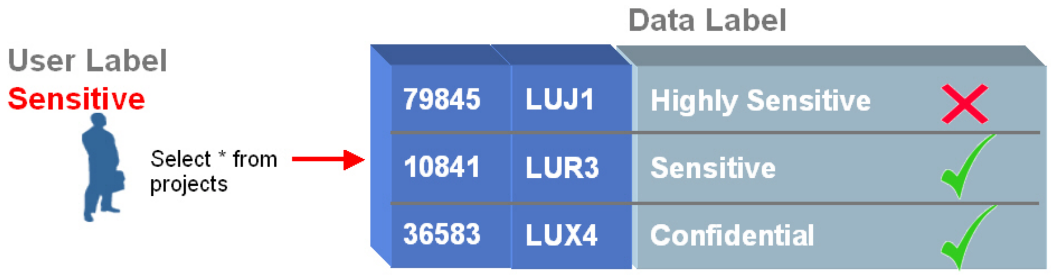
An Oracle White Paper
September 2009

Oracle Label Security with Oracle Database 11g Release 2

Introduction 1
Data Label Components 2
Oracle Label Security Policies 2
User Labels 4
Application Users 5
User Privileges 5
Trusted Stored Procedures 6
Enforcement Options 6
Conditional Where Clauses.. 7
Oracle Label Security Manageability 8
Conclusion 9

Introduction

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 unneccessary administrative overhead. However, consolidating databases sometimes means combining sensitive customer data with confidential customer data. Oracle Label Security provides the ability to tag data with a data label or a data classification. This capability allows the database to inherently know what data is sensitive and allows the sensitive data to be combined in the same table as the larger data set without compromising security.



79845	LUJ1	Highly Sensitive	✗
10841	LUR3	Sensitive	✓
36583	LUX4	Confidential	✓

Figure 1. Oracle Label Security Access Control

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

Data Label Components

Data labels are comprised of a hierarchical level combined with compartments and groups. These label components are used to create data labels as well as to assign security clearances to database or application type users. *Levels* are hierarchical in nature and are used to assign the degree of sensitivity. *Compartments* are used to segregate data within a given *Level* and *Groups* are used to segregate data organizationally within a given *Level*. A given data label can have one *level*, zero or more *compartments* and zero or more *groups* associated with it.

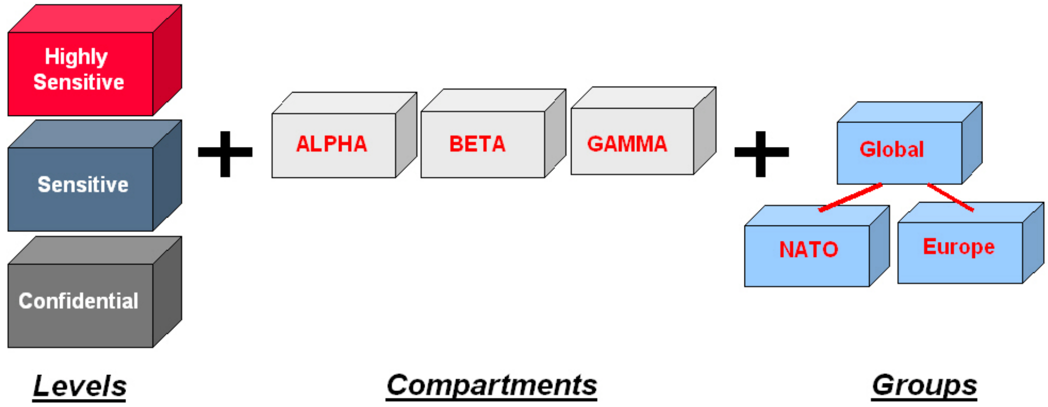


Figure 2. Oracle Label Security Label Components

Oracle Label Security Policies

Oracle Label Security policies are *named* containers for a collection of data labels, user labels, and protected objects. Multiple policies can be defined within a single database. Each Oracle Label Security policy can have a default set of protective enforcement options, such as READ CONTROL and WRITE CONTROL. The default enforcement options are used when a policy is applied to an application table. Enforcement options can also be customized on a per table basis. When defining a Oracle Label Security policy, a column name must be provided to store the data classification label. When a policy is applied to an existing application table, the additional column can be appended as a *hidden* column, thus enabling existing SQL statements to continue working without any changes.

