Oracle® Financial Data Manager

Administration Guide

Release 4.5

July 2000
Part No. A82944-01

ORACLE®

Oracle Financial Data Manager Administration Guide, Release 4.5

Part No. A82944-01

Contents

3 Managing Security

4 Managing Objects

5 Migrated Data

Glossary

Index

Send Us Your Comments

Oracle Financial Data Manager Administration Guide, Release 4.5

Part No. A82944-01

Oracle Corporation welcomes your comments and suggestions on the quality and usefulness of this document. Your input is an important part of the information used for revision.

- Did you find any errors?
- Is the information clearly presented?
- Do you need more information? If so, where?
- Are the examples correct? Do you need more examples?
- What features did you like most?

If you find any errors or have any other suggestions for improvement, please indicate the document title and part number, and the chapter, section, and page number (if available). You can send comments to us in the following ways:

- Electronic mail - fsdocmail@us.oracle.com
- FAX - (650) 506-7200   Attn: Oracle Financials Documentation Manager
- Postal service:
  Oracle Corporation
  Oracle Financials Documentation Manager
  500 Oracle Parkway
  Redwood Shores, CA 94065
  USA

If you would like a reply, please give your name, address, telephone number, and (optionally) electronic mail address.

If you have problems with the software, please contact your local Oracle Support Services.

Preface

This reference guide describes the features of Oracle Financial Data Manager (FDM) Administration. This preface describes the following information about the reference guide:

- Intended Audience

- Organization

- Report-Related Changes

- Related Documents

- Conventions

- Customer Support Information

Intended Audience

This manual is written for anyone who is responsible for database system administration. You should be familiar with relational database concepts, relational database management systems (RDBMSs), the operating system running Oracle, and the Oracle Financial Services applications used at your location. This manual assumes that FDM Administration is already installed.

Organization

This manual is organized into the following chapters:

Chapter 1	"Introduction" describes the new features in Release 4.5, overviews the Oracle Financial Services applications, and provides a tour of FDM Administration components.
Chapter 2	"Managing Users" describes the workflows to manage users, user groups, and privileges.
Chapter 3	"Managing Security" describes database and application security, including roles, security profiles, ID folders, and object privilege categories.
Chapter 4	"Managing Objects" discusses the steps required to use objects in the FDM environment.
Chapter 5	"Migrated Data" describes the workflow for migrated data.

A glossary and index are also included.

Report-Related Changes

Oracle Discoverer is the recommended reporting tool for OFSA Release 4.5. Discoverer is fully integrated with the following OFS applications:

- Oracle Financial Data Manager Administration

- Oracle Financial Data Manager Balance & Control

- Oracle Performance Analyzer

- Oracle Risk Manager

- Oracle Transfer Pricing

This release supports both Oracle Discoverer and the reporting tool used in prior OFSA releases. You can find information about both reporting tools in the following documents:

Reporting Tool	Documentation
Oracle Discoverer	Oracle Discoverer User Guide
	Oracle Discoverer Administrator Guide
OFSA reporting tool	Oracle Portfolio Analyzer Reference Guide

The following report-related chapters and appendixes have been removed from OFSA reference guides and moved to the *Oracle Portfolio Analyzer Reference Guide*:

- Report ID
- Report Macros
- Report Runner Dialog
- Report Stratification ID
- Standard Reports
- Subtotal ID

Related Documents

For more information, see the following manuals:

- *Oracle Financial Services Installation and Configuration Guide*
- *Oracle Financial Data Manager Data Dictionary*
- *Oracle Financial Data Manager Reporting Administration Guide*

Conventions

This reference guide uses the following conventions:

Convention	Meaning
. . .	Vertical ellipsis points in an example mean that information not directly related to the example has been omitted.
. . .	Horizontal ellipsis points in statements or commands mean that parts of the statement or command not directly related to the example have been omitted.
boldface text	Boldface type in text indicates a term defined in the text, the glossary, or in both locations.
`bold monospace`	Bold monospace type in text indicates information that you type in.
Italics	Italics emphasize a word or phrase.
< >	Angle brackets enclose user-supplied names (for example, <Branch Name>).

Convention	Meaning
[ ]	Brackets enclose function and terminal keys. In common syntax, brackets denote one or more optional items.
{ }	Braces are used to denote variables, and in command syntax, a choice within a mandatory item.
	Example of command syntax:
	Warning: INIT file {filename} already exists.
	Example of choices:
	{EXIT	QUIT}
->	This arrow indicates a menu path.

Symbols

- Bullets indicate a list of items or topics.

1. Numbered lists are used for sequential steps in completing a procedure.

Orientation of Procedures

Procedures in OFS reference guides are generally menu-driven rather than command- or icon-driven. If you prefer to use the toolbar icons, refer to Chapter 1, "Introduction."

Notes, Cautions, and Warnings

Certain information may be set off in boxes for purposes of emphasis:

- *Note* refers to important information about the product.

- *Caution* indicates the possibility of damage to a product, system, or data.

- *Warning* refers to a situation that is potentially hazardous to people.

Customer Support Information

Product support is available through Oracle Support Services. Contact your project manager for information about using the support options offered in your geographic region. These options may include the following:

- MetaLink (which provides online access to information about Technical Libraries, Patches, TARs, and Bugs and is available at metalink.oracle.com)

- Telephone support

1

Introduction

Oracle Financial Data Manager (FDM) Administration is a database and security administration tool for the Oracle Financial Services (OFS) applications—part of the Oracle data warehouse for the financial services industry. With FDM Administration, you grant database, application, and function privileges to the users of OFS applications. As a component of Oracle Financial Data Manager, FDM Administration is based on an enhanced data model so that you can work within an integrated data environment.

This chapter describes:

- New Features in Release 4.5
- A Quick Tour of FDM Administration
- Seeded Data
- Schemas
- Registration
- Upgrading to Release 4.5

New Features in Release 4.5

FDM Administration offers new features for user, security, and object management:

In Release 4.5 of FDM Administration, you can	For more information, see
Register users for use in the FDM environment	"Registration" in this chapter
Create user groups based on application access needs	"FDM Administration Workflow" in Chapter 2
Use seeded user groups to reduce administrative tasks	"Seeded Data" in this chapter

In Release 4.5 of FDM Administration, you can	For more information, see
Designate ad hoc sets of privileges for users	"Workflow for Granting Ad Hoc User Group Privileges" in Chapter 2
Use seeded roles to simplify database security	"Seeded Data" in this chapter
Use security profiles to assign collections of privileges to user groups	"Seeded Data" in this chapter
Grant privileges for a function (an application task)	"Application and Function Privileges" in Chapter 3
Distinguish between internal and external privileges	"Roles—Internal and External" in Chapter 3
Register tables in the FDM environment	Chapter 4, "Managing Objects"

FDM Administration also supports universal database login; that is, users can log in to the database from any Oracle-compatible tool (SQL*Plus, Enterprise Manager, Discoverer Integrator) or from a SQL script with the same user name and password.

Oracle Financial Services Applications

Your data environment includes one or more of the OFS applications, which provide comprehensive decision-support solutions for budgeting and planning, performance measurement, risk management, and transfer pricing functions. Using FDM Administration, you grant database, application, and function privileges to the users of OFS applications.
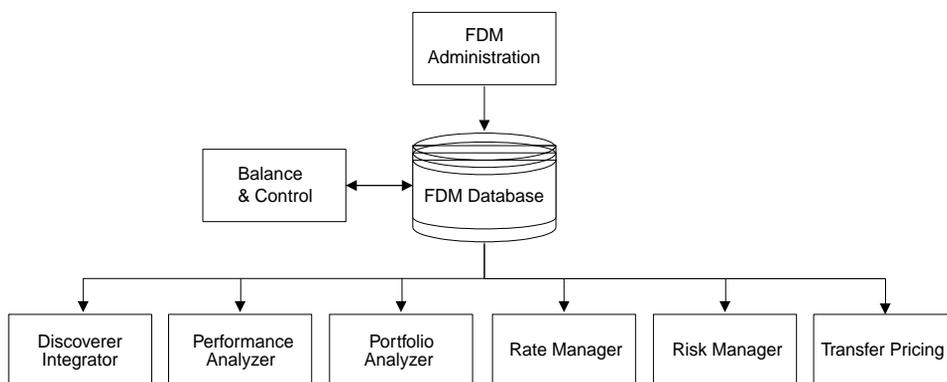
Oracle Financial Data Manager Balance & Control   Balance & Control validates, corrects, and aggregates data from the FDM database.

Oracle Financial Data Manager/Discoverer Integrator   Discoverer Integrator integrates the FDM database with Oracle Discoverer, which provides ad hoc reporting, analysis, and web publishing capabilities.

Oracle Performance Analyzer   Performance Analyzer provides comprehensive and flexible cost and equity allocations. It measures product, business unit, and customer profitability.

Oracle Portfolio Analyzer   Portfolio Analyzer assesses profit structure by analyzing product portfolios, customer data, and market segments.

Oracle Rate Manager   Rate Manager manages interest rate and exchange rate information, improving on and replacing the Historical Rates ID.

Oracle Risk Manager   Risk Manager forecasts cash flows, interest income, and market value to manage rate risk.

Oracle Transfer Pricing   Transfer Pricing calculates a transfer rate for each account and a charge or credit for funds for each asset or liability.

A Quick Tour of FDM Administration

To log in to FDM Administration, you need a user name, password, and the name of the database you are accessing. As the FDM administrator, you will log in with either the FDM schema user name and password or with a user name and password that grants you FDM administrator privileges. Use the same user name and password when you log in to SQL*Plus or Enterprise Manager.

