ORACLE

Oracle Database Security Assessment Tool

Learn how secure your databases are with DBSAT

Nov 2026, Version 1.0.1
Copyright © 2026, Oracle and/or its affiliates
Public

With constant data breaches and changing privacy rules, organizations must ensure their databases are secure. However, it can be difficult to know if databases are configured correctly, who has access, and where sensitive data is stored. As part of Oracle's defense-in-depth capabilities, the Oracle Database Security Assessment Tool (DBSAT) helps identify areas where your database configuration, operation, or implementation introduces risks. DBSAT recommends targeted changes and controls to reduce those risks.

Evolving regulatory compliance

Security configuration scanning is now required by regulations such as the EU General Data Protection Regulation (EU GDPR), the Payment Card Industry Data Security Standard (PCI-DSS), state and local laws, and industry standards. Additionally, various organizations, such as the Center for Internet Security (CIS) and the U.S. Department of Defense, offer recommendations for security configuration best practices. Security controls matter more than ever. New and changing regulations all aim to protect organizations' most valuable asset: data.

Cryptographic controls are central to protecting data at rest and in transit, and they are increasingly important to security and compliance reviews. As algorithms and recommended configurations evolve, outdated or weak settings can expose sensitive data, including through *harvest now, decrypt later* attacks, in which encrypted traffic or backups collected today may be targeted for decryption in the future.

Before implementing new controls, organizations face a major challenge: understanding their database security posture. They must quickly determine how securely their databases are configured, where sensitive data resides, how much sensitive data they hold, who has access, which security controls are in place, and which cryptographic algorithms are used to protect data.

Whether your database runs on premises or in the cloud, the Oracle Database Security Assessment Tool (DBSAT) identifies potentially sensitive data and areas where your database configuration, operation, or implementation introduces risk. DBSAT collects and analyzes metadata and configurations to spot security risks. DBSAT also recommends target-specific changes and controls to mitigate those risks.

Think like a hacker

Attackers often spend significant time preparing and conducting reconnaissance before launching an attack. They use tools that automate the discovery of databases, identify unpatched vulnerabilities, automate application and SQL injection attacks, and execute brute-force password attacks. After probing, they assess the weakest links and plan their next moves. Attackers evaluate your security posture to find ways to access sensitive data. Some common questions attackers try to answer while probing your databases include:

- What version of the database is running? – Identifying outdated versions with known vulnerabilities.
- Are default or weak credentials in use? – Exploiting accounts with weak or unchanged passwords.
- Which privileged users exist? – Escalating access by compromising high-privilege accounts.
- Is auditing enabled? – Determining whether actions will be logged and monitored.
- Is the data encrypted? – Assessing if they can steal raw data from storage or backups.
- Could encrypted network traffic or database backups copied today be decrypted later? - The **harvest now, decrypt later** threat puts long-lived sensitive data at risk as quantum capabilities advance.
- Is there a copy of this database that is less likely to be audited? – Finding the least risky approach to data theft.

Hackers use the answers to these questions to plan their attacks and steal your data. As data custodians, you must think like hackers to harden your database's security posture.

Even when organizations know what's needed to evaluate their security posture, many struggle to assess database security due to limited expertise, time constraints, poor prioritization, or misunderstanding of the risks. Security knowledge is often split between database administrators (DBAs) and IT security teams, who typically focus on protecting networks and endpoints.