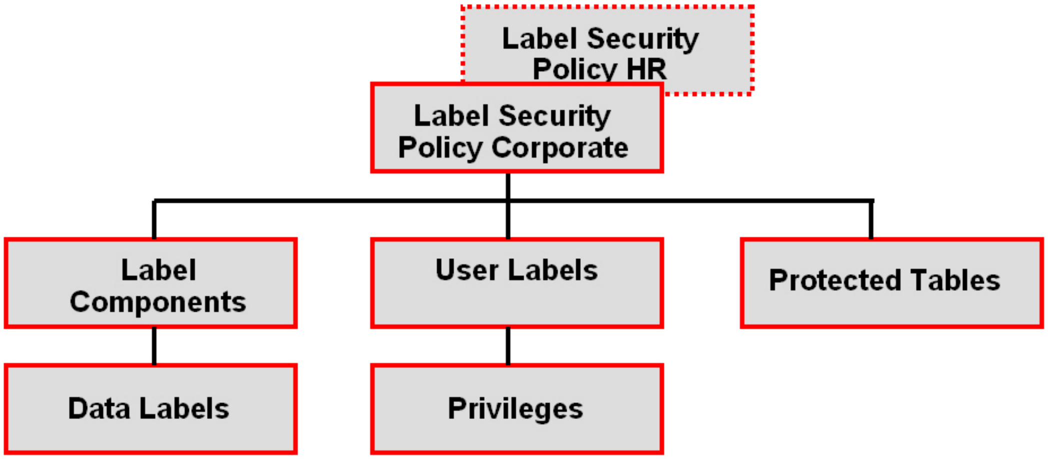


Figure 3. Oracle Label Security Policies

Oracle Label Security provides the ability to define data labels to match specific business and organizational requirements such as healthcare, law enforcement and human resources.

TABLE 1 INDUSTRY SPECIFIC POLICIES AND DATA LABELS

INDUSTRY	LEVEL	COMPARTMENT	GROUP
Government and Defense	Confidential Secret Top Secret	Alpha Beta	NATO Homeland Security
Law Enforcement	Level 1 Level 2 Level 3	Border Security Drug Enforcement	Local Jurisdiction FBI Justice Department
Human Resources	Confidential Sensitive Highly Sensitive	PII Data Investigation	Global United States Europe
Health Care	Confidential Public	VIP Controls	Physician Laboratory

User Labels

User labels are an important part of Oracle Label Security and determine whether a user can access information protected with a data label. User labels are comprised of a minimum and maximum level, a default level and a row level. In addition, user labels can have compartments and groups. For example, a user can be assigned a maximum level of *Sensitive* and a minimum level of *Public*. Database users also have a default label that is initialized when the user connects to the database. This is sometimes referred to as the *active session label*. The *session label* is simply the user's *current level* combined with *compartments and groups*.

TABLE 2 ORACLE LABEL SECURITY – SECURITY CLEARANCE COMPONENTS

CLEARANCE COMPONENT:	DESCRIPTION:
Maximum Level	The maximum sensitivity level a user is authorized to access. For example this might be Sensitive or Highly Sensitive.
Minimum Level	The minimum sensitivity level a user is authorized to write data. For example, an administrator can prevent users from labeling data as Confidential by assigning a minimum level of Sensitive.
Default Level	The level used by default when a user connects to the database. For example, a user can set his or her default level to Sensitive. When he or she connects to the system, the default level will be initialized to Sensitive.
Row Level	The default level used to label data inserted into the database by the user through the application or directly through a tool such as SQL*Plus.
Read Compartments	The set of compartments assigned to the user and used during READ access mediation. For example, if a user has compartments A, B and C, he could view data which has compartments A and B but not data which has compartments A, B, C and D.
Write Compartments	The set of compartments assigned to the user and used during WRITE access mediation. For example, a user could be given READ and WRITE access to compartments A and B but READ-ONLY access to compartment C. If an application record was labeled with compartments A, B and C, the user would not be allowed to update the record because he or she does not have WRITE access on compartment C.
Read Groups	The set of groups assigned to the user and used during READ access mediation. For example, if a user had the group Manager, he could view data that has the Manager group but not data that had only the Senior VP group.
Write Groups	The set of groups assigned to the user and used during WRITE access mediation. For example, a user could be given READ and WRITE access to group *Senior VP* but READ-ONLY access to group *Manager*. If an application record was labeled with a single group, *Manager*, the user would not be allowed to update the record because he or she does not have WRITE access on the *Manager* group.

Application Users

Oracle Label Security supports common application architectures including situations where the middle-tier connects to the database using a single database account. Oracle Label Security does not enforce a relationship between physical database users and user labels. For example, user labels and Oracle Label Security privileges can be assigned to a database user named SCOTT who happens to have a database account or an application user such as JSMITH who is only known to the application layer and doesn't have a real account in the database. The only difference is that when the user SCOTT logs into the database Oracle Label Security will automatically establish an active session label based on levels, compartments and groups assigned to SCOTT. In order for the active session label to be established for application user JSMITH a call to the Oracle Label Security function set_access_profile is required. This function acts as a proxy for Oracle Label Security and accepts an Oracle Label Security policy name along with an application user name.