After logging in, you will see a window divided into:

- The metadata pane—the navigation tree that lists the metadata (data about data) that you manage

- The data management pane—tab pages where you query on and maintain data, add and remove recipients and privileges, and assign security

Metadata: The Navigation Tree

FDM Administration metadata includes data about table classifications, object regis-
tration, data structures, display names, and column properties. Double-click items
on the navigation tree.
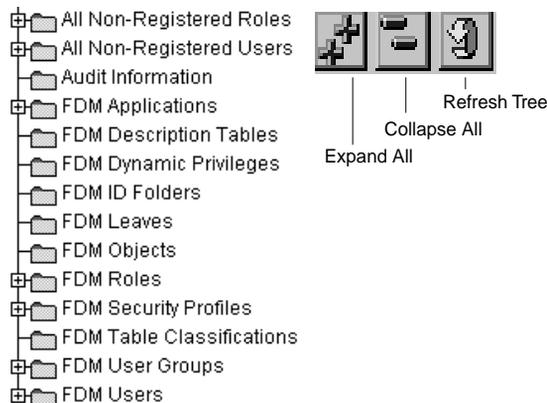
The Expand All and Collapse All buttons apply to + and - on the navigation tree.
Click Refresh Tree to see the most up-to-date view of the metadata. Brief descrip-
tions of the metadata follow:

All Nonregistered Roles	Nonregistered roles exist in the database but have not been identified for use in the FDM environment.
All Nonregistered Users	Nonregistered users exist in the database but have not been identified for use in the FDM environment.
Audit Information	Audit information displays the logged results from running an FDM Administration stored procedure. When the procedure is executed, the audit information is logged in the OFSA_STP table. The tab page displays the SQL command executed by the procedure and a return code indicating success or failure.
FDM Applications	See "Oracle Financial Services Applications" in this chapter for the applications managed with FDM Administration. **Note:** Oracle Customer Householding and Oracle Market Manager are not managed with FDM Administration.

FDM Description Tables	Description tables contain code descriptions—mappings between the code columns and alphanumeric descriptions that are used for display names and reporting. See Chapter 4, "Managing Objects".
FDM Dynamic Privileges	Use dynamic object privileges to predesignate access to a database object, such as a results table, that is created during processing.
FDM ID Folders	ID folders are logical groupings of IDs, stored in the database and used to manage privileges. (IDs are processing instructions and assumptions used for financial analysis in the OFS applications.)
FDM Leaves	Leaves are columns that provide dimensionality for instrument and account data tables. Leaf columns provide a means for categorizing data for these tables.
FDM Objects	Objects are tables or views that have been registered in the FDM environment.
FDM Roles	A role is a set of database and system privileges, often associated with a specific application, to which user groups are assigned.
FDM Security Profiles	A security profile is a group of privileges for access to tables, functions, and ID folders, assigned to user groups or users.
FDM Table Classifications	Table classifications ensure that an object needed to run one of the OFS applications has the required characteristics. See "Step Three: Classifying an Object" in Chapter 4.
FDM User Groups	A user group is a collection of users who use the same set of features in an application.
FDM Users	An FDM user is registered to use one or more of the OFS applications.

Data Management: The Tab Pages

The tab pages are where you manage security and objects. Double-click an item in the navigation tree to produce the associated tab pages. Some tab pages, such as the Role Recipients tab, provide query capability and add and remove functions.

For example, the Role Recipients tab shows that the user group G_TP_VIEWONLY is the recipient of two roles, OFDM_R_REPORT_MART and OFDM_R_TP. In other words, the two roles are assigned to the user group. If you want to unassign one of the roles from G_TP_VIEWONLY, select the role (by checking the box) and click Remove Recipient. This removes the role from the user group. That is, the user group is no longer the recipient of the removed role. (The role itself is not removed or deleted from the database.)
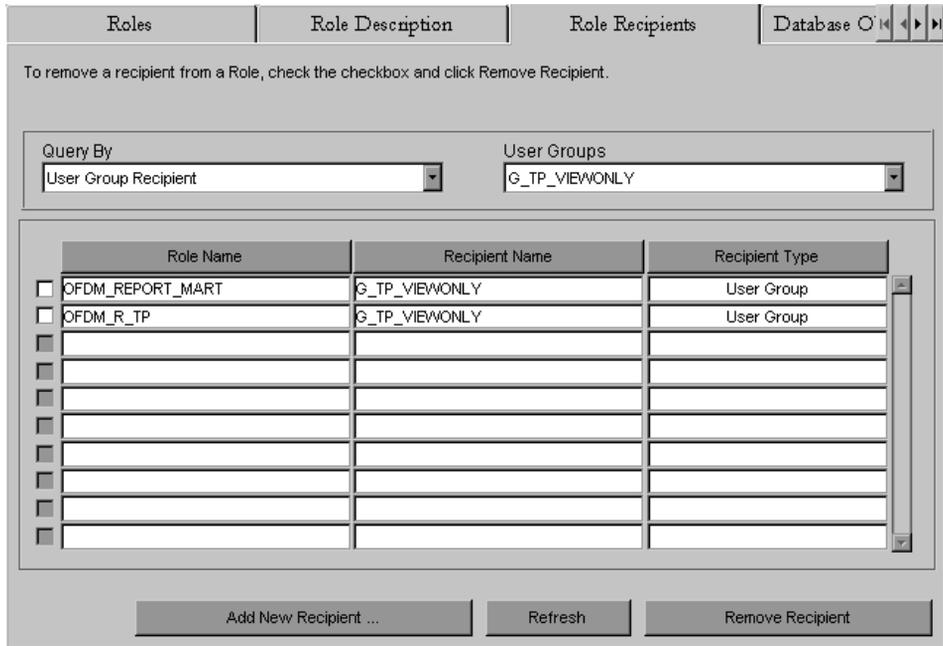
Other functions, such as on the Roles tab, let you delete references from the FDM metadata (Unregister), query the database (Refresh), or update passwords (Password). The Apply button saves changes to the database.

Other features on the tab pages let you:

- Click a column title to sort the column alphabetically.

- Double-click a description to see the full text.

- Click a description and press CNTL-E to edit the text. (After exiting the editor, click Apply to save the change to the database.)

Menus and Toolbars

FDM Administration provides the following menus and menu items. An asterisk indicates that the function is also available from the vertical toolbar.

Menu	Menu Item	Description
File	Exit	Exits the program.
Wizards	Create* Register* Security	Walks you through the steps to create ID folders, roles, security profiles, users, and user groups; to register leaves, objects, roles and users; and to assign security. See "Wizards" in this chapter.

Menu	Menu Item	Description
Tools	Discoverer Admin* Discoverer User* Discoverer Integrator* Enterprise Manager* SQL*Plus	Starts tools installed on your PC to run simultaneously with FDM Administration.
Maintenance	Column Property Assignment Code Description Mappings Table Classification Assignment Database Privileges Database Objects	See Chapter 4. The Database Privileges -> Grant functions ensure that creation, registration, and assignments are valid in the database. Database Objects -> Analyze All Objects performs the Oracle RDBMS command to analyze table estimate statistics for all FDM-registered tables. Database Objects -> Create Public Synonyms creates public synonyms in the instance for all FDM-registered objects.
Window	Arranges multiple windows; displays a numbered list of open windows from which you can select and activate one.	
Help	Contains all the information in this reference guide, plus the Display Errors feature. When you encounter an Oracle database error, select Display Errors to identify the statement in which the error occurred.	

The Shortcut Menu

A shortcut menu is available for the Create, Register, and Security wizards. Position the pointer over the navigation tree and click the right mouse button.

Wizards

When you need to add ID folders, roles, security profiles, and user groups other than those provided in the seeded data, or when you add new users or make security assignments, wizards are available from the Wizards menu. Wizards are also available for registering leaves, objects, roles, and users, and for reregistering an object. A wizard includes a series of windows to step through the process, with instructions at the top of the window and Next, Back, and Finish buttons as appropriate. Required input labels appear in red on your monitor.

The wizard windows guide you in selecting from lists of query types, entities, and recipients. In the User Group Assignment window, for example, Query Type lists user group assignments to applications, functions, roles, users, and so on. The entity, that is, what you are assigning to, is the user group. The recipients are names of applications. Click an available recipient and click Add to move it to Current and New Recipients Names. If you want to remove a user name from Current and New Recipient Names (before clicking Apply), click Refresh Lists and start the add process again. The Apply button saves your assignments to the database.
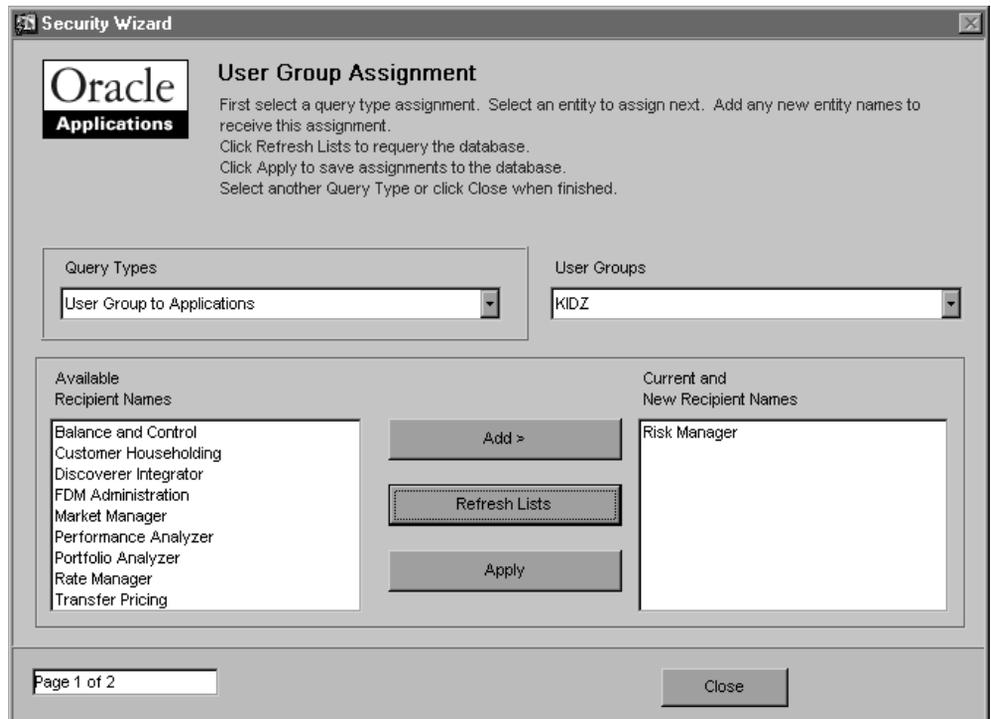
You may need to use more than one wizard to complete a task; for example, after creating a user you will probably register the user using another wizard. Check Run the Registration wizard after this wizard to proceed directly to the next wizard.

Some Wizards feature a checkbox that lets you base a new role or security profile on an existing one. Like a Save As function, it copies the properties of the existing role or security profile, which you can later modify to fit the needs of the users.

