ORACLE

ORACLE Database 23ai

Oracle Label Security

Oracle Label Security enables companies and government organizations to consolidate data with similar sets of sensitive data – but with different access requirements (including government classified data) – into the same database. Label Security implements multi-level access controls based on the classification of the data and the access label (security clearance) of the application user. This powerful capability enables enforcement for sensitive R&D projects, non-public financial information, and multi-level security requirements inside the Oracle Database Enterprise Edition, which is included as part of the Autonomous Database, Exadata cloud service and the High Performance and Extreme Performance editions of the Oracle Base Database Service.

Key Business Benefits

- Reduce operational and storage costs by enabling different sets of data, with varying sensitivity levels, to co-mingle in the same system environment.
- Reduce development costs to meet row-level access control requirements based on clearance levels.
- Provides an easy, cost-efficient route for compliance requirements for multi-level security, mandatory access control, and managing access to data on a "need to know" basis.
- Comply with government and commercial requirements for highly secure products, including Common Criteria certification.
- Optimized to support environments with mandatory access control/ compartmentalization requirements with multiple data and user classification labels.
- Leverage existing Oracle Enterprise Manager skills to build policies and manage labels.

Data classification

Label Security assigns a data label or classification to application data, enabling sensitive data to reside in the same table with less sensitive data. Label Security enforces control by comparing the data label with the label or security clearance of the user requesting access. Data Labels can be attached as hidden columns to tables, providing transparency to existing applications by mediating access based on the data label but not returning the actual data label in the SQL statement. Alternatively, the data label can be explicitly queried, but only if the user has the label authorization for the queried rows.

Figure 1. Label Security data labels

Event	Location	Label
Press Release	USA	PUBLIC
Budget Review	Hong Kong	HIGHLY_SENSITIVE:FINANCE:ASIA
Conference	Spain	PUBLIC
Advertising Plan	South Africa	SENSITIVE::AFRICA
Merger Discussions	USA	HIGHLY_SENSITIVE:MA:USA
Employee Announcement	Global	SENSITIVE
Alpha Project Review	Brazil	HIGHLY_SENSITIVE:ALPHA

Data labels can be comprised of three components. The first component is a mandatory level. Examples of levels include public, confidential, and sensitive. The second component is optional and is known as a compartment. Multiple compartments can be assigned to a data label and are used to enforce additional special access requirements. For example, a data label protecting special customer accounts might contain the compartment VIP. A label's third and final component is optional and known as a group. Examples of groups include organizations or territories such as the Office of the CEO, AMERICAS, and Europe. Labels always include a level and may contain zero or more groups and compartments.

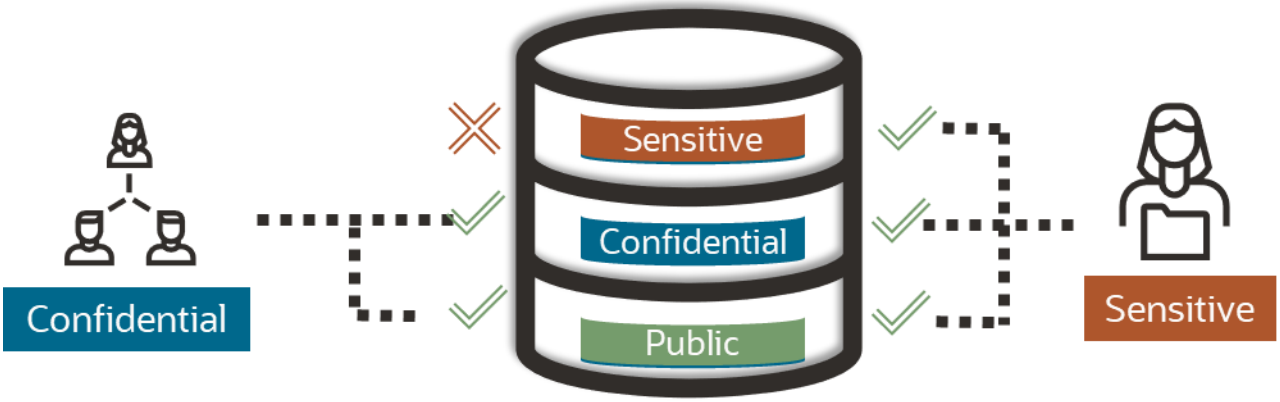
Key features of Oracle Label Security

- Data access enforcement is implemented in the database to enforce access control policies regardless of how and where data is accessed.
- Proxy authorization and built-in access control logic eliminate the requirement to code complex rules into applications.
- Dozens of out-of-the-box label functions, including the least upper bound (LUB) and merge label functions
- Hidden column for data labels
- Flexible and granular enforcement controls, enabling enforcement on READ, UPDATE, INSERT and DELETE operations.
- Enable Trusted Stored Procedures by assigning privileges such as FULL or READ.
- Supports assignment of label authorizations to non-database users such as application users, IP addresses, and other factors
- Integrated with Oracle Database Vault to use security labels as factors for trusted paths.
- Integrated with Real Application Security to allow labels to be assigned to Real Application Security users.

User labels and access mediation

A user label consists of a maximum and minimum level, compartments, and groups. When a user authenticates to the Oracle Database, Label Security initializes the user label. For applications that do not use physical database users, Label Security provides a built-in proxy capability that can be used by the application to enable data access enforcement based on the application user's identity. Label Security provides flexible enforcement controls, enforcing access control on read operations, write operations, or both. When mediating access, Label Security first compares the user level with the level assigned to the data label. Second, it checks that the user has at least one of the groups assigned to the data label. Third, it checks that the user has all the compartments assigned to the data label. For example, a data label of Sensitive:VIP:Executive,CEO would require a user to have access to Sensitive data, the VIP compartment, and either the Executive or CEO groups.

Figure 2. User labels and access mediation



Assigning data labels

Data labels are comprised of a sensitivity level, zero or more compartments, and zero or more groups. Before creating a data label, the valid label components are defined and stored inside the Oracle Database data dictionary. Data labels can be automatically assigned to table rows using a labeling function or the user's current session label. Labeling functions enable the data labels to be computed based on different application attributes. Labels can also be assigned by specifying the actual label in the insert statement using either the numeric label tag or the char_to_label function. For low storage overhead, Label Security uses a numeric tag to represent the data label on each row. The function label_to_char converts a numeric label tag to its external or text version.

Label security and Data Privacy Regulations

Under many privacy regulations including the European Union Data Protection Regulation (EU GDPR), data subjects have the right to request an organization to stop processing their data – Restriction of Processing. In such cases, the organization needs to implement a control to block individual records from continued processing. Label Security may be appropriate for this use case depending on the application, schema design, and application customization.

Label Security can be used to attach security-related metadata to individual data rows. Labels can then be used to control if a row can be further processed (access control). Another use case under the EU GDPR scope is using labels for consent management, where data labels store users' consent definitions. The EU GDPR's right for erasure can also benefit from Label Security and its data-labeling feature. A process could label rows "to be forgotten" and could be later processed by a data erasure procedure.

Manageability

Policy-based administration enables easy management of data labels, user labels, enforcement options, and protected tables. Multiple Label Security policies can exist in the same database. Oracle Enterprise Manager can manage Label Security policies, data labels, user labels, and protected tables.

Related products

Oracle Database 23ai defense-in-depth solutions

- Oracle Data Safe
- Oracle Advanced Security
- Oracle Key Vault
- Oracle Database Vault
- Oracle Data Masking and Subsetting Pack
- Oracle Audit Vault and Database Firewall
- Oracle Database Security Assessment Tool

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