

# ORACLE LABEL SECURITY



## KEY FEATURES AND BENEFITS



- Transparent row level access control using sensitivity labels
- Integrated with Oracle Database Vault
- Policy based administration model allows multiple policies to exist in the same database
- Hidden columns provide complete transparency to existing application SQL
- Implements Multi-Level Security for government and defense
- Evaluated for EAL4+ Common Criteria
- Oracle Database 11g Enterprise Edition Security Option, available for Oracle8i Enterprise Edition Databases and higher

*Oracle Label Security enables transparent row level access control in the Oracle database using sensitivity labels. Used in combination with Oracle Database Vault, sensitivity labels become powerful factors for use in multi-factor authorization, helping address regulatory compliance requirements. Highly flexible and adaptable, Oracle Label Security is the industry's most advanced label based access control product. Policy based administration simplifies the management of sensitivity labels and user label authorizations.*

### Protect Sensitive Data

Oracle Label Security transparently controls access to application data by comparing data sensitivity labels with user label authorizations. Using Oracle Enterprise Manager, security administrators define data sensitivity labels and assign label authorizations to users, including the maximum sensitivity label an individual user is allowed to access. Security administrators can then apply Label Security policies to one or more application tables. Once applied, Label Security will transparently mediate access to application data by

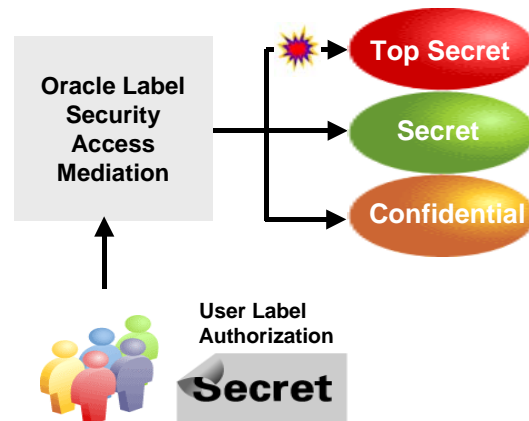


Fig. 1 Oracle Label Security Overview

comparing the user label authorization with the sensitivity label assigned to the data. Only if the user label authorization is equal to or greater than the data sensitivity level will access to the data be allowed. Data sensitivity labels can be comprised of three components. A mandatory, hierarchical level, plus zero or more horizontal compartments, plus zero or more parent child groups. For example, the sensitivity label *Secret:ProjectAthens:ExecOnly* is comprised of the level *Secret*, the compartment *ProjectAthens* and the group *ExecOnly*. Many organizations may only use the level component.

### Integrated With Oracle Database Vault

Used in combination with Oracle Database Vault, sensitivity labels become powerful factors for use in multi-factor authorization, helping address regulatory compliance requirements. For example, user label authorizations can be used in Oracle Database Vault command rules

**ORACLE LABEL SECURITY****RELATED PRODUCTS:**

The following products provide additional security to help meet security, privacy and regulatory requirements:

- Oracle Database Vault
  - Protect application data from DBA and privileged users
  - Transparently control access to applications and databases
  - Protect against database changes
- Oracle Advanced Security
  - Transparent Data Encryption with no modification to application SQL code
  - Supports AES 256
  - Strong Authentication
  - Network Encryption
- Oracle Secure Backup
  - Encrypt database and file system data during tape backup
  - Integrated with Oracle Recovery Manager (RMAN) and supports up to 256 bit AES

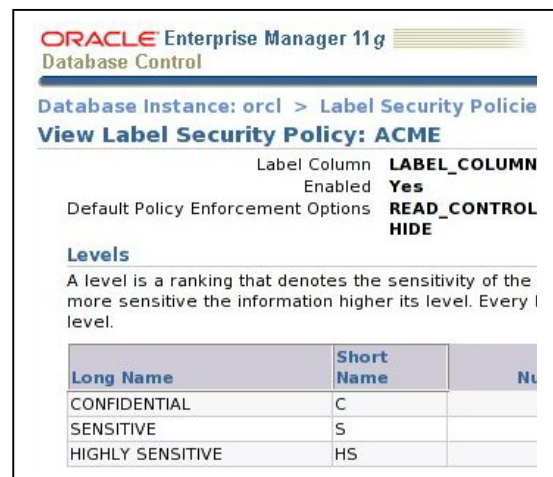
to control access to the database, SQL commands and application tables. This powerful new capability extends Label Security concepts beyond traditional row level access controls to mediation at the database and application level.

**Flexible and adaptable**

Oracle Label Security provides multiple enforcement options for access control at the row level. Policies can be applied for read operations only, update operations only or both. User label authorizations include a maximum read label, default write label and default session label. The maximum read label specifies the maximum data sensitivity label a user is allowed access to, the default write label is the default data sensitivity label assigned to data the user inserts and the default session label is the default sensitivity label a user has when connecting to the database. This must be equal to or less than the maximum read label. Special authorizations allowing access to all data for either read or update operations regardless of the users label authorizations can be granted to users and stored procedures. Special authorizations are useful for patching and maintenance purposes. Proxy capability for one big user applications is provided through the Label Security profile access authorization, allowing the primary application user to assume the label authorizations of an application user. SQL predicates or 'where' clauses can optionally be added to any Label Security policy, extending access control beyond the sensitivity label. Note that label authorizations can be granted to non-database users. This model supports common application architectures.

**Simplified Manageability**

Oracle Label Security provides an easy to use policy based administration model. Policies are the logical containers of sensitivity labels, label authorizations and optionally protected objects. Multiple policies can exist in the same database. Optional integration with Oracle Identity Management provides centralized management of policies and user label authorizations. In addition to the Enterprise Manager Label Security console, a comprehensive Label Security API is provided.



Copyright 2007, Oracle. All Rights Reserved.

This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor is it subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.