Copyright © 2026, Oracle and/or its affiliates / Public

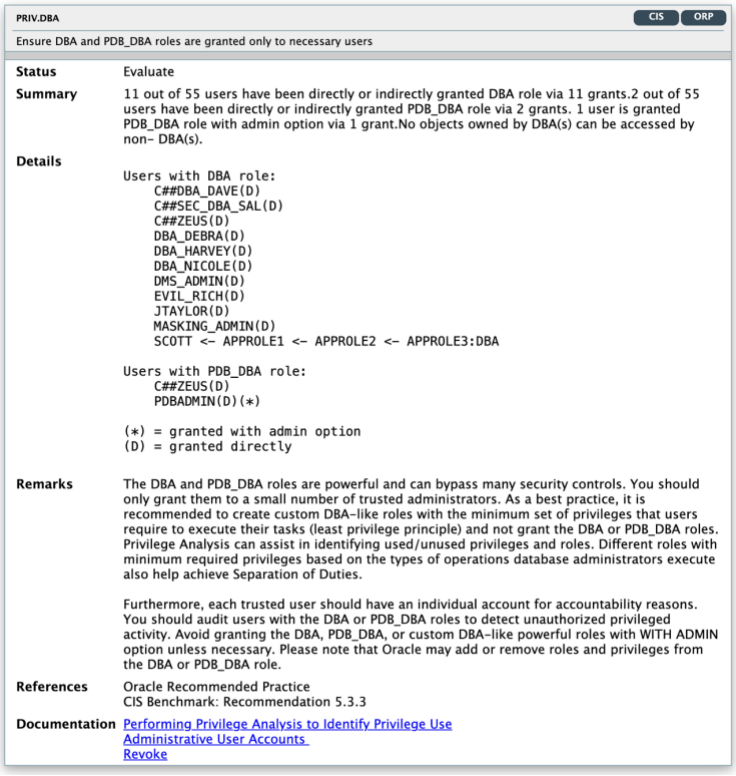
Oracle DBSAT accelerates the assessment process by collecting relevant configuration information from the database and evaluating the current security state to provide recommendations on mitigating the identified risks. DBSAT quickly provides insight into how securely the database is configured, who the users are and their entitlements, what security policies are in place, what security controls are implemented, and where sensitive data resides. The figure below summarizes the security status of a sample database and categorizes its findings by risk levels.

Figure 1. Current Security State Summary of an Oracle Database.

Section	High Risk	Medium Risk	Low Risk	Advisory	Evaluate	Pass	Total Findings
Database Security Basics	1	0	0	0	0	0	1
User Accounts	0	1	5	1	13	5	25
Privileges and Roles	0	0	0	1	25	5	31
Auditing	0	0	0	6	10	4	20
Encryption	0	0	0	0	3	0	3
Authorization Control	0	0	0	1	4	0	5
Fine-Grained Access Control	0	0	0	5	0	0	5
Database Configuration	1	0	0	1	14	11	27
Network Configuration	1	0	0	0	1	0	2
Operating System	0	1	1	0	4	3	9
Total	**3**	**2**	**6**	**15**	**74**	**28**	**128**

DBSAT reports its analysis results as a series of findings. Each finding provides a high-level status, risk level, summary, details, and references, whether it relates to an Oracle Recommended Practice, Oracle Database STIG Rule, CIS benchmark recommendation, GDPR article or recital, and documentation links for Oracle Database 19c and 26ai. The two findings below show which users have the powerful DBA role and how they obtained it (directly or through another role) and which users have default passwords. Checks and recommendations are specific to the database target and its deployment—on premises or in the cloud (Autonomous AI Database Serverless and Dedicated, or Base Database).

Figure 2. Users granted the DBA role and its grant path.



PRIV.DBA — CIS ORP

Ensure DBA and PDB_DBA roles are granted only to necessary users

Status Evaluate

Summary 11 out of 55 users have been directly or indirectly granted DBA role via 11 grants.2 out of 55 users have been directly or indirectly granted PDB_DBA role via 2 grants. 1 user is granted PDB_DBA role with admin option via 1 grant.No objects owned by DBA(s) can be accessed by non- DBA(s).

Details

```
Users with DBA role:
    C##DBA_DAVE(D)
    C##SEC_DBA_SAL(D)
    C##ZEUS(D)
    DBA_DEBRA(D)
    DBA_HARVEY(D)
    DBA_NICOLE(D)
    DMS_ADMIN(D)
    EVIL_RICH(D)
    JTAYLOR(D)
    MASKING_ADMIN(D)
    SCOTT <- APPROLE1 <- APPROLE2 <- APPROLE3:DBA

Users with PDB_DBA role:
    C##ZEUS(D)
    PDBADMIN(D)(*)

(*) = granted with admin option
(D) = granted directly
```

Remarks The DBA and PDB_DBA roles are powerful and can bypass many security controls. You should only grant them to a small number of trusted administrators. As a best practice, it is recommended to create custom DBA-like roles with the minimum set of privileges that users require to execute their tasks (least privilege principle) and not grant the DBA or PDB_DBA roles. Privilege Analysis can assist in identifying used/unused privileges and roles. Different roles with minimum required privileges based on the types of operations database administrators execute also help achieve Separation of Duties.