User Privileges

For added flexibility, users can also be assigned Oracle Label Security specific privileges. Examples of Oracle Label Security specific privileges include *READ* and FULL. The *READ* privilege simply allows a user to view all data regardless of its data classification.

TABLE 3 ORACLE LABEL SECURITY SPECIAL USER PRIVILEGES

PRIVILEGE NAME	DESCRIPTION
READ	The READ authorization enforces no additional read access control. Access mediation is still enforced on UPDATE, INSERT and DELETE operations. Oracle Label Security makes no mediation check on SELECT
FULL	The FULL authorization turns off all Oracle Label Security access mediation. A user with the FULL authorization can perform SELECT, UPATE, INSERT and DELETE operations with no label authorizations. Note that Oracle SYSTEM and OBJECT authorizations are still enforced. For example, a user must still have SELECT on the application table. The FULL authorization turns off the access mediation check at the individual row level.
WRITEDOWN	The WRITEDOWN authorization allows a user to modify the level component of a label and lower the sensitivity of the label. For example, application data which is labeled *Highly Sensitive: Alpha, Beta* could be changed to *Sensitive: Alpha, Beta*. This authorization is only applicable to policies that use the *label update* enforcement option.

WRITEUP	The WRITEUP authorization allows a user to modify the level component of a label and raise the sensitivity of the label. For example, application data which is labeled *Sensitive: Alpha, Beta* could be changed to *Highly Sensitive: Alpha, Beta*. Note that the Maximum Level label authorization assigned to the user would limit modification. This authorization is only applicable to policies that use the *label update* enforcement option.
WRITEACROSS	The WRITEACROSS authorization allows a user to modify the compartments and groups in a label to any valid compartment and group defined in Oracle Label Security for the policy. For example, data labeled *Sensitive: Alpha* could be modified to *Sensitive: Alpha, Beta* even though the user was not authorized for the Delta compartment. This authorization is only applicable to policies that use the label update enforcement option.
PROFILEACCESS	The PROFILE ACCESS authorization allows a user to assume the Oracle Label Security authorizations of another user. For example, user Scott who has access to compartments A, B, and C could assume the profile of user Joe who has access to compartments A, B, C and D. This functionality might be useful in an environment where an application uses a single application account for all application users. Note that the PROFILEACCESS privilege cannot be granted to a stored procedure.

Trusted Stored Procedures

The Oracle Label Security privileges READ and FULL can be granted to stored procedures, enabling access all data within the execution context of stored procedure but not directly by the user calling the stored procedure or function.

Enforcement Options

Oracle Label Security provides flexible enforcement options. The READ CONTROL enforcement options checks the data label on read or *Select* operations. The WRITE CONTROL enforcement option checks the data label on *Insert*, *Update* and *Delete* operations. Default enforcement options can be specified for each policy.

TABLE 4 ORACLE LABEL SECURITY POLICY ENFORCEMENT OPTIONS

ENFORCEMENT OPTION	**DESCRIPTION**
READ CONTROL	Applies policy enforcement to SELECT operations using the Oracle Label Security algorithm for read access.
INSERT CONTROL	Applies policy enforcement to INSERT operations using the Oracle Label Security algorithm for write access.
UPDATE CONTROL	Applies policy enforcement to UPDATE operations using the Oracle Label Security algorithm for write access.

