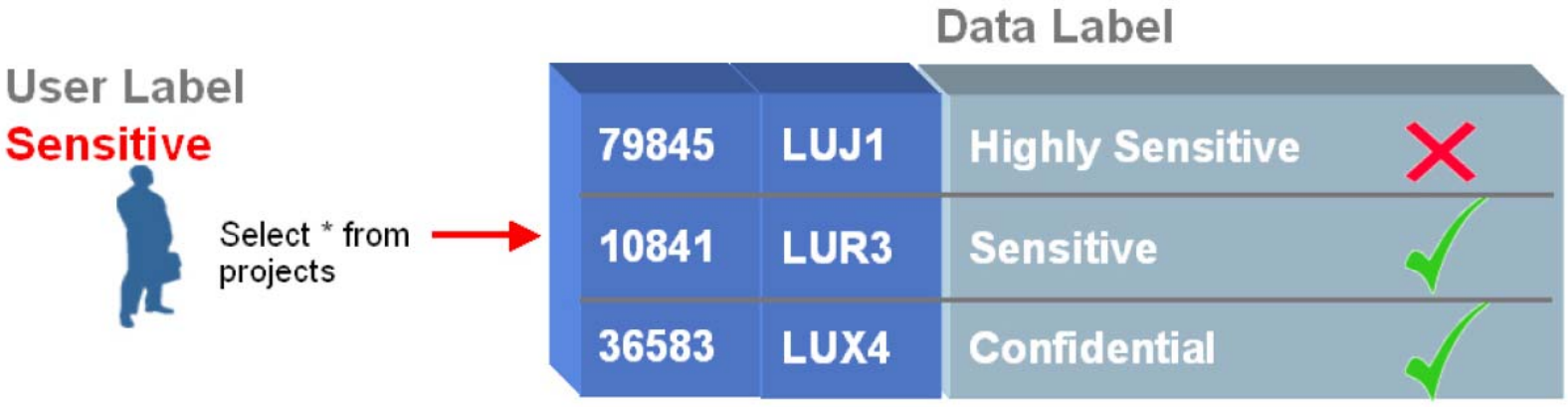
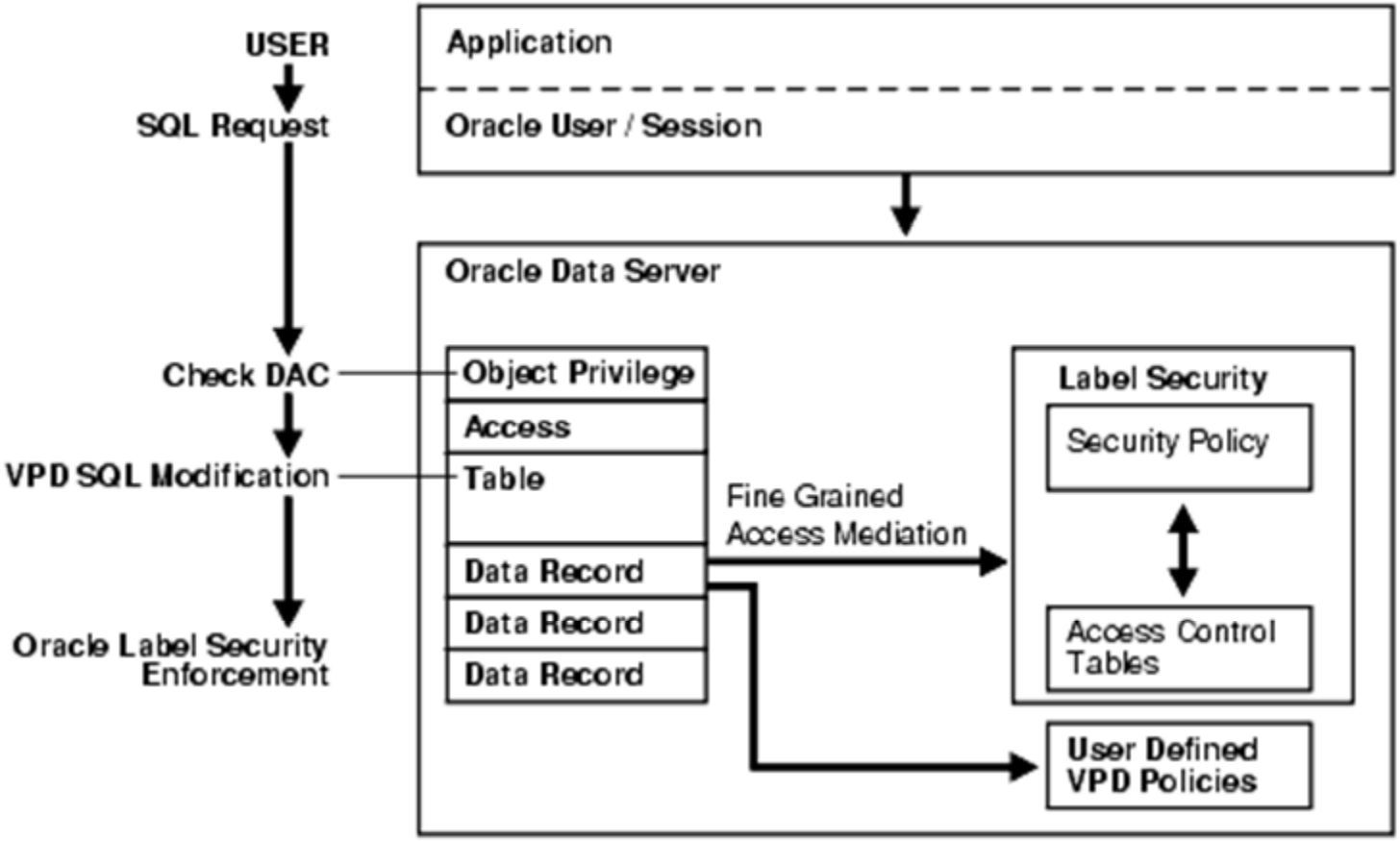
Case Study:
Oracle Label Security