Furthermore, each trusted user should have an individual account for accountability reasons. You should audit users with the DBA or PDB_DBA roles to detect unauthorized privileged activity. Avoid granting the DBA, PDB_DBA, or custom DBA-like powerful roles with WITH ADMIN option unless necessary. Please note that Oracle may add or remove roles and privileges from the DBA or PDB_DBA role.

References Oracle Recommended Practice
CIS Benchmark: Recommendation 5.3.3

Documentation Performing Privilege Analysis to Identify Privilege Use
Administrative User Accounts
Revoke

Copyright © 2026, Oracle and/or its affiliates / Public

In an Oracle Database, the DBA role grants significant privileges that can override numerous security controls. As highlighted in the example, the DBSAT report indicates that the user SCOTT was granted the DBA role indirectly via a series of role grants (APPROLE3 to APPROLE2 to APPROLE1). In contrast, other users were assigned the DBA role directly.

Figure 3. Users with default passwords.

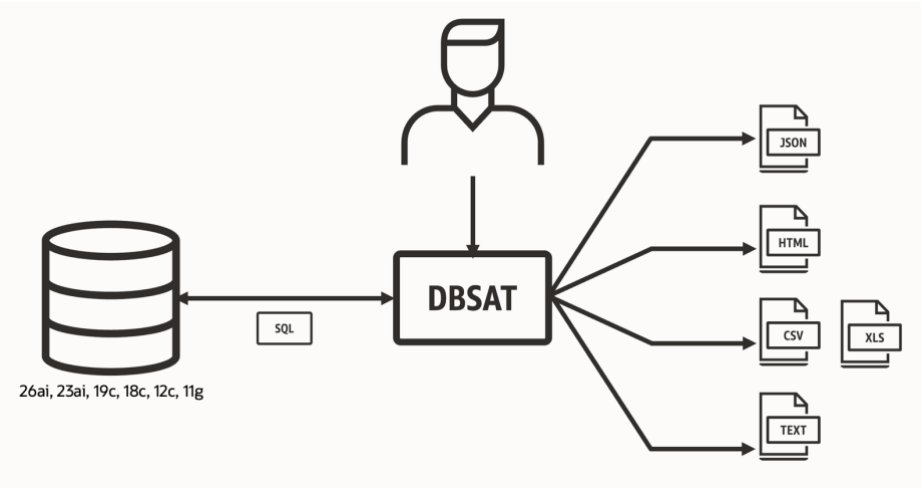
USER.DEFPASSWORD — CIS ORP STIG

User accounts should not have default passwords

Status	High Risk
Summary	Found 1 unlocked user account with default password.
Details	Users with default password: SCOTT
Remarks	Default passwords for predefined Oracle accounts are well known and provide a trivial means of entry for attackers. Database or account administrators should also change well-known passwords for locked accounts. Having default passwords can lead to unauthorized data manipulation and theft of confidential information. Note that if a script creates the database and the SYS and SYSTEM user passwords remain unchanged, these users are considered to possess default passwords. Your database may be at risk due to the password presence within the script. Change the password to improve security.
References	Oracle Recommended Practice CIS Benchmark: Recommendation 4.1 DISA STIG: V-270545
Documentation	Guidelines for Securing Passwords Finding User Accounts That Have Default Passwords DBA_USERS_WITH_DEFPWD

DBSAT findings are provided in multiple formats, including HTML, Microsoft Excel, JSON, and text files, allowing organizations to integrate this data into their configuration and risk management tools.

Figure 4. DBSAT supported target versions and report output formats.



Cryptographic posture assessment

Starting with 26.1, DBSAT provides a cryptographic posture assessment that evaluates an Oracle Database's cryptographic configuration against recommended security baselines involving:

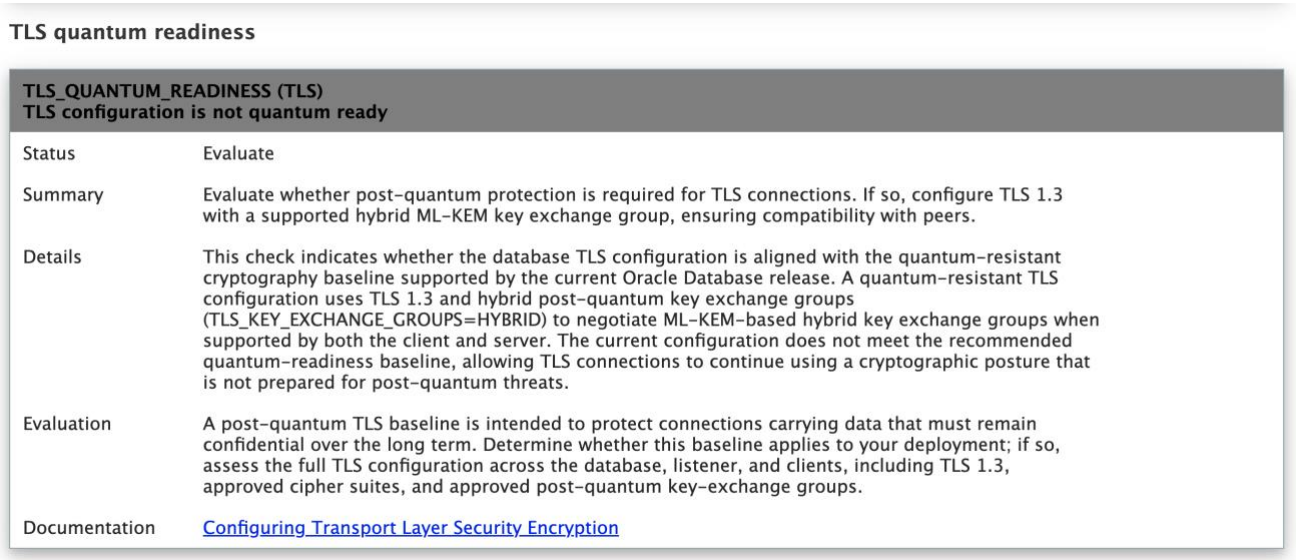
- Encryption at rest and in transit: Covers encryption settings, TLS versions, key exchange settings, and network encryption.
- Certificates and key management: Reviews certificate validity and related configuration, wallets, and key-management settings.
- Backup encryption: Reviews the configuration for encryption of database backups.
- Quantum-readiness indicators: Checks help teams understand cryptographic posture in the context of quantum-era risks.

Each finding describes the current configuration, whether it meets the expected baseline, whether a stronger configuration is recommended, and guidance with Oracle documentation references.

Copyright © 2026, Oracle and/or its affiliates / Public

Example cryptographic posture finding and guidance is shown in Figure5. DBSAT indicates that TLS configuration is not quantum ready and provides guidance on reviewing the TLS version and Key Exchange groups configured in the system.

Figure 5. TLS Quantum readiness posture finding.



TLS quantum readiness

TLS_QUANTUM_READINESS (TLS) TLS configuration is not quantum ready	
Status	Evaluate
Summary	Evaluate whether post-quantum protection is required for TLS connections. If so, configure TLS 1.3 with a supported hybrid ML-KEM key exchange group, ensuring compatibility with peers.
Details	This check indicates whether the database TLS configuration is aligned with the quantum-resistant cryptography baseline supported by the current Oracle Database release. A quantum-resistant TLS configuration uses TLS 1.3 and hybrid post-quantum key exchange groups (TLS_KEY_EXCHANGE_GROUPS=HYBRID) to negotiate ML-KEM-based hybrid key exchange groups when supported by both the client and server. The current configuration does not meet the recommended quantum-readiness baseline, allowing TLS connections to continue using a cryptographic posture that is not prepared for post-quantum threats.
Evaluation	A post-quantum TLS baseline is intended to protect connections carrying data that must remain confidential over the long term. Determine whether this baseline applies to your deployment; if so, assess the full TLS configuration across the database, listener, and clients, including TLS 1.3, approved cipher suites, and approved post-quantum key-exchange groups.
Documentation	Configuring Transport Layer Security Encryption