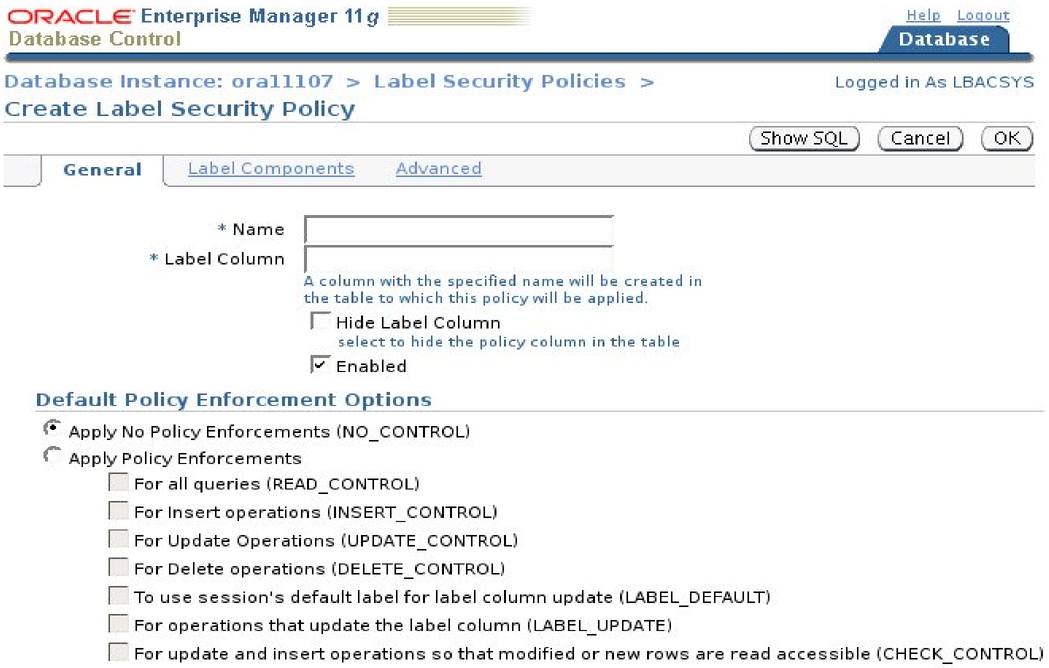
DELETE CONTROL	Applies policy enforcement to DELETE operations using the Oracle Label Security algorithm for write access.
WRITE CONTROL	Applies policy enforcement on INSERT, UPDATE, and DELETE operations. If this option is set, it enforces INSERT_CONTROL, UPDATE_CONTROL, and DELETE_CONTROL.
LABEL DEFAULT	If the user does not explicitly specify a label on INSERT, the user’s default row label value is used. By default, the row label value is computed internally by Oracle Label Security using the user’s label. The default value would be comprised of the default ROW LEVEL combined with the WRITE COMPARTMENTS and WRITE GROUPS. A user can set the row label independently, but only to: A level which is less than or equal to the level of the session label, and greater than or equal to the user’s minimum level. Include a subset of the compartments and groups from the session label, for which the user is authorized to have write access.
LABEL UPDATE	Applies policy enforcement to UPDATE operations that set or change the value of a label attached to a row. The WRITEUP, WRITEDOWN, and WRITEACROSS privileges are only enforced if the LABEL_UPDATE option is set.
LABEL CHECK	Applies READ_CONTROL policy enforcement to INSERT and UPDATE statements to assure that the new row label is read-accessible by the user after and INSERT or UPDATE statement.
NO CONTROL	Applies no enforcement options. A labeling function or a SQL predicate can nonetheless be applied.

Conditional Where Clauses

Oracle Label Security also provides the ability to add a restrictive *‘where*’ clause or *‘condition’* when a policy is applied to an application table. This ‘*where’* clause is used in conjunction with data labels to determine access and provides an easy to use, simple capability similar to creating an Oracle Virtual Private Database (VPD) policy. The *‘where’* clause is attached to the Label Security policy, thus there is no need to create a separate PL/SQL package as is the case with pure VPD type implementations

Oracle Label Security Manageability

Oracle Label Security can be managed from Oracle Enterprise Manager. The Oracle Label Security management link can be found in the *Security* section under the *Server* tab. Oracle Label Security integration with Oracle Identity Management provides centralized management of policy definitions, data labels and user label authorizations. Oracle Identity Management must be licensed separately.



Database Instance: ora11107 > Label Security Policies >

Logged in As LBACSYS

Create Label Security Policy

* Name

* Label Column

A column with the specified name will be created in the table to which this policy will be applied.

□ Hide Label Column

select to hide the policy column in the table

☑ Enabled

Default Policy Enforcement Options

● Apply No Policy Enforcements (NO_CONTROL)

○ Apply Policy Enforcements

□ For all queries (READ_CONTROL)

□ For Insert operations (INSERT_CONTROL)

□ For Update Operations (UPDATE_CONTROL)

□ For Delete operations (DELETE_CONTROL)

□ To use session's default label for label column update (LABEL_DEFAULT)

□ For operations that update the label column (LABEL_UPDATE)

□ For update and insert operations so that modified or new rows are read accessible (CHECK_CONTROL)

FIGURE 4 ORACLE LABEL SECURITY ENTERPRISE MANAGER INTERFACE

Conclusion

Oracle Label Security provides the industries most advanced and flexible data classification solution, enabling the Oracle database to inherently know the sensitivity of data consolidated from multiple databases. Oracle Label Security provides the ability to define data labels, assign user labels and protect sensitive application data within the Oracle database. Oracle Label Security policies provide the ability to define custom data labels for virtually any industry ranging from healthcare to law enforcement. Flexible enforcement options allow access control to be finely tuned. Management of Oracle Label Security policies can be performed using Oracle Enterprise Manager and integration with Oracle Identity Management provides centralized enterprise management.

Oracle Label Security with
Oracle Database 11g Release 2
September 2009
Author: Paul Needham
Contributing Authors:

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com

Oracle is committed to developing practices and products that help protect the environment

0109