Oracle Label Essential Concepts

- Oracle Label Security enables row-level access control, based on the virtual private database technology of Oracle Enterprise Edition
- It controls access to the contents of a row by comparing that row's label with a user's label and privileges
- Administrators can add selective row-restrictive policies to existing databases
- Developers can add label-based access control to their Oracle applications

Oracle Label Architecture

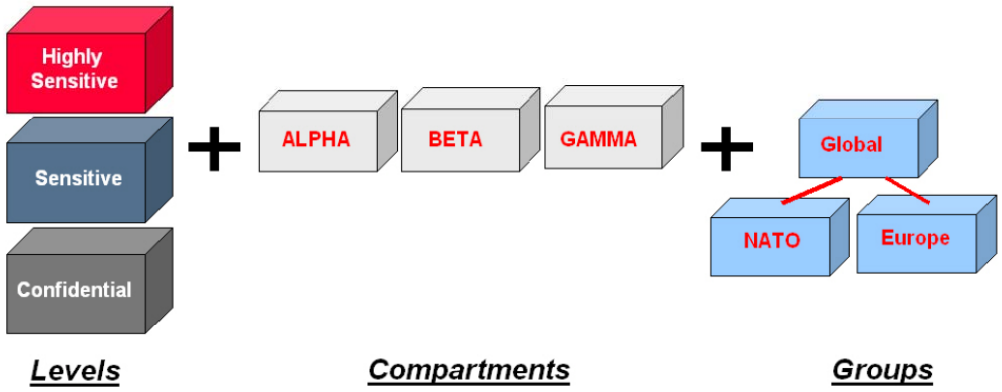


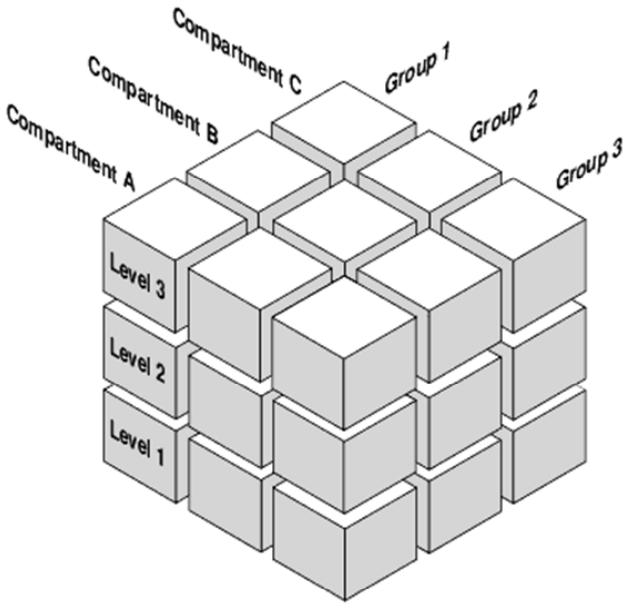
Label policy features

- Oracle label controls the access to data by using 3 factors:
  - The label of the data row to which access is requested
  - The label of the user session requesting access
  - The policy privileges for that user session

