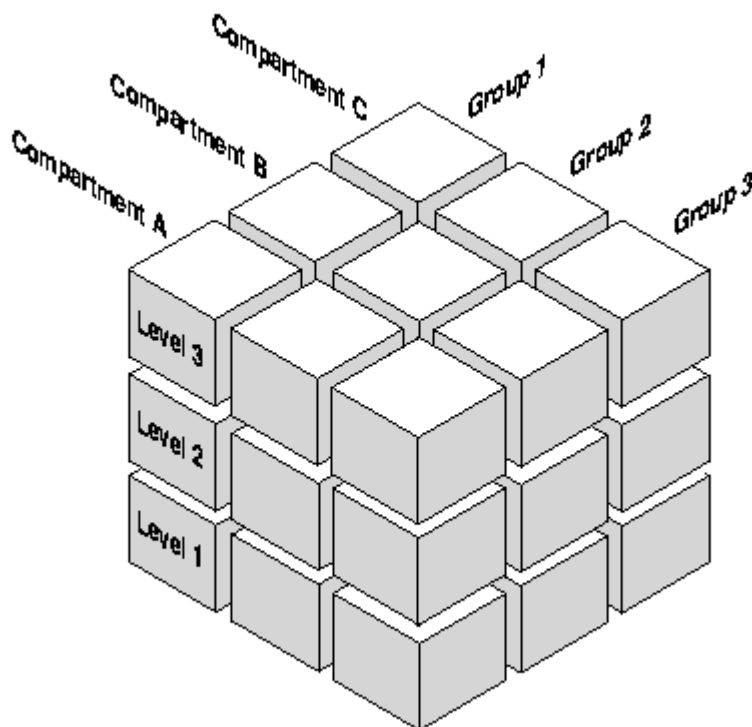


data sheet Oracle9i Label Security™

Traditional information systems have not allowed data to be separated into different sensitivities within a single database. As a result, many organizations were forced to physically separate data on different machines, build complex application code, or rely on highly proprietary operating systems which supported few commercial applications. Oracle9i Label Security is a security option for the Oracle9i Enterprise Edition and dramatically reduces the need to isolate information, build complex application code, and rely on manual or physical controls to protect your data. Oracle9i Label Security mediates access to data by comparing a sensitivity label assigned to a piece of data with label authorizations assigned to an application user. This type of access mediation allows data to be separated into different sensitivities within a single database. Application hosting, database consolidation, healthcare, franchise management, national security, and privacy enforcement are just a few of the areas which can benefit from Oracle9i Label Security.

Access Control

Discretionary access control (DAC) is used to mediate user access to data through database privileges such as SELECT, INSERT, UPDATE and DELETE. Access to data is controlled based on the identity of users and their access privileges. Standard Oracle9i supports extensive DAC and data encryption at a fine level of granularity, satisfying most security requirements. Oracle9i Enterprise Edition with Oracle9i Label Security supports both DAC and label based access control using sensitivity labels, providing multidimensional access control through hierarchical sensitivity levels, information compartmentalization and group/organizational hierarchies.



Flexible and Highly Customizable Policy Management

Oracle9i Label Security policies are collections of sensitivity labels, user label authorizations and enforcement options grouped together and given a unique name. The policy name, assigned by the

security office or application administrator, allows the security policy to be easily managed and applied to application tables or entire database schemes. Once applied to an application table, policy enforcement can be easily fine tuned using Oracle9i Policy Manager (OPM). Oracle Advanced Security encryption can optionally be used to encrypt all traffic flowing between the Oracle9i Policy Manager and the Oracle database.

Oracle9i Policy Manager

Oracle9i Policy Manager is the new Java GUI for managing Oracle Label Security policies as well as user defined Virtual Private Database (VPD) policies. Using Oracle9i Policy Manager you can create policies, define label components, create labels, establish user label authorizations, customize enforcement options, apply policies to schemes and tables, drop policies from schemes and tables, disable policies, define an application context, and create VPD policy groups. Oracle9i Policy Manager is the administration tool for managing policies to protect information at the row level.

Label Management and Data labeling

Oracle9i Label Security labels are managed using Oracle9i Policy Manager or the Oracle9i Label Security command line API. Labels definitions are stored in the Oracle9i database for easy maintenance and security. Oracle Label Security provides numerous methods for labeling data depending on specified enforcement options. These include the DEFAULT_LABEL enforcement option which uses a default label associated with the user. The label must be within the user's label authorization range. The LABEL function option references a PL/SQL function which computes the label based on values contained in the data or other factors.

Networking, Replication and Distributed Environments

Oracle9i Label Security policies are enforced in the database. Policies are enforced regardless of whether you connected via the Internet, client server, n-tier, locally or through a database link. Oracle9i Label Security supports standard replication and advanced replication, including multimaster replication and materialized views (snapshots).

Distributed databases behave in the standard way with Oracle9i Label Security: the local user ends up connected as a particular remote user. Oracle9i Label Security protects the labeled data, whether you connect locally or remotely. If the remote user has the appropriate labels, you can access the data. If not, you cannot access the data.