Registration Wizard

Role Registration

Oracle Financial Services applications

This wizard allows you to register a role from the database for use with FDM. Enter data for all required fields indicated in red.

Passwords must not contain numbers or special characters and must be at least 6 characters long. Spaces will be converted to underscores.

Click Next to continue.

☑ Base Privileges on Existing Role

Available Roles

OFDM_R_RM

Role Name   Description

Creation Wizard

Security Profile Creation

Oracle Financial Services applications

This wizard allows you to create a Security Profile.
Enter data for all required fields indicated in red.
Click Next to continue.

Security Profile Creator   Creation Date

DKBRADSH   20-APR-00

☑ Base Privileges on Existing Security Profile

Available Security Profiles

OFDM_S_RM

Security Profile Name

Description

Seeded Data

Seeded (predefined) data is supplied with FDM Administration. For each OFS application, a seeded user group, seeded role, and seeded security profile are provided. The privileges associated with the seeded entities cannot be modified.

You should assign the seeded entities to a user who needs access to all the functions and tasks of an application. When you need to restrict user access, create a new security profile with fewer privileges.

Using seeded data whenever possible is strongly recommended because it reduces the time you spend assigning privileges and provides tighter security. Seeded data is named according to the following conventions, where XX is an OFS application, such as Risk Manager (shown as RM in the navigation tree):

- OFDM_G_XX for seeded user groups

- OFDM_R_XX and OFDM_R_XX_RPT for seeded roles

- OFDM_S_XX for seeded security profiles

A seeded user group is provided for each OFS application. For example, OFDM_G_ BC is the user group associated with Balance & Control. Assign a user to OFDM_G_ BC to provide full access to Balance & Control, including required database privileges and all the Balance & Control tasks and functions. The user assigned to OFDM_G_BC is automatically assigned to the seeded role, OFDM_R_BC and the seeded security profile, OFDM_S_BC, for Balance & Control. A user automatically gets role, security profile, and ID folder privileges through membership in a seeded user group.

A seeded role provides database system privileges on FDM reserved objects for a specific application. For example, OFDM_R_BC is the seeded role associated with Balance & Control. It grants full access to all Balance & Control tables. A user group assigned to OFDM_R_BC inherits this access. OFDM_R_BC is an example of an internal seeded role. Whenever you create a user group, you will assign it to a seeded role to provide users access to a specific OFS application. External seeded roles (for example, OFDM_R_REPORT_MART and OFDM_R_XX_RPT) provide Select privileges for FDM reserved objects required for reporting. Assign external seeded roles to user groups so that users can report and view results. See "Roles—Internal and External" in Chapter 3, "Managing Security" for more information.

A seeded security profile provides full access to an application and all its tasks and functions. For example, OFDM_S_BC is the seeded security profile associated with

Balance & Control. Assign OFDM_S_BC to a user group requiring full access to Balance & Control. Note that a security profile does not provide database privileges.

See "FDM Administration Workflow" in Chapter 2 for more on how to use seeded data.

Schemas

A schema is a named collection of objects, such as tables, views, clusters, functions, procedures, and packages, associated with a particular user. When you create a user in FDM Administration, an eponymous schema is created for the user. For example, for user MARY_SMITH, the schema named MARY_SMITH is created.

The FDM schema, a user name and password combination, owns the FDM metadata and reserved objects. The FDM schema has all privileges associated with managing security and objects, and designates one or both of these functions to system administrators.

Registration

Registering a leaf, object, role, or user makes it available for use within the FDM environment. Registration wizards (see "Wizards" in this chapter) are available to guide you. For table registration, for example, you use the Object Registration wizard. When you select a table name from the Object Registration window, the column names from the Oracle 8i catalog are displayed. You provide required information for each column, such as the FDM data types and display names, which is saved in an FDM catalog. See Chapter 4 for more information about object registration.

Registering a user populates the FDM metadata with information about the user. When you register a user, a seeded login role is assigned to validate user login to an OFS application. Use the Registration wizards to register leaves, objects, roles, and users.

Unregistering users, user groups, security profiles, roles, ID folders, and objects deletes all references to those entities in the FDM metadata; however, users, roles, and objects still exist in the Oracle 8i catalog. In general you cannot unregister seeded user groups, seeded security profiles, and seeded roles, but see the *Oracle Financial Services Installation and Configuration Guide* for exceptions.

Upgrading to Release 4.5

If you have upgraded to Release 4.5 of FDM Administration and your databases were migrated, you will see both the seeded data and your own data. Migrated users have the same privileges in Release 4.5 that they had in the previous installation. Specifically, users have:

- The same privileges as they previously had as members of a group

- The same database privileges to access user data tables

In Release 4.5, you grant privileges rather than assign restrictions. Therefore, while users have the same privileges as they previously had, you will need to reorganize the privileges, starting with creating new user groups and security profiles. See Chapter 5, "Migrated Data" for details.

2

Managing Users

You should manage user security by assigning users to user groups. A user group is a collection of users who use the same set of features in an application. You typically assign privileges—ID folders, roles, and security profiles—to user groups rather than individual users. This simplifies user-to-assignment tracking and works in conjunction with the seeded (predefined) data provided with FDM Administration.

This chapter describes the FDM Administration workflow in addition to user and user group management. Topics include:

- FDM Administration Workflow

- Creating Users

- Unregistering Users

- Using Seeded User Groups

- Managing Privileges to Users and User Groups

FDM Administration Workflow

This workflow discussion describes how you set up and manage privileges using the seeded data and wizards. It assumes a typical situation in which you want to grant both user data table privileges and provide database access—access to the reserved objects—to run specific OFS applications. This discussion assumes a new installation of FDM Administration. For the workflow for migrated data, see "Workflow for Migrated Data" in Chapter 5.

Workflow for Granting User Data Table Privileges

```
┌─────────────────────────────────┐
│         Create Roles            │
│      *   External               │
│      *   Internal               │
└─────────────────────────────────┘
                 │
                 ▼
┌─────────────────────────────────┐
│         Register Roles          │
└─────────────────────────────────┘
                 │
                 ▼
┌─────────────────────────────────────────┐
│ Assign Database Object Privileges to Roles│
└─────────────────────────────────────────┘
                 │
                 ▼
┌─────────────────────────────────────────┐
│        Assign Roles to User Group        │
└─────────────────────────────────────────┘
```
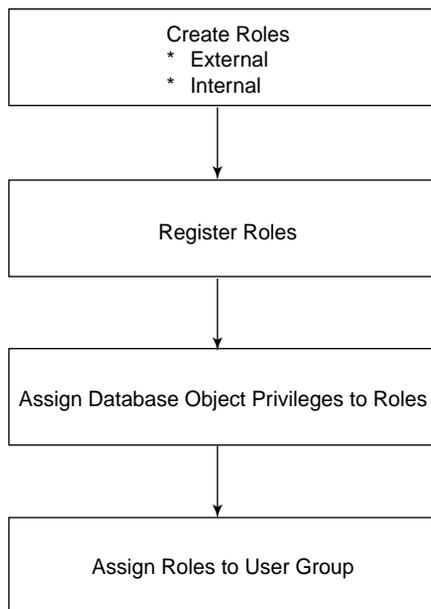
Create Roles Start with the Create Role wizard and create two new roles to manage privileges for user data tables. For example, create two roles to grant a Performance Analyzer user the following:

- Select privilege on user data tables to run Discoverer reports—an external role

- Select, insert, update, and delete privileges for accessing user data tables when running Performance Analyzer—an internal role

Generate the SQL to create the new roles in the database.

Register Roles Using the Role Registration wizard, register the new roles in the FDM metadata. Following the example of the Performance Analyzer user, register one role as an external role and the other as an internal role. The internal role requires a password.

Assign Database Object Privileges to Roles Using the Role Assignment wizard, select the query type—Role to Database Object Privileges. In the Database Object Privilege Assignment window, select the new role, for example, the external role, and choose a table classification (to filter out unneeded tables). For the Performance

Analyzer user, you might select Instrument Profitability. Then check the Select boxes for the needed tables. After you click Apply, repeat the process for the new internal role. Select the internal role, choose a table classification, (for the Performance Analyzer user this will be Instrument Profitability), check the boxes (Select, Insert, Update, and Delete) for the needed tables, and click Apply.

Assign Roles to User Group In the Database Object Privilege Assignment window, select the Role to User Groups query. Select the new external role and assign it to OFDM_G_PA, following the example of the Performance Analyzer user. Do the same for the internal role.

Procedure for Granting User Data Table Privileges

The following steps describe the workflow for granting user data table privileges. The steps describe the entire workflow for the external role. For the internal role, repeat the procedure using the changes shown in "Note."

Creating the Role

1. From the Wizards menu, select Create -> Role.

2. Type the role name.

3. Click Generate SQL.

4. Edit the SQL code if needed and click Next.

5. Check Run the Registration Wizard after This Wizard.

6. Click Finish.

Registering the External Role

After creating the role, you should be in the Role Registration window.

1. From Role Name, select the role name you typed in step 2 of "Creating the Role".

2. Click External and type a description.

3. Click Next.

4. Check Run the Security Assignment Wizard after This Wizard.

5. Click Finish.

> **Note:** For the internal role, change step 2 as follows: Click Internal, type a description, and type a password between 6 and 30 characters.

Assigning Database Object Privileges to the Role

After registering the role, you should be in the Role Assignment window.

1. From Query Type, select Role to Database Object Privileges.

2. From Roles, select the role name you typed in step 2 of "Creating the Role".

3. From Filter by Table Classification, select a classification.

4. Check Select, Insert, Update, or Delete for the objects you want to assign.

5. Click Apply.

Assigning the Role to a User Group

After assigning database object privileges, you should be in the Database Object Privilege Assignment window.

1. From Query Type, select Role to User Groups.

2. From Roles, select the role name you typed in step 2 of "Creating the Role".

3. From Available Recipient Names, click the user group you want to assign and click Add.

4. Repeat step 3 until you have completed the assignments.

5. Click Apply.

6. Click Close.

To summarize, after creating all the external and internal roles needed for access to user data tables, you are ready to provide database access—access to the reserved tables—to run specific OFS applications. You do this by granting the privileges you previously set up (following the example of the Performance Analyzer user, Instrument Profitability table privileges). Thus the next workflow is to create and assign users to seeded user groups.