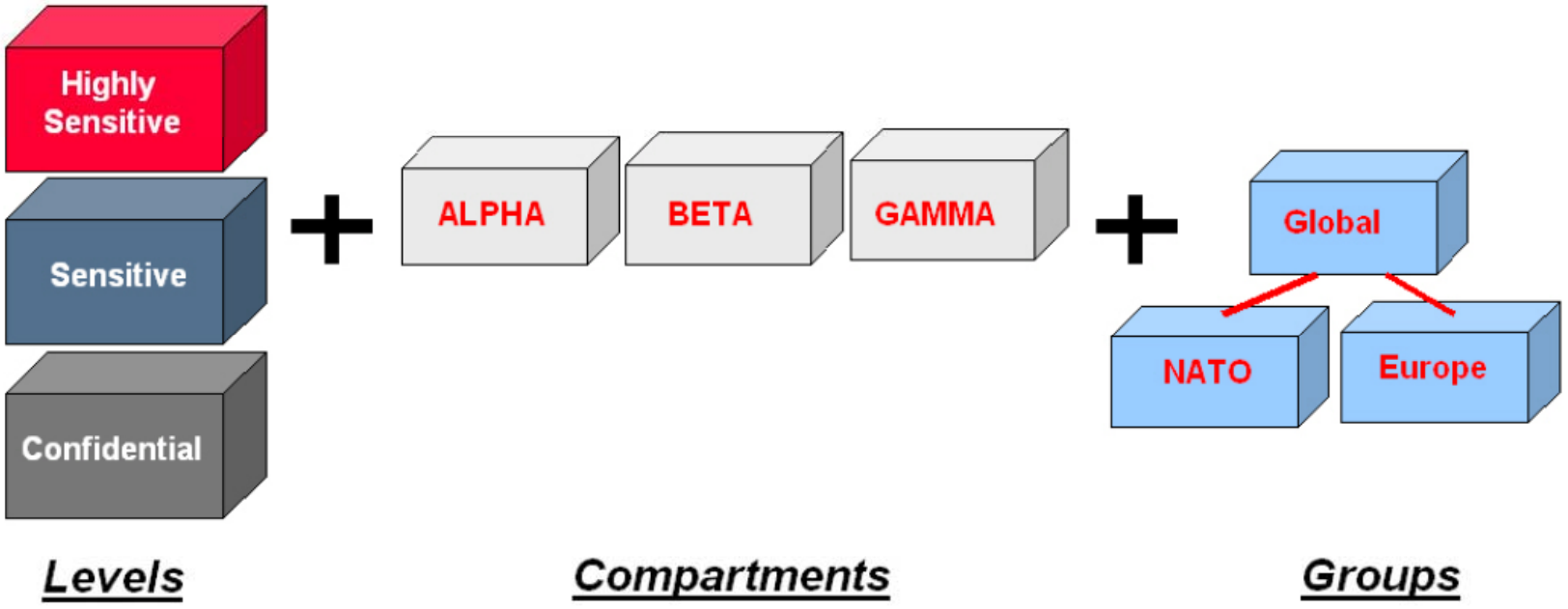
Data Labels

- Every label contains three components:
  - a single level (sensitivity) ranking
  - zero or more horizontal compartments or categories
  - zero or more hierarchical groups





Data Labels



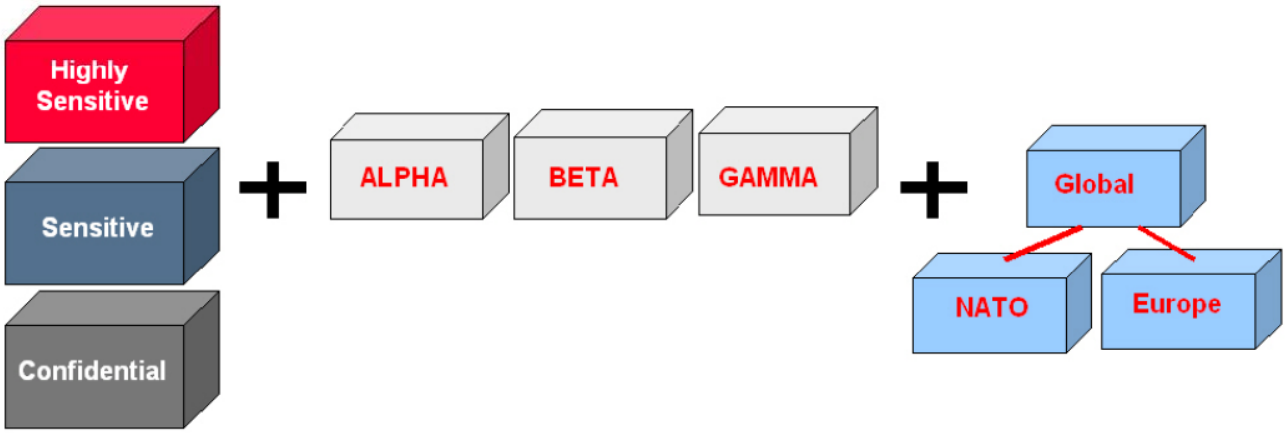
Example:
Confidential (10)
Highly Confidential (20)
Sensitive (30)

The more sensitive the information, the higher its level.
The less sensitive the information, the lower its level.

NOTE: Labels have a character form and a numeric form

Data Labels: Compartments

- Compartments identify areas that describe the sensitivity of the labeled data, providing a finer level of granularity within a level
- The compartment component is not hierarchical



Example:
Confidential (10)
Highly Confidential (20)
Sensitive (30)

Departments:
Finance (it has sensitive and highly confidential data)
Chemical (it has sensitive data)
Operation (it has sensitive, highly confidential and confidential data)

Data Labels: Compartments

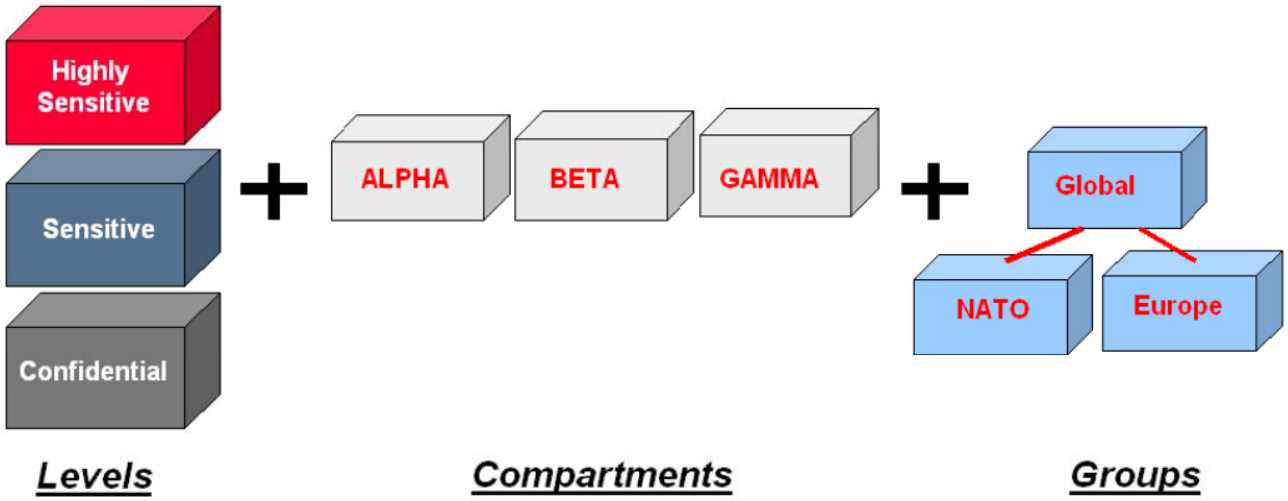
Levels:	**Compartments:**		
Sensitive	Financial	Chemical	Operation
HC	Financial		Operation
Confidential			

- Note that some data in the protected table may not belong to any compartment.
- If compartments are specified, then a user whose level would normally permit access to a row's data will nevertheless be prevented from such access unless the user's label also contains all the compartments appearing in that row's label.

