Release Notes

Release Notes contain important information about Oracle Database Security Central.

New Features In Oracle Database Security Central

Learn about new features and enhancements in Oracle DBSecCentral.

What's New in Oracle Database Security Central

Oracle Database Security Central (DBSecCentral) is the initial release of a customer-managed platform for securing databases across an enterprise fleet. It brings together privileged-user risk analysis, sensitive-data discovery, configuration assessment, activity monitoring, policy management, SQL threat protection, reporting, and AI-assisted operations in a single console.

Security Control Center

- Provides a unified view of database security risk across users, sensitive data, configuration posture, and activity.
- Correlates related signals to identify compound exposures that may not be apparent when findings are reviewed separately.
- Helps security teams prioritize investigation and remediation based on combined risk and business impact.

User 360

- Identifies privileged, high-risk, stale, and dormant database users across the fleet.
- Maps direct and indirect access paths, including privileges inherited through roles.
- Tracks entitlement drift to support least-privilege enforcement and periodic access reviews.

Data 360

- Discovers and classifies sensitive data across production, development, test, and analytics environments.
- Includes more than 181 predefined sensitive-data types across 20 categories and supports custom classifications.

- Combines metadata analysis with row-level validation to improve classification accuracy and consistency.

Configuration 360

- Defines approved security baselines and continuously assesses databases for configuration drift.
- Prioritizes findings based on severity and exposure to help teams focus remediation efforts.
- Maps assessment findings to recognized security and compliance frameworks, including CIS, DISA STIG, and GDPR.

Audit 360

- Centralizes audit collection and activity monitoring for supported Oracle and non-Oracle databases, operating systems, directories, and custom sources.
- Captures security-relevant events such as logons, privilege use, schema changes, configuration changes, administrative activity, and access to sensitive data.
- Provides prebuilt and interactive reports, policy-based alerts, scheduled distribution, and integration with SIEM and business-intelligence platforms.

Unified Policy Management

- Creates and manages audit, alert, Database Vault, Database Firewall, and SQL Firewall policies from one console.
- Deploys policies consistently across databases and target groups to reduce policy drift and manual per-database administration.
- Supports a governed policy lifecycle with centralized definition, deployment, monitoring, refinement, and deployment visibility.

SQL Threat Protection

- Uses Database Firewall to inspect SQL traffic before execution with grammar-based analysis of SQL structure and intent.
- Supports monitoring, alerting, and blocking based on SQL behavior, database user, application, source IP address, and network context.
- Centrally manages SQL Firewall for supported Oracle AI Database 26ai environments to enforce approved SQL and connection paths inside the database kernel.

AI Advisor and Assistant

- Allows users to ask natural-language questions about database activity, user risk, security posture, and compliance data.
- Provides step-by-step guidance for security configuration, investigation, and administrative tasks.
- Translates natural-language alert requirements into structured policy logic for review and deployment.

Deployment and Operations

- Supports customer-managed deployment on premises and in Oracle Cloud Infrastructure, Amazon Web Services, and Microsoft Azure environments.

- Supports single-node, primary-and-standby, and active-active deployment configurations with Oracle Real Application Clusters.
- Supports agent-based and agentless audit collection, centralized data-retention policies, secure archival, enterprise identity integration, and command-line automation.
- Protects the platform with a hardened operating system, encryption at rest and in transit, repository access controls, and separation of administrative and audit duties.

Bug fixes, platform updates, and security improvements:

- Security and stability fixes from Oracle AI Database 26ai (version 23.26.3) for the underlying DBSecCentral repository.
- Security and stability fixes for the underlying components, Oracle APEX, Oracle Rest Data Services (ORDS), Oracle Java SE, Oracle Autonomous Health Framework (AHF), and Oracle GoldenGate.
- Security and stability fixes for the embedded Oracle Linux 8.10 operating system.
- Fixes for several customer-reported and internally discovered issues.

About Oracle DBSecCentral Installable Files

Oracle DBSecCentral software is installed using the `.iso` files.

Oracle DBSecCentral software contains the following installation files:

- Database Firewall utility:

  `Vpart_number.zip` Oracle Database Security Central 26.0.0.0.0 - Utilities. This bundle contains the following files:

  - Npcap installer required for Host Monitoring on Windows: `npcap-utility.zip`
  - Database Firewall utilities to examine Native Network Encryption traffic for Oracle Database and to gather session information from other database types: `dbfw-utility.zip`
  - `Utilities_README`: Instructions for deploying Npcap and Database Firewall utilities patch.
- Audit Vault Server install:

  `Vpart_number.iso` Oracle Database Security Central 26.0.0.0.0 - Audit Vault Server
- Audit Vault Server Azure install:

  `Vpart_number.iso` Oracle Database Security Central 26.0.0.0.0 - Audit Vault Server on Azure
- Audit Vault Server AWS install:

  `Vpart_number.iso` Oracle Database Security Central 26.0.0.0.0 - Audit Vault Server on AWS
- Database Firewall install:

`Vpart_number.iso` Oracle Database Security Central 26.0.0.0.0 - Database Firewall

- Database Firewall Azure install:

  `Vpart_number.iso` Oracle Database Security Central 26.0.0.0.0 - Database Firewall on Azure

- Database Firewall AWS install:

  `Vpart_number.iso` Oracle Database Security Central 26.0.0.0.0 - Database Firewall on AWS

- `Vpart_number.pdf` Oracle Database Security Central 26.0.0.0.0 - Release Notes

> **Tip**
>
> Verify the checksum value for both (the Audit Vault Server ISO file and the Database Firewall ISO file). In case of any error or mismatch in the checksum values, download the ISO files and validate the checksum values again.

> **⚠ Caution**
>
> The installation process wipes out existing operating system on the machine on which you install the Audit Vault Server or Database Firewall, and automatically installs the new operating system that comes along.

Product Compatibility Matrix

Types of targets (databases and operating systems) supported by Oracle DBSecCentral.

See section Product Compatibility Matrix in the *Oracle Database Security Central Installation Guide* for information on supported targets and deployment options for Audit Vault Server.

Downloading Oracle DBSecCentral Documentation

Learn how to access documentation for Oracle DBSecCentral.

- Oracle Database Security Central to download the most current version of this document, and the complete set of Oracle Database Security Central documentation.
- Documentation for other Oracle products

Oracle Database Security Central Release Notes
G59100-01

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.