Workflow for Database Access for OFS Applications (User Registration)

```
┌─────────────────────────────────────┐
│                                     │
│            Create User              │
│                                     │
└─────────────────────────────────────┘
                   │
                   ▼
┌─────────────────────────────────────┐
│                                     │
│           Register User             │
│                                     │
└─────────────────────────────────────┘
                   │
                   ▼
┌─────────────────────────────────────┐
│                                     │
│      Assign User to User Group      │
│                                     │
└─────────────────────────────────────┘
```
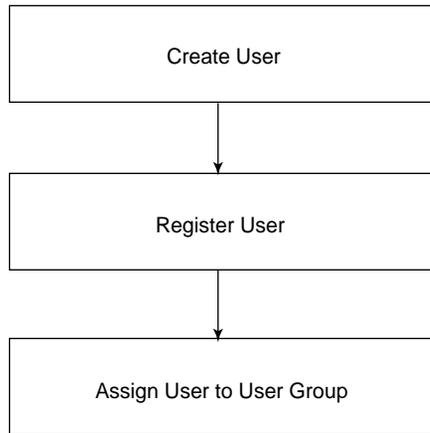
Create User Using the Create User wizard (see "Creating Users" in this chapter), supply the required information and generate the SQL code to create the new user in the database. Check the box to run the Registration wizard and click Finish.

Register User In the User Registration window, supply the required information (labeled in red on your monitor) and click Next.

Assign User to User Group In the Recipient to User Group Assignment window, assign the new user (labeled Recipient Name) to any number of user groups by checking the boxes. For the Performance Analyzer user, check OFDM_G_PA. The Performance Analyzer user is now assigned to the following:

- OFDM_S_PA (the seeded security profile for users assigned to the Performance Analyzer seeded user group)

- OFDM_R_PA (the seeded role for Performance Analyzer)

- An external role (select privilege to run Discoverer reports)

- An internal role (for accessing user data tables to run Performance Analyzer)

Now the Performance Analyzer user can run allocation processing and other Performance Analyzer activities.

Procedure for Database Access for OFS Applications (User Registration)

The following steps describe the user registration workflow to provide users with database access for the OFS applications.

Creating the User

1. From the Wizards menu, select Create -> User.

2. Type the user name and supply the required information.

3. Click Generate SQL.

4. Edit the SQL code if needed and click Next.

5. Check Run the Registration Wizard after This Wizard.

6. Click Finish.

Registering the User

After creating the user, you should be in the User Registration window.

1. From Username, select the user name you typed in step 2 of "Creating the User".

2. Type the first and last name of the user (optional) and click Next.

Assigning the User to a User Group

After registering the user, you should be in the Recipient to User Group Assignment window.

1. Check the name of each user group you want to assign.

2. Click Finish.

Workflow for Granting Ad Hoc User Group Privileges

When the privilege sets available through seeded data are insufficient for your users, you will create and register your own user groups. For example, the typical Risk Manager user will be assigned to the Risk Manager user group (which automatically assigns the Risk Manager seeded role and security profile to the user). If the user also needs to examine Transfer Pricing assumptions, but not change or run Transfer Pricing processes, the following workflow applies:

```
┌─────────────────────────────────────┐
│                                     │
│         Create User Group           │
│                                     │
└─────────────────────────────────────┘
                  │
                  ▼
┌─────────────────────────────────────┐
│                                     │
│      Assign User Group to User      │
│                                     │
└─────────────────────────────────────┘
                  │
                  ▼
┌─────────────────────────────────────┐
│                                     │
│   Assign User Group to Seeded Role  │
│                                     │
└─────────────────────────────────────┘
                  │
                  ▼
┌─────────────────────────────────────┐
│                                     │
│       Create Security Profile       │
│                                     │
└─────────────────────────────────────┘
                  │
                  ▼
┌─────────────────────────────────────┐
│                                     │
│  Assign Security Profile to Application │
│                                     │
└─────────────────────────────────────┘
                  │
                  ▼
┌─────────────────────────────────────┐
│                                     │
│   Assign Security Profile to Function │
│                                     │
└─────────────────────────────────────┘
                  │
                  ▼
┌─────────────────────────────────────┐
│                                     │
│  Assign Security Profile to User Group │
│                                     │
└─────────────────────────────────────┘
```
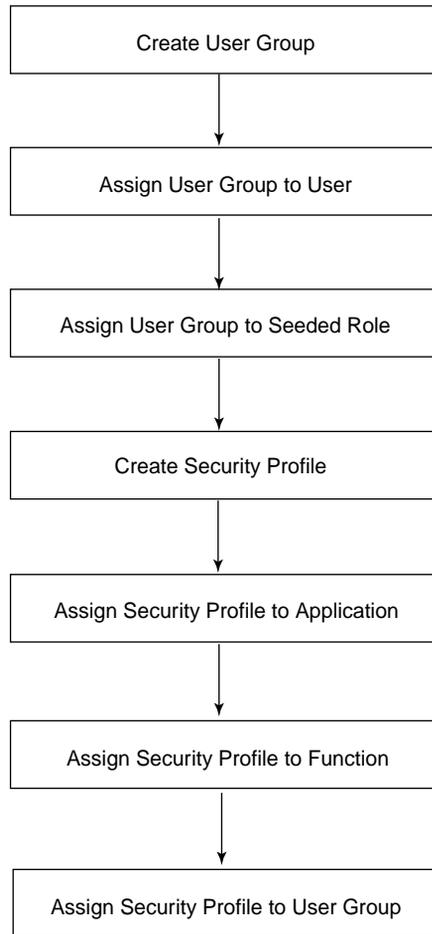
Create User Group Start with the Create User Group wizard to create a new user group, for example, G_TP_VIEWONLY. Check the box to run the Security Assignment wizard and click Finish.

Assign User Group to User   Using the User Group Assignment wizard, add the user as a recipient of G_TP_VIEWONLY and click Apply.

Assign User Group to Seeded Role   Remaining in the User Group Assignment window, select User Group to Roles and select G_TP_VIEWONLY. Add the Transfer

Pricing seeded role, OFDM_R_TP, and click Apply. This provides the user with access to the reserved tables for Transfer Pricing.

Create Security Profile Using the Security Profile Creation wizard, create a new security profile, in this example, S_TP_VIEWONLY. Click Next and check the box to run the Security Assignment wizard. Click Finish.

Assign Security Profile to Application Using the Security Profile Assignment wizard, select Security Profile to Applications and select S_TP_VIEWONLY. Add Transfer Pricing as a recipient. Click Apply.

Assign Security Profile to Function Remaining in the Security Profile Assignment window, select Security Profile to Functions. Select S_TP_VIEWONLY and Transfer Pricing. Sort by Action Name and check the boxes for the Transfer Pricing IDs with view privilege. For example, you might check the boxes for Transfer Pricing constructs and actions (functions) such as TP Process ID–View and Transfer Pricing ID–View. Click Apply.

Assign Security Profile to User Group Remaining in the Function Assignment window, from Query Type, select Security Profile to User Groups. Select S_TP_VIEWONLY and add G_TP_VIEWONLY as a recipient. Click Apply.

Procedure for Granting Ad Hoc User Group Privileges

The following steps describe the workflow for granting ad hoc user group privileges.

Creating the User Group

1. From the Wizards menu, select Create -> User Group.

2. Type the user group name and description.

3. Click Next.

4. Check Run the Security Assignment Wizard after This Wizard.

5. Click Finish.

Assigning the User Group to a User

After creating the user group, you should be in the User Group Assignment window.

1. From Query Type, select User Group to Users.

2. From User Groups, select the user group name you typed in step 2 of "Creating the User Group".

3. From Available Recipient Names, click a user name and click Add.

4. Repeat step 3 until you have completed the assignments.

5. Click Apply.

Assigning the User Group to a Seeded Role

After assigning the user group to a user, you should be in the User Group Assignment window.

1. From Query Type, select User Group to Roles.

2. From User Groups, select the user group you typed in step 2 of "Creating the User Group".

3. From Available Recipient Names, click a role and click Add.

4. Repeat step 3 until you have completed the assignments.

5. Click Apply.

6. Click Close.

Creating a Security Profile

1. From the Wizards menu, select Create -> Security Profile.

2. Type the security profile name and click Next.

3. Check Run the Security Assignment Wizard after This Wizard.

4. Click Finish.

Assigning the Security Profile to an Application

After creating the security profile, you should be in the Security Profile Assignment window.

1. From Query Type, select Security Profile to Applications.

2. From Security Profiles, select the security profile you typed in step 2 of "Creating a Security Profile".

3. From Available Recipient Names, click an application and click Add.

4. Repeat step 3 until you have completed the assignments.

5. Click Apply.

Assigning the Security Profile to a Function

After assigning the security profile to an application, you should be in the Security Profile Assignment window.

1. From Query Type, select Security Profile to Functions.

2. From Security Profiles, select the security profile you typed in step 2 of "Creating a Security Profile".

3. From Application Filter, select an application.

4. In Sort By, click Action Name.

5. Check the construct name and action combinations you want to assign.

6. Click Apply.

Assigning the Security Profile to a User Group

After assigning the security profile to a function, you should be in the Function Assignment window.

1. From Query Type, select Security Profile to User Groups.

2. From Security Profiles, select the security profile you typed in step 2 of "Creating a Security Profile".

3. From Available Recipient Names, click a user group and click Add.

4. Repeat step 3 until you have completed the assignments.

5. Click Apply.

6. Click Close.

Creating Users

For new installations of FDM Administration, you create users with the Create Users wizard. Instructions on the screen step through the procedure.

You can also create users using tools such as SQL*Plus or Enterprise Manager. No matter how you create a user, you must register the new user in FDM Administration. Registered users are listed in FDM Users. Click the Refresh button to query the database for the most up-to-date list.

Migrated users are also listed under FDM Users. Managing migrated users requires additional steps. You will need to remove privileges at the individual user level, create custom user groups and security profiles, and assign security profiles and users

to the new user groups. For details on how to do this, see "Workflow for Migrated Data" in Chapter 5.

Registering Users

Registering a user populates the FDM metadata with information about the user. FDM Administration *automatically* does the following when you register a user:

- Assigns the user to ALL, the ID folder in the OFSA_ID_FOLDER_ACCESS table

- Creates an eponymous ID folder for the user

- Assigns the user to OFDM_R_LOGIN, the seeded role that provides privileges needed for connectivity to an OFS application

- Creates a Configuration ID for the user, if one does not already exist in OFSA_ ID_CATALOG_OF_IDS

Unregistering Users

Unregistering a user deletes all references to the user in the FDM metadata; however, the user still exists in the Oracle8i catalog. All the IDs of an unregistered user are moved to the seeded ID folder DELETED_USERS and the eponymous ID folder of the user is deleted.