Data Labels: Groups

- The group component is hierarchical and is used to reflect ownership
- EXAMPLE: suppose one has two groups of users, Finance and Engineering. Users with the label Finance cannot access to data labeled Engineering (and vice versa), because they are “at the same level”
- Suppose that one has a group Board of Directors (BoD). Users in this group must be allowed to access the data of both Finance and Engineering group.
- To this end, one can establish a group hierarchy, where BoD is the group “parent” of Finance and Engineering groups

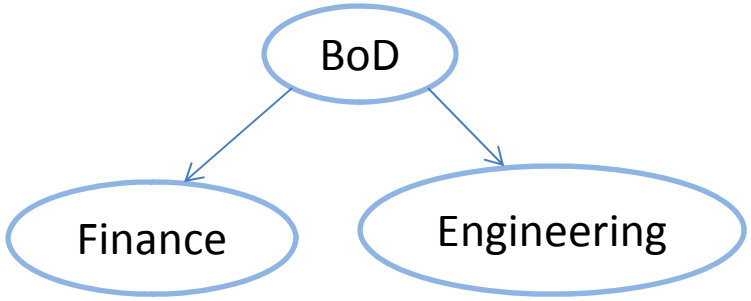
Data Labels: Groups



Example:
Confidential (10)
Highly Confidential (20)
Sensitive (30)

Departments:
Finance
Chemical
Operation

Groups:



Data Labels

- A label can be any one of the following four combinations of components:
  - a single level component, with no groups or compartments, such as U::
  - a level and a set of compartments with no groups, such as U:Alpha, Beta:
  - a level and a set of groups with no compartments, such as U::FIN, ASIA
  - a level with both compartments and groups, such as U:Beta,Psi:ASIA,FIN

