ORACLE

Oracle Label Security

Frequently Asked Questions

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 compartmentalized customer data is costly and creates unnecessary administrative overhead. However, consolidating databases sometimes means combining sensitive financial, HR, medical, or project data from multiple sources or 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 classification, allowing the database to inherently know what data a user or role is authorized to access. It enables organizations to combine data from different sources in the same table without relying on application access controls.

Oracle Label Security controls access to sensitive data by comparing the data label with the requesting user's label or access clearance. A user label or access clearance works like an extension to standard database privileges and roles. Oracle 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 provides an overview of features and enhancements included in Oracle Database 23ai. It is intended solely to help you assess the business benefits of upgrading to 23ai and planning for the implementation and upgrade of the product features described.

PRODUCT OVERVIEW

What is Oracle Label Security?

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

Who should consider Oracle Label Security?

Virtually every industry uses sensitivity labels in some form. These industries include health care, law enforcement, energy, retail, national security, and defense. Examples of label use include:

- Identifying data from individual branch stores, franchisees, or regions
- Financial companies managing data for customers spanning multiple countries with strong government privacy controls
- Consolidating and securing sensitive R&D projects
- Minimizing access to individual healthcare records
- Protecting HR data from different divisions
- Securing classified data for Government and Defense use
- Complying with 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 Oracle Label Security do for my security needs?

Oracle Label Security can label data and restrict access with high granularity. Managing access based on labels is particularly useful when multiple organizations, companies, or users share a single application. Sensitivity labels can be used to restrict application users to a subset of data within an organization without changing the application. Data privacy is important to consumers, and many government jurisdictions continue enacting stringent regulatory

measures. Oracle Label Security can be used to implement privacy policies on data, restricting access to only those with a need-to-know.

COMPONENTS AND FEATURES

What are the main components of Oracle Label Security?

Label Security provides row-level data access controls for application users. With Label Security, each user and each data record have 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 changeable by the user.

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

Data security labels have the same three components as the User and Session labels.

Label components – 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. For a user to access a record, the user (and session) level must be equal to or greater than the data level for that record.
- Data can be part of zero or more compartments. The user/session label must have every compartment of the record data 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 in the group component. 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 Oracle Label Security provide column-level access control?

No, Oracle Label Security is not column-aware. If column-level access control is required, a column-sensitive Virtual Private Database (VPD) policy can determine access to a specific column by evaluating OLS user labels. Users can specify a VPD policy so that it only becomes active when a particular column (the 'sensitive' column) is part of a 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 it returns all rows, with all cells in the sensitive column being empty, except those values the user is allowed to see.

Can I base Secure Application Roles on Oracle Label Security?

Yes. When using Security Application Roles, the procedure determining if the 'set role' command is executed can evaluate OLS user labels.

What are Trusted Stored Program Units?

Trusted stored program units are stored procedures, functions, and packages executed with the definer's system and object privileges (Discretionary Access Control or DAC). If the invoker is a user with OLS 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 procedures that are either granted the OLS privilege 'FULL' or 'READ.' When a trusted stored program unit runs, 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 Oracle Label Security?

Users can create and manage OLS policies in a convenient and integrated environment with Oracle Enterprise Manager Cloud Control.

DEPLOYMENT AND ADMINISTRATION

Where can I find Oracle Label Security?

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

Should I use Oracle 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. OLS policies only need to be applied to the most sensitive table or tables.

Are there guidelines for using Oracle 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 the Oracle Database Enterprise Edition (for example, system and object privileges, database roles, and secure application roles) will be sufficient to address security requirements. Customers should consider Oracle Label Security when applications require access control security 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 really need protection. For applications that join multiple tables to retrieve sensitive data, try to identify the primary table and apply labels to that table instead of every table in a join.
- Do not apply OLS policies to schemas.
- Usually, there is only a small set of different data classification labels; if the table is mainly used for READ operations, we suggest building a Bitmap Index over the (hidden) OLS column and adding this index to existing indexes in that table.

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

Yes. You can use Oracle Label Security user labels as factors within Oracle Database Vault. Security labels can be assigned to Real Application Security (RAS) users so RAS users will be constrained by OLS policies when you access labeled data. Oracle Label Security also integrates with Oracle Advanced Security Data Redaction, enabling security clearances to be used in Data Redaction policies.

Can I use Oracle Label Security with Oracle E-Business Suite?

Oracle Label Security can be used with Oracle E-Business Suite. Please review Implementation of Security Products on Target Systems EBS, Hyperion and ODI (Doc ID 2884668.1) for more information.

MORE INFORMATION

Where can I find more information on Oracle Label Security?

Website: For more information, please see the Oracle 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 LiveLabs is a great way to try out database features. Oracle Label Security LiveLabs can be run on your tenancy or on a live sandbox that is created just for you.

https://apexapps.oracle.com/pls/apex/dbpm/r/livelabs/view-workshop?wid=676&session=3123740061464

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