To unregister a user, do the following:

1. Expand the FDM Users folder and double-click the user name.

2. Click the General tab.

3. Click Unregister.

Using Seeded User Groups

For both new and upgraded installations of FDM Administration, you assign each user to one or more seeded (predefined) user groups. To do this, use the User Assignment wizard from the Wizards menu. A user assigned to a seeded user group inherits the privileges of the group and its associated role and security profile. See "Seeded Data" in Chapter 1, "Introduction" for more information. The following seeded user groups are provided:

User Group Name	Provides Privileges For
OFDM_G_ALL_APPS	All applications (except FDM Administration)

User Group Name	Provides Privileges For
OFDM _G_BC	Balance and Control
OFDM _G_DI	Discoverer Integrator
OFDM _G_FDMA_OBJ	FDM Administration object management
OFDM _G_FDMA_SEC	FDM Administration security management
OFDM _G_FDMA_USER	FDM Administration maintenance tasks (e.g., Grant All)
OFDM _G_PA	Performance Analyzer
OFDM _G_PFA	Portfolio Analyzer
OFDM _G_REPORT_MART	Reporting Data Mart
OFDM _G_RM	Risk Manager
OFDM _G_RTM	Rate Manager
OFDM _G_TP	Transfer Pricing

Managing Privileges

For a comprehensive list of privilege assignments to users, user groups, and security profiles, use Oracle Discoverer FDM Administration standard security reports. You can open Discoverer User and Discoverer Administration directly from the FDM Administration Tools menu or toolbar.

FDM Administration standard security reports show privilege assignments and the sources of the privileges. For example, a report on user AHONG shows that he has privileges for five applications: Balance & Control, FDM Administration, Portfolio Analyzer, Risk Manager, and Transfer Pricing. The report also shows that AHONG has Balance & Control privileges from three sources:

- Balance & Control is assigned to the individual user AHONG

- Balance & Control is assigned to the security profile for Balance & Control, OFDM_S_BC

- AHONG is assigned to a user group that is assigned to the security profile for Balance & Control, OFDM_S_BC

	Application Privilege	Privilege Source	Privilege Source Entity Type
Page Items: User Name: AHONG ▼			
1	Balance and Control	AHONG	User
2	Balance and Control	OFDM_S_BC	Security Profile
3	Balance and Control	OFDM_S_BC	Security Profile (from User Group)
4	FDM Administration	G_<ENG_TSER:	User Group
5	Portfolio Analyzer	AHONG	User
6	Risk Manager	OFDM_S_RM	Security Profile (from User Group)
7	Transfer Pricing	OFDM_S_TP	Security Profile (from User Group)

Users should ideally have privileges based on user assignments to user groups (and the associated security profiles and roles of those user groups). Therefore, in the case of AHONG, you should remove the privilege assignments to the individual user (line 1 in the report sample) and to the security profile (line 2, the profile that is not assigned from a user group).

Removing Privileges: An Example

To remove the Balance & Control privilege granted to AHONG (as an individual), do the following:

1. In the metadata pane, expand the FDM Users folder and double-click AHONG.

2. Click the Application tab.

3. Check the box next to Balance & Control.

4. Click Remove Recipient.
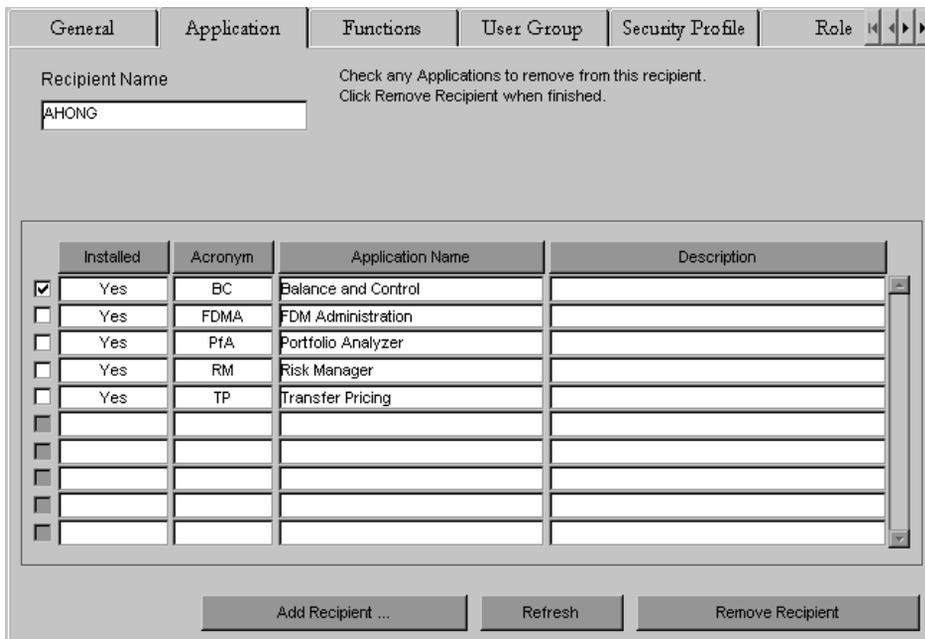
To remove the Balance & Control privilege granted to OFDM_S_BC (the profile that is not assigned from a user group), do the following:

1. In the metadata pane, double-click FDM Security Profiles.

2. Click the Security Profile Recipients tab.

3. In Query By, select Security Profile.

4. In Security Profiles, select OFDM_S_BC.

5. Check the OFDM_S_BC box assigned to AHONG.

6. Click Remove Recipient.

For details about FDM Administration standard security reports, see the *Oracle Financial Data Manager Reporting Administration Guide, Release 4.5.*

In summary, use FDM Administration standard security reports and the tab pages to inquire on or update assignments. General instructions for user and user group assignments follow.

> **Note:** To remove an assignment to a user, you must remove all sources of assignment. Use the FDM Administration standard security reports to list all sources of assignments.

Inquiring on or Updating User Assignments

The following procedure describes how to inquire on or update (add and remove) user assignments.

1. In the metadata pane, expand the FDM Users folder and double-click a user name.

2. Click one of the following tabs:

- ■ Application

- ■ Functions

- ■ User Group

- ■ Security Profile

- ■ Role

- ■ ID Folders

    A list of assignments to the user appears.

3. Optionally you can:

    - ■ Check the items you want to remove from the user and click Remove Recipient.

    - ■ Click Add Recipient and follow the Security Wizard for User Assignment.

Inquiring on or Updating User Group Assignments

The following procedure describes how to inquire on or update (add and remove) user group assignments. Start with the security profile assignments of the user group. After you determine which security profiles a user group is assigned to, you will query by the security profile to determine which applications and functions are assigned to it.

1. In the metadata pane, double-click one of the following:

    - ■ FDM Security Profiles—to inquire on or update the application and functions the user group is assigned, as inherited from its security profiles

    - ■ FDM Roles—to inquire on or update database privileges

2. Click one of the recipient tabs:

    - ■ Security Profile Recipients—if you selected FDM Security Profiles in step 1

    - ■ Role Recipients—if you selected FDM Roles in step 1

3. In Query By, select User Group Recipient.

4. Select a user group.

    A list of assignments to the user group appears.

5. Optionally, you can:

- Check the items you want to remove from the user group and click Remove Recipient.

- Click Add New Recipient and follow the instruction in the Security Wizard window.

Next you query by the security profile.

Querying by the Security Profile

1. In the metadata pane, double-click FDM Applications.

2. Click one of the recipient tabs:

   - Application Recipients

   - Function Recipients

3. In Query By, select Security Profile Recipient.

4. Select a security profile.

   A list of assignments to the security profile (and thus inherited by the user group) appears.

5. Optionally, you can:

   - Check the items you want to remove from the user group and click Remove Recipient.

   - Click Add New Recipient and follow the instruction in the Security Wizard window.

3

Managing Security

Roles and security profiles are crucial to managing security, as the "FDM Administration Workflow" discussion shows in Chapter 2. This chapter describes the use of roles, security profiles, ID folders, function privileges, database system privileges and dynamic table privileges for database and application security.

Topics include:

- Database Security
- Application Security
- Object Privilege Categories

Database Security

You use roles, dynamic table privilege assignments, and database system privilege assignments to manage database security.

Roles—Internal and External

FDM Administration distinguishes between internal privileges—available only to users logging in through an OFS application—and external privileges—available for any database session. When registering a role, you specify internal or external use. The user login associated with an external role can log in to Enterprise Manager, SQL*Plus, or Oracle Discoverer, for example, in addition to specified OFS applications. Internal roles require passwords. See the *Oracle Financial Services Installation and Configuration Guide* for more information on using roles with FDM Administration.

When you use seeded user groups, the necessary seeded role is automatically assigned to the group, as discussed in "Workflow for Database Access for OFS

Applications (User Registration)" in Chapter 2. The seeded role in turn provides the user with the required database access for an application. Therefore, you do not need customized internal roles to provide privileges on FDM reserved objects are not needed. As discussed in "Workflow for Granting User Data Table Privileges" in Chapter 2, you will create new internal roles to provide users access to user data and account tables. See "Object Privilege Categories" in this chapter for more information about roles.

Assigning and Revoking Roles

You assign roles to users and user groups. When you assign a role to a user group, all members of the group are automatically assigned to the role in the Oracle RDBMS.

If you remove an internal role from a user in FDM Administration, only that user, not the user group, has a revoked role. You can remove a role from a user either by removing that user from a user group or by revoking the role from the user. Additionally, if the user receives the same role from multiple sources, such as different user groups, the role is revoked from the user only if he is removed from all user groups.

External roles are never revoked, since they can be shared within a data warehouse environment.