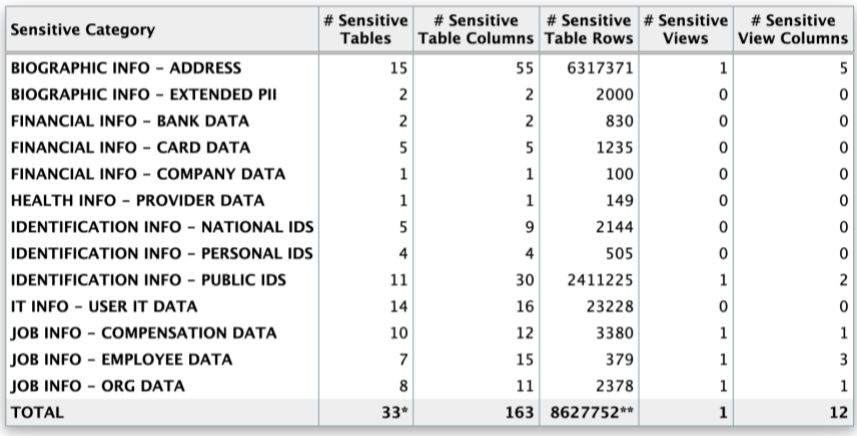
A cryptographic posture assessment helps reveal hidden vulnerabilities in an organization's encryption defenses, so teams can identify gaps and prioritize changes before future decryption capabilities emerge.

Discover sensitive data

Regulations like the EU GDPR, U.S. California CCPA, Brazil's LGPD, and India's DPDPA mandate that organizations safeguard personally identifiable information (PII). A critical first step in compliance is identifying the personal data they hold and its location.

DBSAT facilitates this by scanning database metadata for sensitive data using customizable regular expression patterns. It provides detailed reports on the volume and type of sensitive data discovered. Beyond supporting English-based data dictionaries (e.g., column names and comments), DBSAT also accommodates major European languages, including Dutch, French, Italian, German, Greek, Portuguese, and Spanish. This multilingual capability offers organizations greater visibility into the extent and location of sensitive data, empowering them to implement robust security measures such as access controls, auditing, data masking, and encryption. The figure below illustrates a summary report generated from a database metadata scan.

Figure 6. Sensitive Data Landscape 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

DBSAT provides an assessment of an Oracle Database. For fleet-wide visibility, automated assessments, configuration-drift detection, and centralized security insights, use Oracle Data Safe or Oracle Database Security Central.

Copyright © 2026, Oracle and/or its affiliates / Public

Assessment using Oracle Data Safe

Oracle Data Safe is a cloud service that lets you assess the security of databases both in the cloud and on-premises. It offers a comprehensive suite of security capabilities, including user, security and cryptographic posture assessments. With Oracle Data Safe's, you can assess multiple databases at once, set a security baseline, and generate a comparison report that show changes from the baseline. Oracle Data Safe includes APIs for automating and integrating database security assessments into CI/CD pipelines.

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

Assessment using Oracle Database Security Central

Oracle Database Security Central provides a centralized security assessment solution for enterprises by integrating the Database Security Assessment Tool for Oracle Databases. The full-featured assessment with compliance mappings and recommendations helps organizations understand the security posture of all their Oracle databases in one place.

To learn more about Oracle Database Security Central, please visit https://www.oracle.com/security/database-security/database-security-central/.

Summary

Knowing where sensitive data is and how the database is configured is the foundation for a strong defense. No system is completely secure, but skipping the basics makes it much easier for attackers.

Oracle Database Security Assessment Tool (DBSAT) quickly identifies sensitive data and areas where your database configuration, operation, or implementation introduce risk.

DBSAT is free for customers with an active Oracle support contract. For more information or to download DBSAT, visit https://www.oracle.com/security/database-security/assessment-tool/.

Copyright © 2026, Oracle and/or its affiliates / Public

Key features

- Identifies configuration settings that may increase your risk exposure.
- Identifies sensitive user accounts, their entitlements, and security policies.
- Discovers sensitive data in English-based data dictionaries and major European languages.
- Recommends and prioritizes relevant security controls and findings.
- Assesses cryptographic configuration against recommended baselines, including encryption, TLS, certificates, key management, backups, and quantum-readiness indicators.

Related products

- Oracle Data Safe
- Oracle Database Security Central
- Oracle Advanced Security
- Oracle Key Vault
- Oracle Database Vault
- Oracle Data Masking and Subsetting pack
- Oracle Label Security

Copyright © 2026, Oracle and/or its affiliates / Public

ORACLE

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 facebook.com/oracle twitter.com/oracle

Copyright © 2026, 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.