The database link sets up the connection to the remote database and identifies the user that will be associated with the remote session. Your Oracle9i Label Security authorizations on the remote database are based upon those of the remote user identified in the database link.

Auditing

Oracle9i Label Security auditing supplements standard Oracle9i auditing by tracking use of its own administrative operations, and use of the policy privileges. You can use Oracle9i Policy Manager to set and change the auditing options for an Oracle Label Security policy.

When you create a new policy, a label column for that policy is added to the database audit trail. The label column is created regardless of whether auditing is enabled or disabled, and independent of whether database auditing or operating system auditing is used. Whenever a record is written to the audit table, each policy provides a label for that record to indicate the session label. The administrator can create audit views using a supplied API package to display these labels. Note that in the audit table, the label does not control access to the row; instead, it simply records the sensitivity of the row.

Export

Oracle9i Label Security is approved for export worldwide.

Evaluations

Oracle9i Label Security will be evaluated under the ISO/IEC 15408 Common Criteria. Security

evaluations provide an independent security assessment of the security protection mechanisms provided with Oracle9i Label Security.

Performance

Oracle9i Label Security is highly optimized for row level security.

KEY FEATURES

Multi-dimensional access control

- 10,000 Levels
- 10,000 Compartments
- 10,000 Groups
- Multiple policies per table
- Hidden policy enforcement column option

Customizable Enforcement

- Row level READ CONTROL
- Row level WRITE CONTROL
- Label WRITEUP protection - prohibit increasing sensitivity
- Label WRITEDOWN protection - prohibit decreasing sensitivity
- Label WRITEACROSS protection - prohibit compartment and group modification
- SQL*Predicate interface

Data Labeling Options

- User specified default
- Explicit label specification
- Intelligent label computation functions
- Trusted stored program units

Selective protection

- Protect entire schemes or individual tables
- Customizable enforcement on a per table basis
- Read and write authorization granularity on individual groups and compartments

Standard Operating Systems

- Oracle9i Label Security is available on

Administratively Controlled Individual User Label Authorizations

- Maximum level - maximum accessible sensitivity level for user
- Minimum level - minimum accessible sensitivity level for user
- Default level - default sensitivity level after application authentication for user
- Row level - sensitivity level assigned for new data inserted by user
- Read compartments - list of compartments user is authorized to read. User can read a row if he or she has all compartments in a label
- Read groups - list of groups user is authorized to read. User can read a row if he or she has one of the groups in a label
- Write compartments - list of compartments user is authorized to write. User can write to a row if all compartments in a label are in this list.
- Write groups - list of groups user is authorized to write. User can write to a row if one of the groups in a label are in this list.

Administratively Controlled Policy Enforcement Options

- READ control - protection on read/select operations
- INSERT control - protection on insert operations
- UPDATE control - protection on update operations
- DELETE control - protection on delete operations
- LABEL Update - protects modification of the label

most commercial operating systems including Sun Solaris and HP/UX.

Stringent Row Level Security

- Product functionality is based on stringent government and commercial requirements for row level security

Policy Administration and Management Tools

- Oracle9i Policy Manager
- Comprehensive API - see the Oracle9i Label Security Administrator's guide and the Oracle9i Application Developer's Guide.

Documentation and Training

- A comprehensive Oracle9i Label Security administrator's guide is provided with the Oracle9i Enterprise Edition. The administrator's guide can be viewed in PDF and HTML.
- A no-cost, web based e-Seminar is available on the Oracle Learning Network. Visit the Oracle Technology Network and select the training and support tab.

RELATED PRODUCTS AND SERVICES

Oracle9i Label Security is a database option and provides row level security. The Oracle9i Advanced Security database option is also available.

Oracle9i Advanced Security Database

- LABEL Check - perform READ check after label assignment to prevent accidental over classification
- NO CONTROL - disables enforcement
- LABEL Default - label new data using application users default sensitivity label

Administratively Controlled Special User Authorizations

- READ - User with this authorization can perform read/select operations without row level security enforcement. Other Oracle9i Label Security enforcement options are still enforced. Read operations are still restricted by standard Oracle discretionary access controls.
- FULL - User with this authorization has access to all data and is restricted only by standard Oracle discretionary access controls. No row level security enforcement.
- PROFILE ACCESS - User with this authorization can assume the Oracle9i Label Security authorizations of another user.

Trusted Program Units

- Assign Oracle PL/SQL stored procedures Oracle9i Label Security READ and FULL authorizations, reducing need to authorize individual users.
- Convenient for administrative reports which need to access all data.

Standards

- Oracle9i Label Security will be evaluated under the ISO/IEC 15408 Common Criteria.

GETTING STARTED

Oracle9i Label Security is an add-on option available with the Oracle9i Enterprise Edition. Oracle9i Policy Manage is installed by default with the Oracle9i Enterprise Edition.

Option

- Enterprise user security / LDAP directory integration
- Single sign-on
- Network encryption
- Public Key Infrastructure (PKI)
- Strong authentication

Oracle9i Label Security is not installed by default with the Oracle9i Enterprise Edition. To install Oracle9i Label Security, start the installer and select the custom installation option.

[Top of Page](#) | [Copyright and Corporate Info](#)