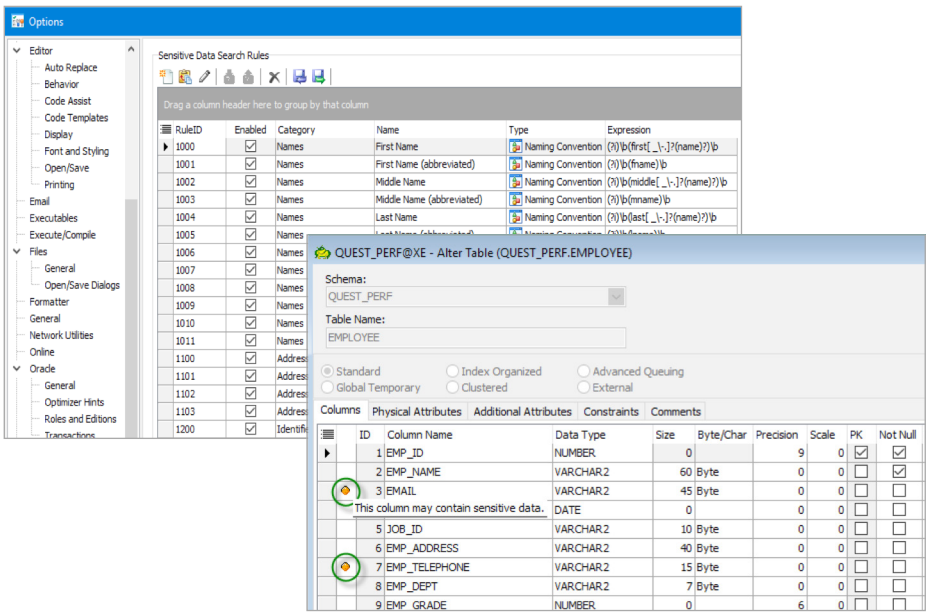
Toad® for Oracle - Sensitive Data Protection

Find and control sensitive data across all your Oracle databases quickly and easily.

Data breaches are more prevalent than ever and involve companies across the revenue spectrum, raising concerns in many organizations about what a data breach means in terms of financial impact, reputational damage and potential loss of business. As an Oracle DBA, you're tasked with ensuring the data within your databases is protected, which is daunting work, as you contend with a multitude of business applications and databases strewn throughout your organization and in the cloud. Are you tired of manually trawling through thousands of tables in multiple databases using column names to locate sensitive data?

When you rely on vendor provided tools that use metadata to locate potentially sensitive data, it can take a long time to locate sensitive data across all your databases. Because these tools assume your database tables and columns follow strict naming conventions, they can be ineffective and risk that sensitive data exists in places you don't know about. What if you could use sophisticated search technology and automation to streamline this process? This would mean you'd save time and reduce risk.

With Toad® for Oracle - Sensitive Data Protection, you can search with a tool that performs data sampling across all your tables using a range of regular expressions in a set of predefined rules to judge what is sensitive data. This solution allows you to customize and create your own rules and refine your search parameters across your Oracle databases. Then, when you locate sensitive data in a table, you can apply Oracle's native redaction, encryption and audit techniques.



Apply your sensitive data search rules to find sensitive data across all your Oracle databases.

Simplify and automate the identification and reporting of sensitive data. Then, quickly apply the necessary data protection measures.

BENEFITS:

- Discover sensitive data across all your Oracle databases faster
- Notify developers automatically when sensitive data fields are referenced during coding
- Automate the discovery process and simplify reporting
- Integrates into many Toad features such as Editor, VOEs and DB Health Check

SYSTEM REQUIREMENTS

Same as Toad for Oracle Professional Edition or higher, but requires internet access to activate the license for Sensitive Data Protection.

The consequences of noncompliance with data privacy regulations, such as GDPR and California's Data Privacy Act, can be significant and include hefty fines and potential damage to brand reputation. Be ready. Reduce your risk exposure and achieve compliance by identifying where sensitive data is in your Oracle databases and applying the appropriate protection quickly and easily.

FEATURES

Sensitive Data Awareness

Available in Toad for Oracle Professional Edition (or higher) 13.1.

- **Customizable rules —** Provides configurable rules to define what sensitive data means to you.
- **Sensitive Data Awareness —** Flags sensitive data usage in object and code editors automatically.

Sensitive Data Search

Available only in the Sensitive Data Protection module, which is part of Toad for Oracle Professional Edition (or higher) 13.2. Note that a separate license key is required to activate Sensitive Data Protection.

- **Customizable rules —** Provides configurable rules to define what sensitive data means to you for column and data patterns.
- **Sensitive Data Search —** Searches across Oracle database schemas based on metadata and data polling.
- **Sensitive Data Protection —** Enables you to apply appropriate protection measures using Oracle features for data encryption, redaction and audit.
- **Streamlined workflow —** Allows DBAs and data protection officers to apply protective measures in-situ.
- **Reporting —** Runs reports across one or multiple databases. Exports results as part of data privacy compliance for sensitive data.
- **Automation —** Automates search and reporting functions to identify and locate data on which no policy has yet been applied.
- **Database Health Check —** Enables you to include and automate Sensitive Data Protection with other routine DBA tasks.

ABOUT QUEST

Quest provides software solutions for the rapidly-changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid datacenters, security threats and regulatory requirements. Our portfolio includes solutions for database management, data protection, unified endpoint management, identity and access management and Microsoft platform management.

Quest
4 Polaris Way, Aliso Viejo, CA 92656 | www.quest.com
If you are located outside North America, you can find local office information on our Web site.

DataSheet-Toad4Oracle-SensitiveDataProtection-US-KS-38644