Assigning Database System Privileges

Use the Database System Privilege Assignment window (accessed from Wizards -> Security -> Role Assignment) to grant system privileges to roles. Then selectively assign the roles with system privileges to advanced users or application developers.
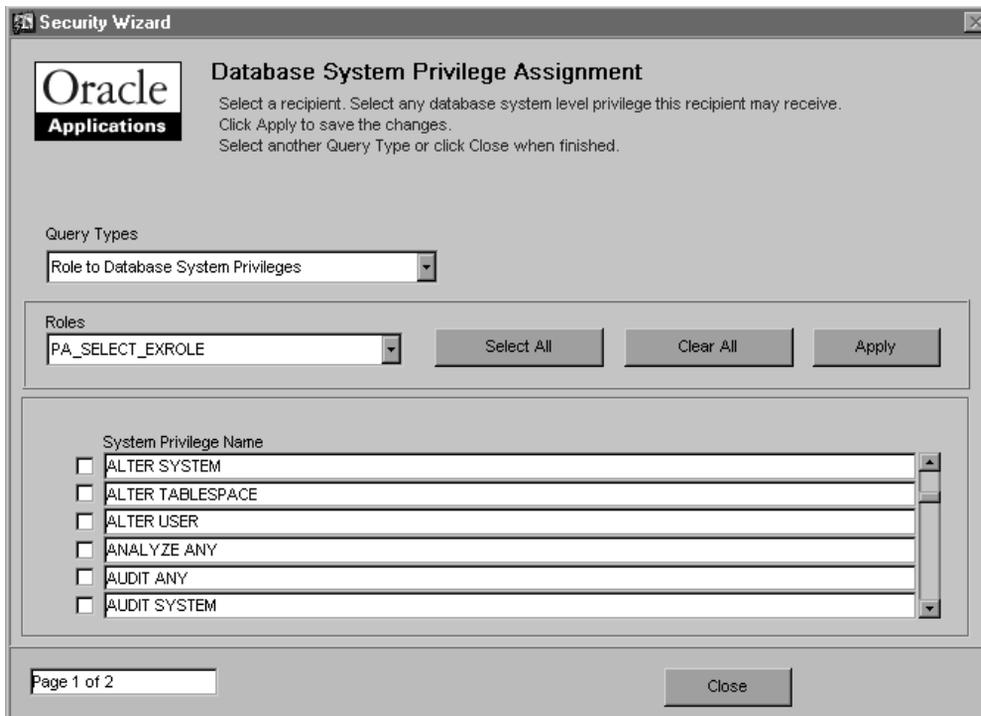
For more information about system privileges, see the *Oracle8i Administrator's Guide* or *Oracle8i Concepts.*

Assigning Dynamic Table Privileges

Use the following windows (accessed from Wizards -> Security) to grant privileges for dynamically created tables such as results tables:

- Dynamic Table Privilege Assignment
- Dynamic Table Classification Privilege Assignment

To grant a user access on a specific table name, rather than all tables within a table classification, use the Dynamic Table Privilege Assignment wizard. The table must already exist in the database. However, after you define the dynamic assignment, the grant is reapplied by the OFSA processing engine whenever the table is recreated.

To grant a user access on all tables within a table classification, use the Dynamic Table Classification Privilege Assignment wizard. In both assignment types, the tables must already exist in the database. However, once the dynamic assignment is defined, the grant is reapplied by the OFSA processing engine whenever the tables are recreated.

You can grant dynamic privileges to roles, user groups, and users. A user who creates Risk Manager result tables and Transformation ID result tables (dynamic tables because they are created during processing) has full access to the tables automatically. For other recipients, you can grant dynamic object privileges on these tables when the tables are created. You can also create your own internal or external roles to manage these privileges. Dynamic table privilege assignment replaces the 4.0 Report Mart Security Manager.
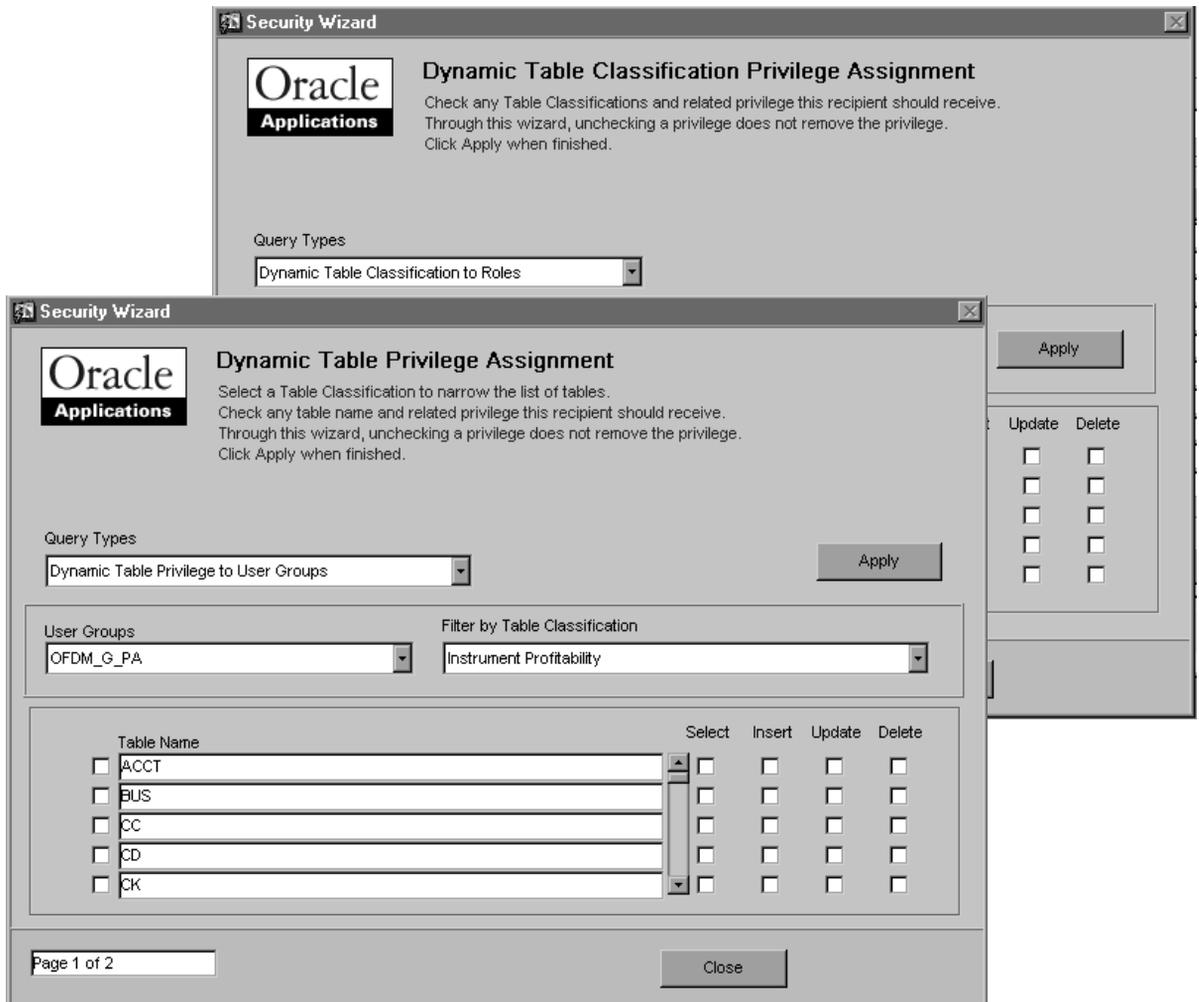
To grant privileges for static tables, use the Database Object Privilege Assignment window from the Role Assignment wizard. See "Workflow for Granting User Data Table Privileges" in Chapter 2.

Application Security

Use security profiles and ID folders to manage the two components of application security—application privilege assignment and function privilege assignment.

Security Profiles

Use security profiles to grant application and function privileges. Seeded security profiles are provided for each of the OFS applications and for FDM Administration tasks (managing objects, managing security, and maintenance tasks). The necessary seeded security profile is automatically assigned to a user group when you use seeded user groups, as discussed in "Workflow for Database Access for OFS Applications (User Registration)" in Chapter 2. The following seeded security profiles are provided:

User Group Name	Provides Privileges For
OFDM _S_BC	Balance and Control
OFDM _S_DI	Discoverer Integrator
OFDM _S_FDMA_OBJ	FDM Administration object management
OFDM _S_FDMA_SEC	FDM Administration security management
OFDM _S_FDMA_USER	FDM Administration maintenance tasks (e.g., Grant All)
OFDM _S_PA	Performance Analyzer
OFDM _S_PFA	Portfolio Analyzer
OFDM _S_RM	Risk Manager
OFDM _S_RTM	Rate Manager
OFDM _S_TP	Transfer Pricing

Creating Security Profiles

You create security profiles when privileges available through seeded data are insufficient for your users. As shown in "Workflow for Granting Ad Hoc User Group Privileges" in Chapter 2, you can create a new security profile for the Transfer Pricing user who needs to examine Transfer Pricing assumptions, but not change or run Transfer Pricing processes. Using the Security Profile Creation wizard, check the box Base Privileges on Existing Security Profile and select the seeded security profile for Transfer Pricing. This copies all the Transfer Pricing privileges to the new profile.

Then remove privileges to restrict access to view only.

ID Folders

ID folders are logical groupings of IDs, stored in the database. IDs are processing instructions and assumptions used for financial analysis in the OFS applications. You can assign an ID folder to users and user groups. Granting access to an ID folder allows the user to access all the IDs in the folder.

When you double-click FDM ID Folders and click the ID Folders tab, you will see two kinds of ID folders in the list—individual and group. (Click the Folder Type column heading to sort by type.) An individual ID folder is created automatically when you register a user. The individual ID folder has the same name as the user name. Only the ID creator has access to the IDs in his eponymous folder. Group ID folders are used to store IDs that are shared by users. You will create group ID folders based on your needs. For example, you may create a group ID folder for users who share Risk Manager Process IDs, as exemplified in the workflow description.