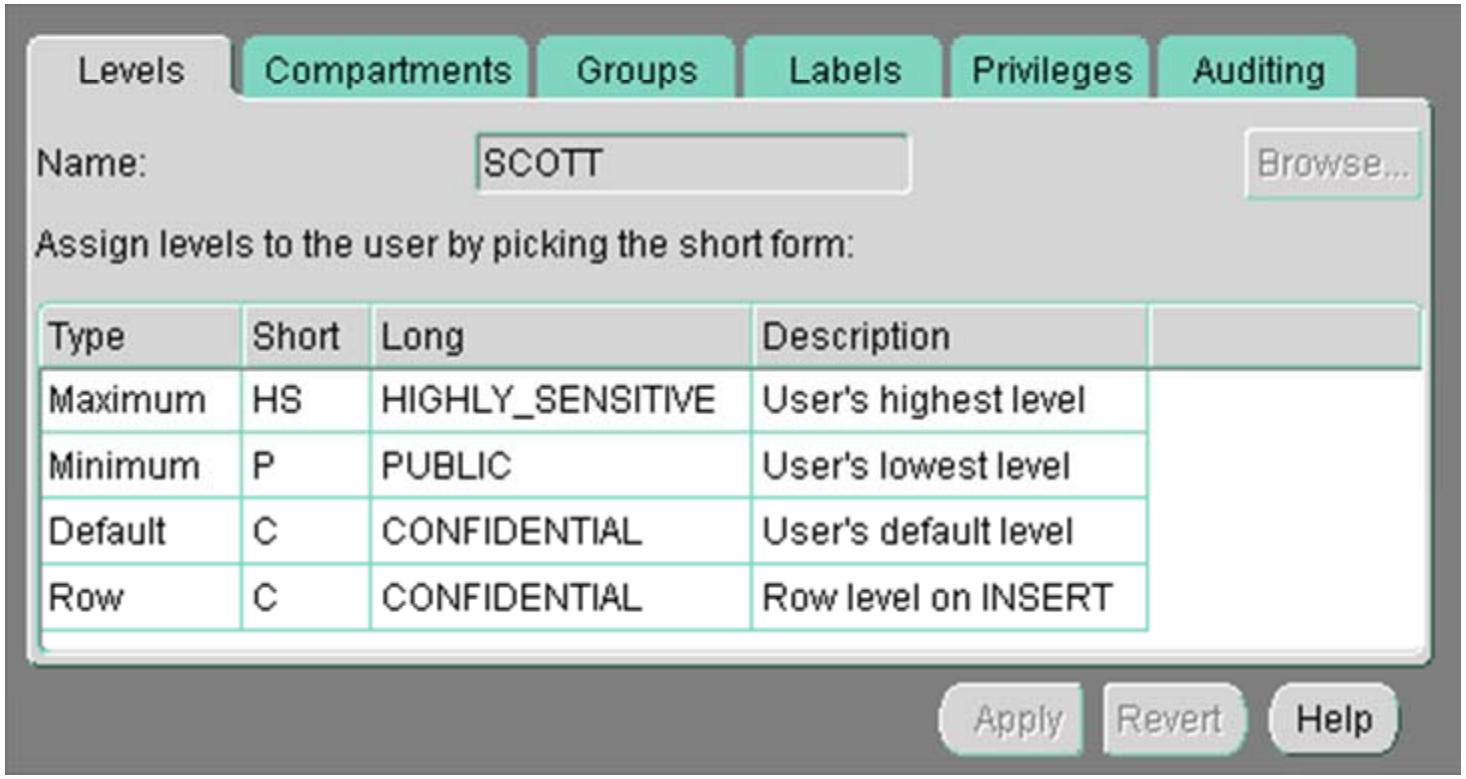
Examples

Industry	Levels	Compartments	Groups
Defense	TOP_SECRET SECRET CONFIDENTIAL UNCLASSIFIED	ALPHA DELTA SIGMA	UK NATO SPAIN
Financial Services	ACQUISITIONS CORPORATE CLIENT OPERATIONS	INSURANCE EQUITIES TRUSTS COMMERCIAL_LOANS CONSUMER_LOANS	CLIENT TRUSTEE BENEFICIARY MANAGEMENT STAFF
Judicial	NATIONAL_SECURITY SENSITIVE PUBLIC	CIVIL CRIMINAL	ADMINISTRATION DEFENSE PROSECUTION COURT
Health Care	PRIMARY_PHYSICIAN PATIENT_CONFIDENTIAL PATIENT_RELEASE	PHARMACEUTICAL INFECTIOUS_DISEASES	CDC RESEARCH NURSING_STAFF HOSPITAL_STAFF

User Labels

- A user label specifies that user's sensitivity level plus any compartments and groups that constrain the user's access to labeled data.
- Each user is assigned a range of levels, compartments, and groups, and each session can operate within that authorized range to access labeled data within that range.

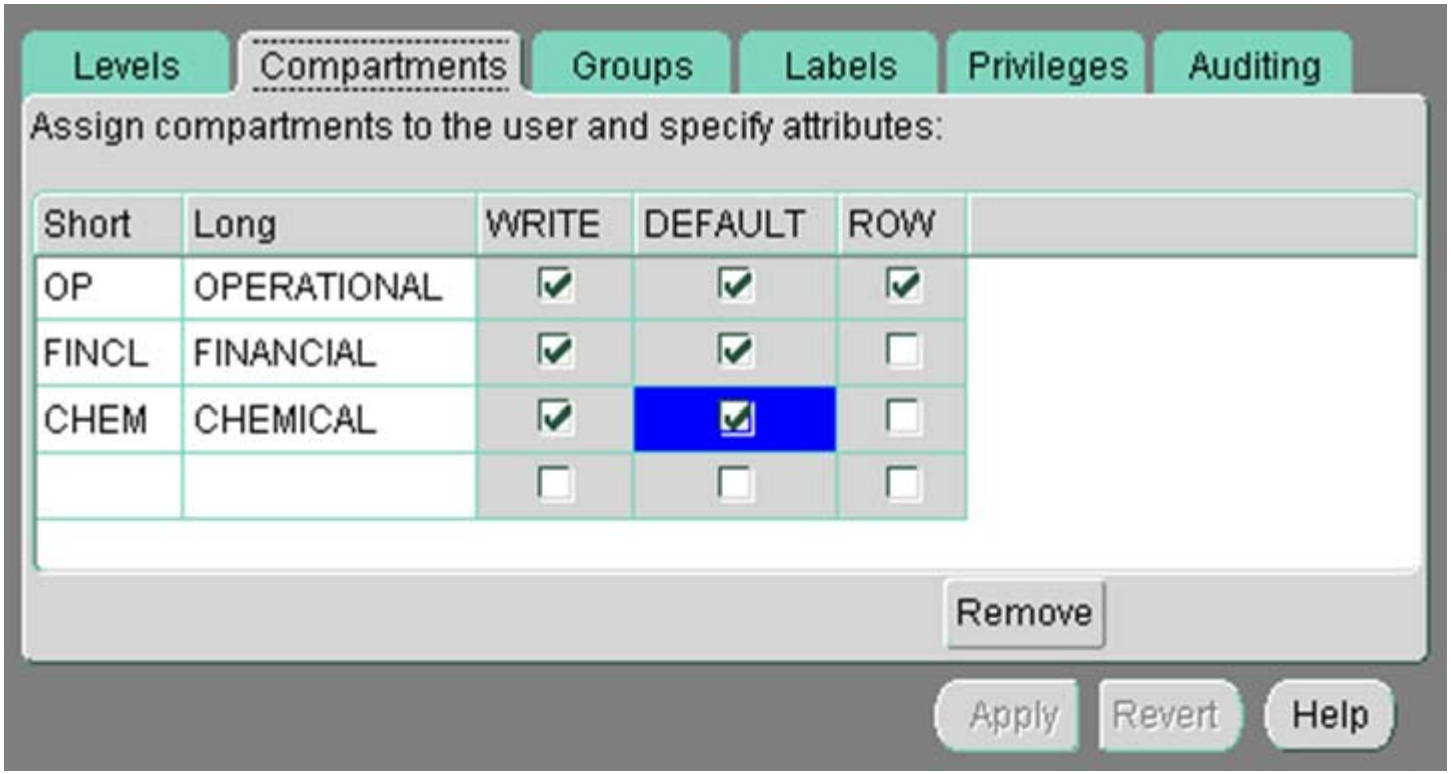
User Labels and level authorizations



User Default Level: The level that is assumed by default when connecting to Oracle

