# Oracle® Database

## Security Guide

23ai
F46690-21
April 2025

Oracle Database Security Guide, 23ai

F46690-21



Primary Author: Patricia Huey

Contributors: Suraj Adhikari, Tammy Bednar, Ji-Won Byun, Yuechen Chen, Nishant Chaudhary, Rajnish Chitkara, Chi Ching Chui, Angeline Dhanarani, Naveen Gopal, Rishabh Gupta, Yong Hu, Dana Joly, Srinidhi Kayoor, Peter Knaggs, Imran M. Khan, Sanjay Kulhari, Anup A. Kumar, Scott McKinley, Misaki Miyashita, Hari Mohankumar, Gopal Mulagund, Abhishek Munnolimath, Marudha Sudharshan R, Kumar Rajamani, Vipin Samar, Saravana Soundararajan, Ankit Srivastava, Siu Tam, Luna Tan, Ruchi Tayal, Kamal Tbeileh, Rohit Thatte, Can Tuzla, Anand Verma, Alan Williams, Peter Wahl, Jinglei Xie, Deepak Yadav, Quan Yang

# Contents

## 3 Configuring Authentication

## 4 Configuring Privilege and Role Authorization

## 5 Performing Privilege Analysis to Identify Privilege Use

## 6 Configuring Centrally Managed Users with Microsoft Active Directory

## 8 Authenticating and Authorizing Microsoft Azure Users for Oracle Databases

## 9 Managing Security for Definer's Rights and Invoker's Rights

## 10 Managing Fine-Grained Access in PL/SQL Packages and Types

## 11 Managing Security for a Multitenant Environment in Enterprise Manager

## 14 Using Oracle Virtual Private Database to Control Data Access

## 15 Using Transparent Sensitive Data Protection

## 16 Encryption of Sensitive Credential Data in the Data Dictionary



## 17 Securing and Isolating Resources Using DbNest

## 18 On-Demand Encryption of Data



# Part IV Securing Data on the Network

## 19 Securing Data for Oracle Database Connections

## 20 Configuring Oracle Database Native Network Encryption and Data Integrity



## 21 Configuring Transport Layer Security Encryption

## 25 Configuring PKI Certificate Authentication



## 26 Configuring RADIUS Authentication

## 32 Administering the Audit Trail

## B Managing Oracle Database Wallets and Certificates

## C Oracle Database FIPS 140-2 Settings

# Preface

Welcome to *Oracle Database Security Guide*. This guide describes how you can configure security for Oracle Database by using the default database features.



## Audience

*Oracle Database Security Guide* is intended for database administrators (DBAs), security administrators, application developers, and others tasked with performing the following operations securely and efficiently.

It covers these areas:

- Designing and implementing security policies to protect the data of an organization, users, and applications from accidental, inappropriate, or unauthorized actions
- Creating and enforcing policies and practices of auditing and accountability for inappropriate or unauthorized actions
- Creating, maintaining, and terminating user accounts, passwords, roles, and privileges
- Developing applications that provide desired services securely in a variety of computational models, leveraging database and directory services to maximize both efficiency and ease of use

To use this document, you need a basic understanding of how and why a database is used, and basic familiarity with SQL.

## 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 customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.

# Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

# Related Documents

For more security-related information, see these Oracle resources:

- *Oracle Database Data Redaction Guide*
- *Oracle Database Transparent Data Encryption Guide*
- *Oracle Database Vault Administrator's Guide*
- *Oracle Label Security Administrator's Guide*
- Oracle Key Vault documentation library
- Audit Vault and Database Firewall documentation library
- Oracle Data Masking and Subsetting documentation library
- Oracle Data Safe documentation library
- Oracle Database Security Assessment Tool
- *Oracle Database PL/SQL Packages and Types Reference*
- *Oracle Database Reference*
- *Oracle Database SQL Language Reference*
- *Oracle Database Net Services Reference*
- *Oracle Database Administrator's Guide*
- *Oracle Database Concepts*
- *Oracle Multitenant Administrator's Guide*

Many of the examples in this guide use the sample schemas of the seed PDB, which you can create when you install Oracle Database. See *Oracle Database Sample Schemas* for information about how these schemas were created and how you can use them yourself.

**Oracle Technical Services**

To download the product data sheet, frequently asked questions, links to the latest product documentation, product download, and other collateral, visit Oracle Technical Resources (formerly Oracle Technology Network). You must register online before using Oracle Technical Services. Registration is free and can be done at

`https://www.oracle.com/technical-resources/`

### My Oracle Support

You can find information about security patches, certifications, and the support knowledge base by visiting My Oracle Support (formerly Oracle*MetaLink*) at

https://support.oracle.com

# Conventions

The following text conventions are used in this document:

| Convention | Meaning |
|---|---|
| **boldface** | Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary. |
| *italic* | Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values. |
| `monospace` | Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter. |