Workflow for ID Folders

```
┌─────────────────────────────────────┐
│                                      │
│          Create User Group           │
│                                      │
└─────────────────────────────────────┘
                    │
                    ▼
┌─────────────────────────────────────┐
│                                      │
│       Assign User to User Group      │
│                                      │
└─────────────────────────────────────┘
                    │
                    ▼
┌─────────────────────────────────────┐
│                                      │
│           Create ID Folder           │
│                                      │
└─────────────────────────────────────┘
                    │
                    ▼
┌─────────────────────────────────────┐
│                                      │
│      Assign ID Folder to User Group  │
│                                      │
└─────────────────────────────────────┘
```
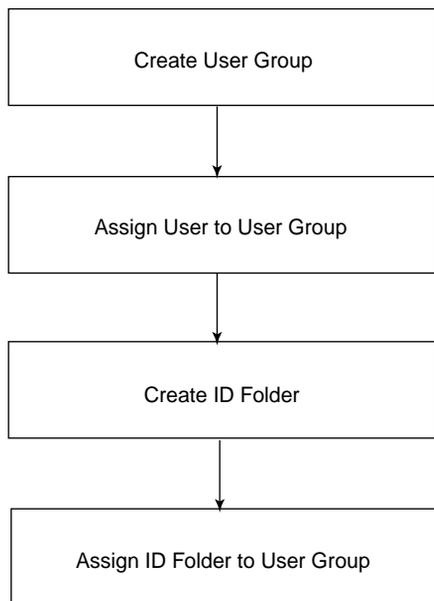
Create User Group Use the User Group Creation wizard to create a new group for Risk Manager Process ID users; for example, you might create RM_PROCESS_G.

Assign Users to User Group In the User Group Assignment window, assign the Risk Manager Process ID users to RM_PROCESS_G.

Create ID Folder   Using the Create ID Folder wizard, create a folder for the Risk Manager Process IDs, for example, RM_PROCESS_ IDS.

Assign ID Folder to User Group In the ID Folder Assignment window, assign RM_PROCESS_G to RM_PROCESS_ IDS.
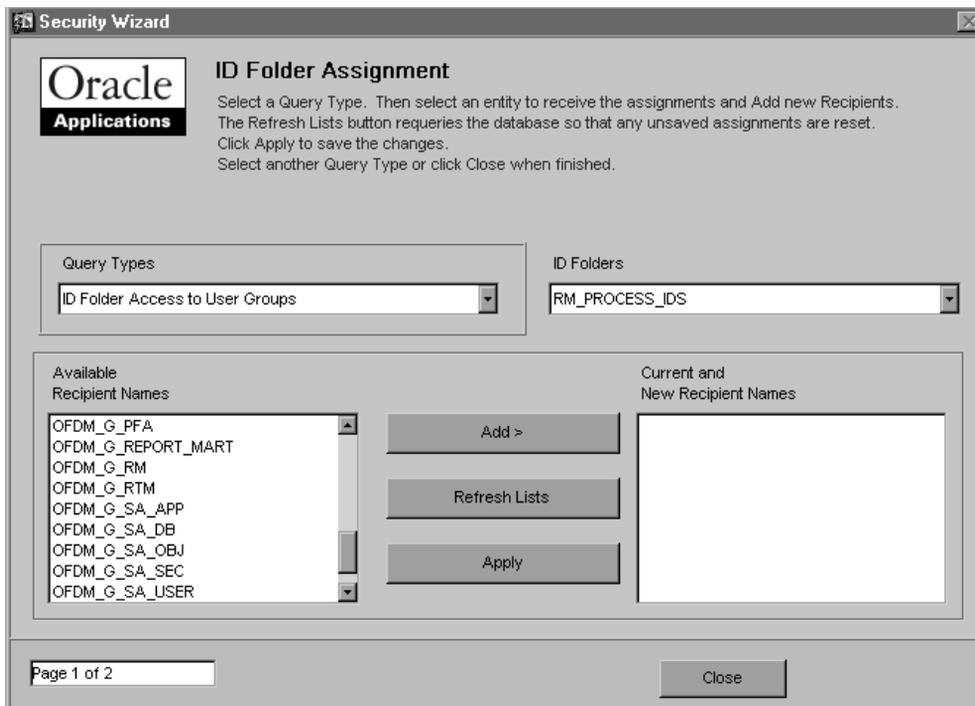
As the ID Folder Assignment window shows, you can assign more than one user group to a group ID folder.

The following seeded ID folders are also provided:

- ALL—where all users can share IDs. This ID folder is automatically assigned to a newly registered user.

- OFSA—where reserved IDs installed with the database (and needed for reporting by users migrated from an earlier installation) are located. You should not create any IDs in this folder.

- DELETED_USERS—where the ID folders of unregistered users are automatically moved. See "Unregistering Users" in Chapter 2.

Application and Function Privileges

Grant application privileges to a user's security profile so that the user can log in to the applications listed under FDM Applications. (Customer Householding and Market Manager, however, are not managed with FDM Administration.) See "Proce-

dure for Granting Ad Hoc User Group Privileges" in Chapter 2 for how to assign application privileges.

Grant function privileges to a user's security profile when the user needs to perform a specific task for which he does not have privileges through his typical set of privileges. If a user needs to run an Allocation ID, you will create a security profile, for example, S_PA_ALLOC, to which you assign the Allocation ID (under Construct Name) and the actions Create, Delete, Run, Update, and View.
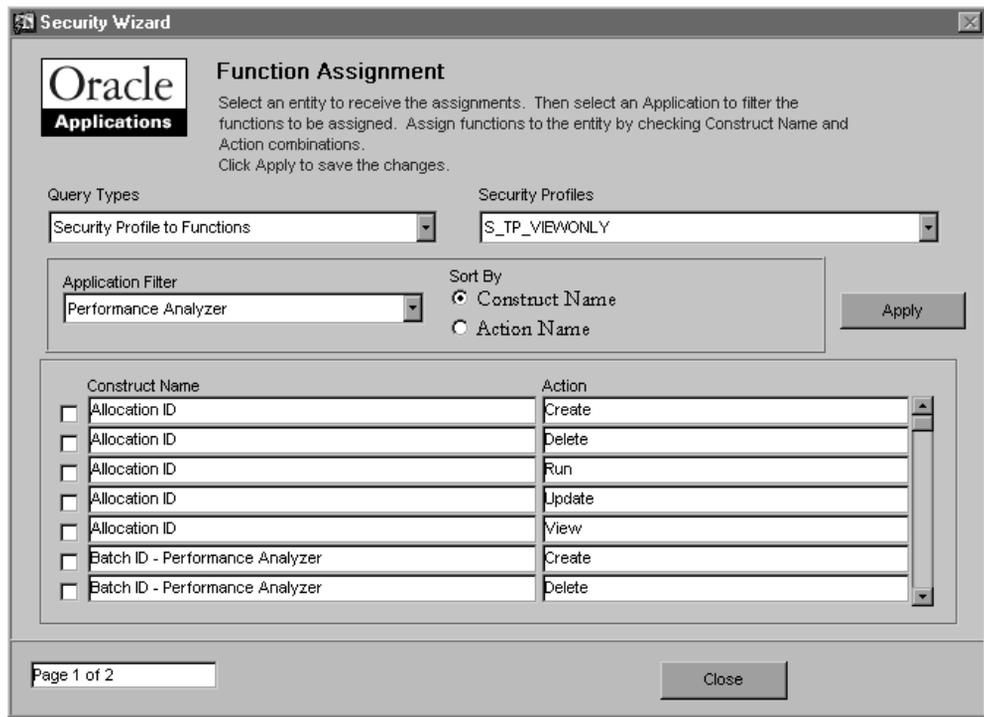
For a complete discussion of this process, see "Workflow for Granting Ad Hoc User Group Privileges" in Chapter 2.

Object Privilege Categories

Categories of privileges required for using the OFS applications are:

- Internal Application Objects
- Instrument and Client Data

- Reporting Data Mart
- Dynamic Tables

Internal Application Objects

Each OFS application requires a specific set of privileges to access internal objects. This includes retrieving FDM metadata information, operations against OFSA ID tables (such as inserting a new ID), and retrieving sequence numbers. Because these objects are reserved for FDM use, it is unlikely that administrators require any special database security rules for the objects. FDM Administration provides a seeded role for each application.

Most of the seeded roles are internal. (See "Roles—Internal and External" in this chapter.) Exceptions include OFDM_R_LOGIN and OFDM_R_DI. Privileges for the internal roles are available to users only when they are logged in to one of the OFS applications. Because these roles provide full privileges to all internal tables accessed by the application, administrators should rely on functional security assignments (see "Application Security" and "Application and Function Privileges" in this chapter) to restrict undesired operations from specific users. As discussed in Chapter 2, "Managing Users", granting a user privileges to the seeded user group for an OFS application grants the user all of the required database privileges for that application. The seeded internal roles are listed in the *Oracle Financial Services Installation and Configuration Guide*. With FDM Administration you can also create your own internal roles to manage privileges for OFS application objects.

Instrument and User Data

Privilege management for instrument and user data tables (including LEDGER_STAT) is the purview of the individual administrators. With FDM Administration, you can create and manage your own internal and external roles for such tables. By default, users have no privileges for these tables.

Typically, at least two roles, one internal and one external, are required to manage privileges for these tables. The internal role provides full select, insert, update, and delete privileges on these tables so that users can perform application operations such as running Allocation IDs or Correction Processing IDs. User actions against these tables are controlled using application and function security.

The external role provides the privileges necessary for reporting. This role provides select access on these tables so that users are able to run reports in Discoverer or SQL*Plus. Depending on the implementation, you may require additional roles to manage the instrument and user data tables.

For customers migrating from 3.5 and 4.0, a dynamically seeded role is created to facilitate the transition to the Release 4.5 database environment. See the *Oracle Financial Services Installation and Configuration Guide* for more information.

Reporting Data Mart

Privileges required for users to access OFSA reserved tables for Discoverer reports are provided by the external seeded role OFDM_ R_REPORT_MART. See the *Oracle Financial Services Installation and Configuration Guide* for more information.

4

Managing Objects

In the context of OFS applications, an object is a database table or view. You may use one or more objects in generating reports or executing OFS operations. Object management refers to making an object available within the FDM metadata for use with the OFS applications.

Object management encompasses two activities: preparing an object for use and maintaining a previously-prepared object. Both activities are handled from within FDM Administration.

The process of preparing an object for use (called registering an object) comprises the following steps:

1. Identifying the object

2. Assigning column properties

3. Classifying the object

4. Mapping code descriptions

After you register an object, you may view it and modify it.

This chapter gives a detailed description of, and procedures for, registering, viewing, and modifying objects for use within the FDM environment.

Step One: Identifying an Object

The first step in registering an object for use within the FDM environment is to identify it. This enables the FDM metadata and other OFS applications to recognize it as a unique entity.

In identifying an object you name it, describe its purpose, and specify the characteristics of its columns. This is done with the help of a wizard.

When you register an object, FDM Administration automatically checks it for validity, compares it to existing objects to prevent duplication, and identifies default data types for its columns.

