Database Security Assessment Tool for Oracle Databases. The full-featured assessment with compliance mappings and recommendations will help organizations understand their security posture for all their Oracle Databases in one central place. With Audit Vault and Database Firewall, you'll be able to:

- Set a database security baseline
- See a comparison report with the drift against the baseline
- Get insight into user entitlements
- Address your company or regulatory requirements requiring database activity monitoring, assessing your database security posture, and preventing SQLInjection attacks.

To learn more about Oracle Audit Vault and Database Firewall, please visit <https://www.oracle.com/security/database-security/audit-vault-database-firewall/>.

## More Information

### **Where can I find more information on DBSAT?**

Go to the DBSAT [oracle.com](https://www.oracle.com) page.

### **Where do I go for more details on the Oracle Database Security Assessment program?**

Multiple Oracle teams across the globe have created their Oracle Database Security Assessment programs. Please talk to your Oracle Account Manager for assistance.

## Connect with us

Call **+1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at: **oracle.com/contact**.

 [blogs.oracle.com](https://blogs.oracle.com)

 [facebook.com/oracle](https://facebook.com/oracle)

 [twitter.com/oracle](https://twitter.com/oracle)

Copyright © 2023, Oracle and/or its affiliates. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.