ORACLE

Oracle Label Security

Frequently Asked Questions

[1.0]

The need for more sophisticated controls on access to sensitive data is becoming increasingly important as organizations address emerging security requirements around data consolidation, privacy, and compliance. Maintaining separate databases for highly sensitive customer data is costly and creates unnecessary administrative overhead. However, consolidating databases sometimes means combining sensitive financial, HR, medical, or project data from multiple locations into a single database for reduced costs, easier management, and better scalability. Oracle Label Security provides the ability to tag data with a data label or a data classification to allow the database to inherently know what data a user or role is authorized for, and will enable data from different sources to be combined in the same table as a more extensive data set without compromising security.

Access to sensitive data is controlled by comparing the data label with the requesting user's label or access clearance. A user label or access clearance can be considered an extension to standard database privileges and roles. Label Security is centrally enforced within the database, below the application layer, providing strong security and eliminating the need for complicated application views.

This document includes an overview of features and enhancements included in release 23ai. It is intended solely to help you assess the business benefits of upgrading to 23ai and planning for implementing and upgrading the product features described.

PRODUCT OVERVIEW

What is Label Security?

Label Security is a security option for Oracle Database Enterprise Edition. It mediates access to data rows by comparing labels attached to data rows in application tables (sensitivity labels) and user labels (clearance labels). Label Security is also included in the Oracle Autonomous Database and the High Performance and Extreme Performance editions of the Oracle Cloud Infrastructure (OCI) databases.

Who should consider Label Security?

Sensitivity labels are used in some form in virtually every industry. These industries include health care, law enforcement, energy, retail, national security, and defense. Examples of label use include:

- Separating data for individual branch stores, franchisees, or regions.
- Financial companies separating customer data spanning multiple countries with strong government privacy controls.
- Consolidating and securing data for sensitive R&D projects.
- Minimizing access to individual healthcare records to only the health professionals providing direct care
- Protecting HR data from different divisions of a company.
- Securing classified data based on user clearance level for government and defense use.
- Complying with the U.S. State Department's International Traffic in Arms (ITAR) regulations.
- Supporting multiple customers in a multi-tenant SaaS application.
- Restricting data processing, tracking consent, and handling right to erasure requests under EU GDPR

What can Label Security do for my security needs?

Label Security can label data and restrict access with high granularity. This is particularly useful when multiple organizations, companies, or users share a single application. Sensitivity labels can limit application users to a subset of data within an organization without changing the application. Data privacy is important to consumers, and stringent regulatory measures continue to be enacted. Label Security can be used to implement privacy policies on data, restricting access to only those who have a need to know.

ORACLE

COMPONENTS AND FEATURES

What are the main components of Label Security?

Label Security provides row-level data access controls for application users. Label Security is so named because each user and data record has an associated security label.

The User label consists of three components: a level, zero or more compartments, and zero or more groups. It is assigned as part of the user authorization and is not modifiable by the user.

Session labels also consist of the same three components and are different from the user label based on the session established by the user. For example, if the user has a Top Secret level component but logged in from a Secret workstation, the session label level would be Secret.

Data security labels have the same components as the User and Session labels. The three label components are level, compartment, and group.

- **Levels** indicate the sensitivity level of the data and the authorization for a user to access sensitive data. To access that record, the user (and session) level must be equal to or greater than the data level.
- Data can be part of zero or more **compartments**. The user/session label must have every compartment that the record data label has for the user to retrieve the record successfully. For example, if the data label compartments are A, B, and C, the session label must at least contain A, B, and C to access that data record.
- Data can have zero or more **groups**. The user/session label needs at least one group that matches a data record's group(s) to access the data record. For example, if the data record had Boston, Chicago, and New York as groups, then the session label needs only Boston (or one of the other two groups) to access the data.
- Protected objects are tables with labeled records.
- Label Security policies combine User labels, Data labels, and protected objects.

Does Label Security provide column-level access control?

No, Label Security policies do not operate on columns. However, a column-sensitive Virtual Private Database (VPD) policy can determine access to a specific column by evaluating Label Security user labels.

A VPD policy can be written so that it only becomes active when a particular column (the 'sensitive' column) is part of an SQL statement against a protected table. With the 'column sensitivity' switch on, VPD either returns only those rows that include information in the sensitive column the user is allowed to see, or all rows with all cells in the sensitive column being empty, except those values the user can access.

Can I base Secure Application Roles on Label Security?

The procedure determining if the 'set role' command is executed can evaluate Label Security user labels. The Label Security policy does not need to be applied to a table since row labels are not part of this solution.

What are Trusted Stored Program Units?

Stored procedures, functions, and packages execute with the definer's system and object privileges (Discretionary Access Control or DAC). If the invoker is a user with Label Security user clearances (labels), the procedure executes with a combination of the definer's DAC privileges and the invoker's security clearances.

Trusted stored procedures are granted the Label Security privilege 'FULL' or 'READ.' When a trusted stored program unit executes, the policy privileges in force are a union of the invoking user's and program unit's privileges.

Are there any administrative tools available for Label Security?

Oracle Enterprise Manager Cloud Control can create and manage Label Security policies in a convenient and integrated environment.

DEPLOYMENT AND ADMINISTRATION

Where can I find Label Security?

Label Security is an option in Oracle Database Enterprise Edition. It is installed as part of the database and only needs to be enabled.

Should I use Label Security to protect all my tables?

The traditional Oracle discretionary access control (DAC) object privileges SELECT, INSERT, UPDATE, and DELETE, combined with database roles and stored procedures, are sufficient for most tables. Label Security policies only need to be applied to the most sensitive table or tables.

Are there any guidelines for using Label Security and defining sensitivity labels?

Yes, a comprehensive Label Security Administrator's Guide is available online. In most cases, the security mechanisms included with Oracle Database Enterprise Edition (system and object privileges, database roles, secure application roles) will be sufficient to address security requirements. Label Security should be considered when security is required at the individual row level.

How can I maintain the performance of my applications after applying Label Security access control policies?

As a best practice:

- Only apply sensitivity labels to those tables that need protection. When multiple tables are joined to retrieve sensitive data, apply sensitivity labels to the driving table
- Do not apply Label Security policies to schemas.
- Usually, there is only a small set of different data classification labels; if the table is mainly used for READ operations, try building a Bitmap Index over the (hidden) Label Security column and add this index to existing indexes in that table.

Can I use Label Security with Oracle Database Vault, Real Application Security, and Data Redaction?

Yes. Label Security can provide user labels, which can be used as factors within Oracle Database Vault, and security labels can be assigned to Real Application Security users. Label Security also integrates with Oracle Data Redaction, enabling security clearances to be used in redaction policies.

Can I use Label Security to limit which vector rows get selected in a query?

Yes. Data labels can be applied to rows that include a vector type. For example, when building a generative AI model, labels can limit which data samples are searched during retrieval-augmented generation.

MORE INFORMATION

Where can I find more information on Label Security?

For more information, please see the Label Security page on the Oracle website. Various helpful information is available online, including a datasheet, technical report, and end-user documentation.

https://www.oracle.com/security/database-security/label-security/

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