User Default Row Level: The level that is used by default when inserting data into Oracle

User Labels and compartments



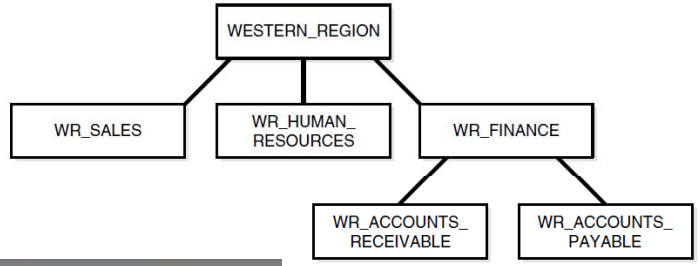
The administrator specifies the list of compartments that a user can place in her session label.

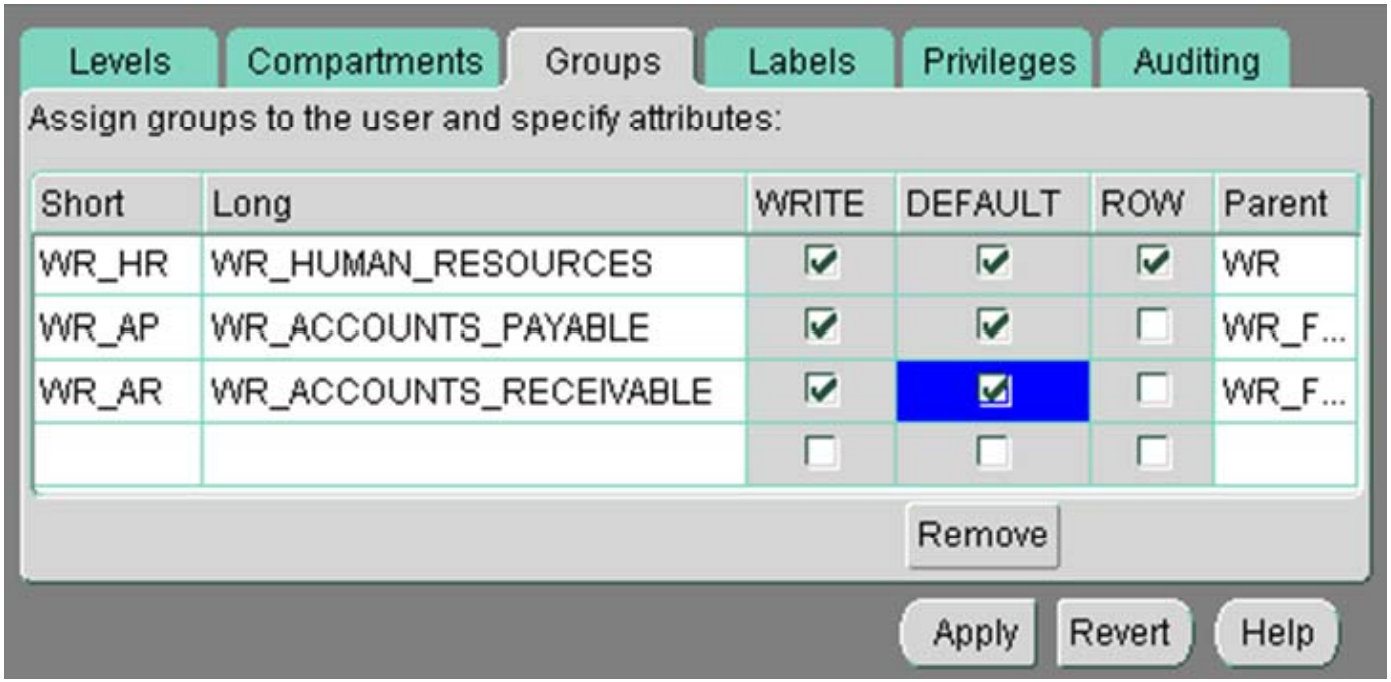
Write access must be explicitly given for each compartment

The Row designation indicates whether the compartment should be used as part of the default row label for newly inserted data.

A user cannot directly insert, update, or delete a row that contains a compartment that she does not have authorization to write.

User Labels and authorized groups





The administrator specifies the list of groups that a user can place in her session label.

Write access must be explicitly given for each group listed.

Row designation indicates whether the group should be used as part of the default row label for newly inserted data.

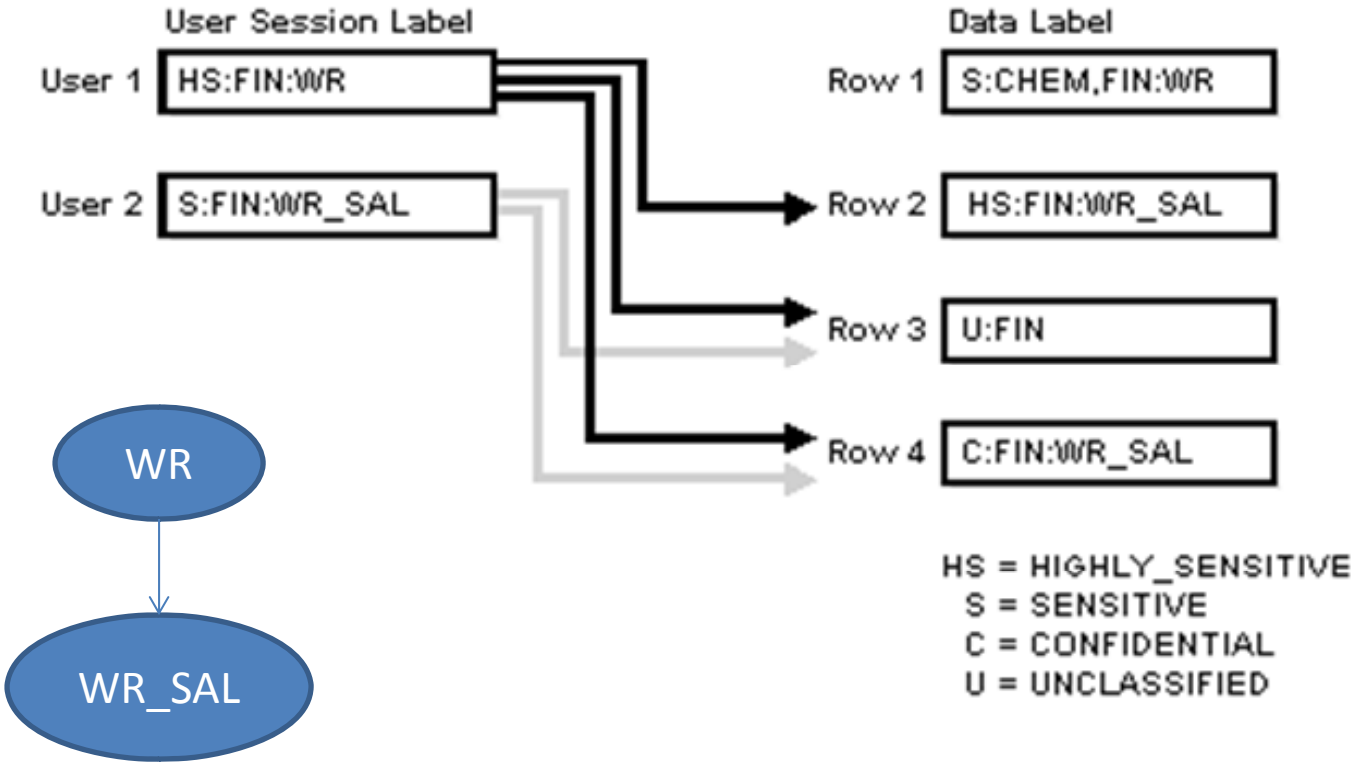
Session Labels

- The *session label is the particular combination of level, compartments, and groups at which a user works at* any given time.
- The user can change the session label to any combination of components for which he is authorized.
- When a user writes data without specifying its label, a *row label is assigned automatically, using the user's* session label.

How Data Labels and User Labels Work Together

- Each Oracle Label Security user can only access data within the range of his or her own label authorizations.
- Each user has:
  - Maximum and minimum levels
  - A set of authorized compartments
  - A set of authorized groups (and, implicitly, authorization for any subgroups)
  - For each compartment and group, a specification of read-only access, or read/write access
- Example:
  - if a user is assigned a maximum level of Highly Confidential, then the user potentially has access to Highly Confidential, and Confidential data. The user has no access to Sensitive data.

How Data Labels and User Labels Work Together



Policy Privileges

- The policy privileges enable a user or a stored program unit to bypass some aspects of the label-based access control policy
- The administrator can also authorize the user or program unit to perform specific actions, such as the ability of one user to assume the authorizations of a different user
- Privileges can be granted to program units, authorizing the procedure, rather than the user, to perform privileged operations

Privileges in Oracle Label Security Policies

- Oracle Label Security supports special privileges that allow authorized users to *bypass certain parts of the policy.*

Security Privilege	Explanation
READ	Allows read access to all data protected by the policy
FULL	Allows full read and write access to all data protected by the policy
COMPACCESS	Allows a session access to data authorized by the row's compartments, independent of the row's groups
PROFILE_ACCESS	Allows a session to change its labels and privileges to those of a different user
WRITEUP	Allows users to set or raise only the level, within a row label, up to the maximum level authorized for the user. (Active only if LABEL_UPDATE is active.)
WRITEDOWN	Allows users to set or lower the level, within a row label, to any level equal to or greater than the minimum level authorized for the user. (Active only if LABEL_UPDATE is active.)
WRITEACROSS	Allows a user to set or change groups and compartments of a row label, but does not allow changes to the level. (Active only if LABEL_UPDATE is active.)

Privileges in Oracle Label Security Policies

- READ
  - A user with READ privilege can read all data protected by the policy, regardless of his authorizations or session label. The user does not even need to have label authorizations.
  - A user with READ privilege can *write to any data rows for which* he or she has write access, based on any label authorizations.
  - The READ privilege enables optimal performance on SELECTs, since the system behaves as though the Oracle Label Security policy were not even present.
  - Useful
    - for system administrators who need to export data, but who should not be allowed to change data.
    - for people who must run reports and compile information, but not change data.

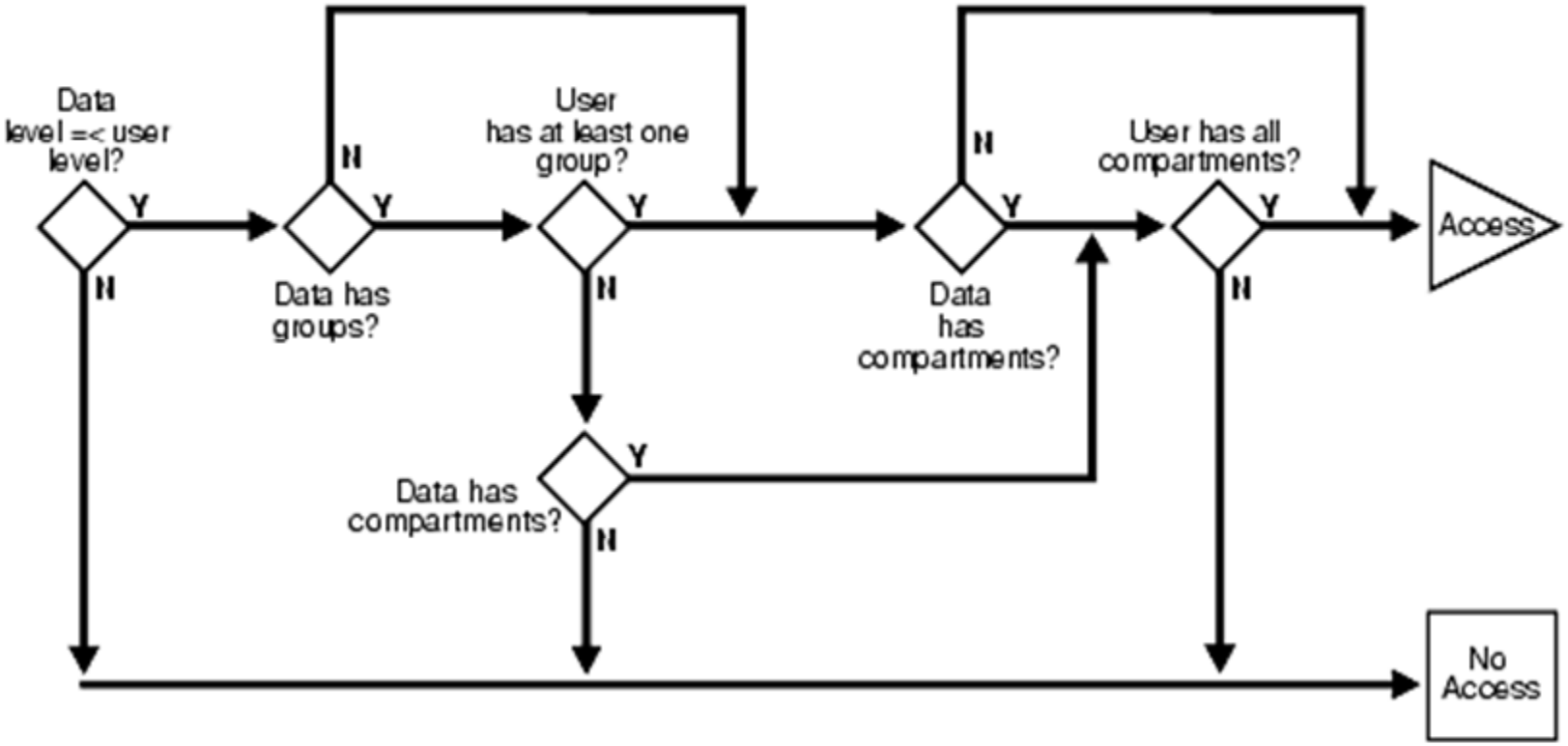
- FULL
  - The FULL privilege has the same effect and benefits as the READ privilege, with one difference: a user with FULL privilege can also *write to all the data.*

Privileges in Oracle Label Security Policies

COMPACCESS

- The COMPACCESS privilege allows a user to access data based on the row label's compartments, independent of the row label's groups.
- If a row label has no compartments, then access is determined by the group authorizations. However, when compartments do exist, and access to them is authorized, then the group authorization is bypassed.
- This allows a privileged user whose label matches all the compartments of the data to access any data in any particular compartment, independent of what groups may own or otherwise be allowed access to the data.

Label Evaluation Process for Read Access with COMPACCESS Privilege



Privileges in Oracle Label Security Policies

PROFILE_ACCESS

- The PROFILE_ACCESS privilege allows a session to change its session labels and session privileges to those of a different user.
- This is a very powerful privilege, since the user can potentially become a user with FULL privileges.
- This privilege cannot be granted to a trusted stored program unit.

Special Row Label Privileges

- Once the label on a row has been set, Oracle Label Security privileges are required to modify the label.
- These privileges include WRITEUP, WRITEDOWN, and WRITEACROSS.

Special Row Label Privileges

- WRITEUP
  - The WRITEUP privilege enables the user to raise the level of data within a row, without compromising the compartments or groups.
  - The user can raise the level up to his or her maximum authorized level.
    - For example, an authorized user can raise the level of a data row that has a level lower than his own minimum level. If a row is UNCLASSIFIED and the user's maximum level is SENSITIVE, he can raise the row's level to SENSITIVE.
  - He can raise the level above his current session level, but cannot change the compartments.

Special Row Label Privileges

- WRITEDOWN
  - The WRITEDOWN privilege enables the user to lower the level of data within a row, without changing the compartments or groups. The user can lower the level to any level equal to or greater than his or her minimum authorized level.
- WRITEACROSS
  - The WRITEACROSS privilege allows the user to change the compartments and groups of data, without altering its sensitivity level.

Documentation

- **Oracle® Label Security** Administrator's Guide
- 11*g Release 2 (11.2)* **E10745-02**
  - http://docs.oracle.com/cd/E11882_01/network.112/e10745.pdf