> **Note:** FDM Administration provides default FDM Data Types for all columns within new objects. These defaults are based on attributes such as name and size. For example, a column named MATURITY_DATE has a default FDM data type of DATE.

If, during a validity check, FDM Administration discovers that a given column already exists in another table, it selects the existing column's definitions for use with the new column. You may change these default settings as needed.

If you are registering an object from another schema, FDM Administration creates a view in the FDM schema. FDM Administration then displays, for your review, the SQL statement it used to create the view.

How to Identify an Object

To identify an object, do the following:

1. From the Wizards menu, select Register -> Object.

   The first page of the wizard appears.

2. Select from the pull-down list a user name in which the object to be registered exists. Do likewise for the object name.

3. Enter a display name for the object. This name will appear in lists of values within OFS applications.

4. Indicate whether or not you want the object displayed in OFS applications.

5. Optional: enter a description of the object.

6. Click Next.

   The second page of the wizard appears. This page contains the following column information:

   - A display name
   - FDM Data Type
   - Database file name
   - A detailed description of the column, if one was entered

7. If necessary, modify the following data:

   - Database file (DBF) name
   - Column display names that appear as defaults
   - FDM data types

8. For each column, choose whether or not to display it in OFS applications.

9. Optional: enter a description for each column.

10. Click Next.

    A report appears, describing the object and columns as you have defined them. If you want to make any changes, click the Back button.

11. When you are satisfied with the object definition, choose one of the following options:

    ■ To continue the registration process, click the checkbox for the Column Properties Assignment wizard. Then click Finish.

       If you proceed to the Column Properties Assignment wizard, the first screen appears. Otherwise, the main tree of FDM Administration returns to your screen.

    ■ To save the identification and exit the wizard, click Finish.

       Note: The object is not fully registered and valid until all four steps of the registration process have been completed.

Step Two: Assigning Column Properties

The second step in registering an object is to assign properties to its columns. Column properties are the attributes that columns need in order to meet certain requirements or produce particular results. There are 12 properties, divided into the following categories:

- The processing key

- Mutually exclusive properties

- Multiplier properties

- The Related Field property

- Properties assigned automatically by Risk Manager

- The Reporting Not Visible property

A description of the each category follows.

> **Note:** Unless otherwise noted, a column can have two or more properties from a given category.

FDM Administration references column properties during the next step of the registration process (table classification). Two other OFS applications use column properties: Discoverer Integrator and Performance Analyzer.

Column Properties

The Processing Key

The processing key is a set of columns that uniquely identifies the rows for the purpose of data manipulations. In general, the processing key is the same as the primary key.

Assign the processing key to columns in all objects.

Mutually Exclusive Properties

The following properties are mutually exclusive; you can assign only one to a given column.

Standard Rates Assign this property when the value stored in a column is a pure rate, and not a weighted rate.

This applies to columns in instrument tables that have an FDM Data Type of *RATE*.

Balance Weighted Object Assign this property when the rate value stored in the column is weighted by a balance, and is not a pure rate.

This applies to columns in non-instrument tables that have an FDM Data Type of *RATE*.

Transformation Processing assigns this property to all rate columns in the Transformation output tables.

Statistic Assign this property to a column storing statistical information.

Balance Assign this property to a column storing balance information

Multiplier Properties

Assign multiplier properties to columns of the following FDM Data Types:

- MULT (Multiplier)
- TERM (Term)
- FREQ (Frequency)

Multiplier Related Field Assign this property when the column is a multiplier and has an FDM Data Type *TERM* or *FREQ*. When you assign it, also assign the Related Field property to specify the unit of time, such as day, month, or year. (See "The Related Field Property" in this chapter.)

Term Multiplier Assign this property to columns that are term multipliers, such as Amortization Term Multiplier.

Frequency Multiplier Assign this property to columns that are frequency multipliers, such as Payment Frequency Multiplier.

The Related Field Property

The Related Field property identifies columns that specify units of time. Assign it when you assign Multiplier Related Field, as previously described.

> **Note:** In this example, a table has a column titled Amortization Term and another titled Amortization Term Multiplier. You would do the following:
>
> 1. Assign the Amortization Term column two properties: Multiplier Related Field and Related Field.
>
> 2. For the first property, Multiplier Related Field, leave the related field unassigned.
>
> 3. For the second property, Related Field, specify that the related field is Amortization Term Multiplier.
>
> 4. For the column titled Amortization Term Multiplier, assign only one property: Term Multiplier. Leave the related field unassigned.

Properties Automatically Assigned by Risk Manager

Risk Manager processing automatically assigns the following properties:

RM Scenario Relationship The column identifies a Risk Manager scenario.

RM Result Type Relationship The column identifies a Risk Manager Result Type.

The Reporting Not Visible Property

Assign this property when the column does not need to be accessible for reporting, such as long description columns in Code Values tables.

How to Assign Column Properties

1. Access the wizard for this step by doing one of the following:

   - From the preceding wizard (in which you identified the object), select the Column Property Assignment wizard.

   - From the Maintenance menu, select Column Property Assignment.

   - From the Column Properties tab page, click Add New Assignment.

   In the first screen, the column properties that have already been assigned appear in the upper portion. The lower portion is reserved for making new assignments.

2. Select the column name to which you want to assign the column property.

3. Select the property column name.

4. Click Add New Assignment.

5. Repeat steps 2 through 4 for any other columns within the object.

6. When you finish adding assignments, click Apply to save them to the database.

> **Note:** If you do not click Apply, your new assignments will not be recorded.

7. To run the next wizard in the sequence (the Table Classification wizard), click the checkbox.

8. To exit the wizard, click Close.

Step Three: Classifying an Object

After identifying an object and defining its columns, the third step of registration is to tell the FDM database how to use it. This is done by selecting and inputting one or more classification codes.

Types of Classifications

There are two types of classification codes, one for each type of object: reserved and user-assignable. Reserved objects are those the FDM database creates for use within itself and within other OFS applications. The database also assigns classification codes to these objects. With few exceptions, you cannot modify or classify reserved objects. You can, however, modify and classify user-assignable objects. These comprise client data objects and objects you have defined.

> **Note:** The FDM Instrument tables that were installed with the database are user-assignable objects. Therefore, you may modify and classify them.

Some user-assignable classifications require an object to meet requirements pertaining to column names, column characteristics, and stored procedures (validation logic). If you assign a particular classification to an object and the object does not meet the given requirements, FDM Administration will reject the classification. It will then produce a report describing the discrepancy, enabling you to correct the error.

The following is a description of user-assignable classifications. For a description of reserved classifications, see the section on table classification in the *Oracle Financial Services Installation and Configuration Guide, Release 4.5.*

> **Note:**   A subset of reserved object classifications, called dynamic table classifications, is available to administrators. See the section on dynamic table classifications in the *Oracle Financial Services Installation and Configuration Guide, Release 4.5.*

User-Assignable Classifications

The following is a summary of user-assignable classifications. Those having requirements are noted in the Description column.

Code	Classification	Description
20	Instrument	The object stores client account data.
		FDM Administration automatically assigns this classification when you assign the following classification codes: 200, 210, 300, 310, 330, 360, and 370.
		There are no requirements for this classification.
100	Portfolio	The object has the set of portfolio columns. It is available for use with any portfolio-compatible OFSA ID.
		This is the only classification you may edit and control. Refer to the *Configuration Guide* for instructions on editing the list of columns that compose this classification.
		There are no requirements for this classification.

Code	Classification	Description
200	TP Cash Flow	The object is used for Transfer Pricing Cash Flow processing.
		The following property requirements must be met:
		■ Basic Instrument
		■ Cash Flow Processing
		■ Cash Flow Edit
		■ Multi-Currency
		■ TP Basic Requirements
		■ Valid Instrument Leaves
		■ Valid Instrument Key
210	TP Non-Cash Flow	The object is used for Transfer Pricing Non-Cash Flow processing.
		The following property requirements must be met:
		■ Basic Instrument
		■ Multi-Currency
		■ TP Basic Requirements
		■ Valid Instrument Leaves
		■ Valid Instrument Key
295	User-Defined Codes	The object is base table for storing user-defined code values.
		Assign this code when you have added a new code column to the Financial Data Model.
		There are no requirements for this classification.
296	Multi-Language Support (MLS) Descriptions User-Defined	The object stores translatable descriptions for a code column.
		Assign this code when you have added a new code column to the Financial Data Model in a multi-language support environment.
		There are no requirements for this classification.
298	Code Descriptions User-Defined	The object retrieves descriptions for a code column.
		There are no requirements for this classification.

Code	Classification	Description
300	Transaction Profitability	The object is a transaction summary, to be used in Performance Analyzer allocation processing. The following property requirements must be met: ■ Basic Instrument ■ Multi-Currency ■ Valid Instrument Leaves ■ Valid Transaction Key
310	Instrument Profitability	The object is an instrument table, to be used for Performance Analyzer allocation processing. The following property requirements must be met: ■ Basic Instrument ■ Multi-Currency ■ Valid Instrument Leaves ■ Valid Transaction Key
320	User-Defined	The object you created is not assigned to any other table classification. There are no requirements for this classification.
330	Data Correction Processing	The object is to be used with Balance and Control Data Correction processing. The following property requirement must be met: Valid Correction Key
360	RM Standard	The object is to be used for Risk Manager processing. The following property requirements must be met: ■ Basic Instrument ■ Multi-Currency ■ Cash Flow Procedure ■ Valid Instrument Leaves ■ Valid Instrument Key

Code	Classification	Description
370	TP Option Costing	The object is to be used for Transfer Pricing Option Costing processing.
		The following property requirements must be met:
		■ Basic Instrument
		■ Multi-Currency
		■ TP Basic Requirements
		■ TP Option Costing Requirements
		■ Valid Instrument Leaves
		■ Valid Instrument Key

How to Classify an Object

1. To run the wizard for this step, do one of the following things:

   ■ From the preceding wizard (Assigning Column Properties), select the Table Classification Assignment wizard to follow automatically.

   ■ From the Table Classification Assignments tab page, click Add New Assignment.

   ■ From the Maintenance menu, select Table Classification Assignment.

   The first page of the wizard provides a list of the table classifications.

2. Check all classifications you want to assign to the object.

3. Click Next.

FDM Administration examines your selections for unmet requirements, such as missing columns and validation failure. Then it generates a report of the results, which appears as the second page of the wizard.
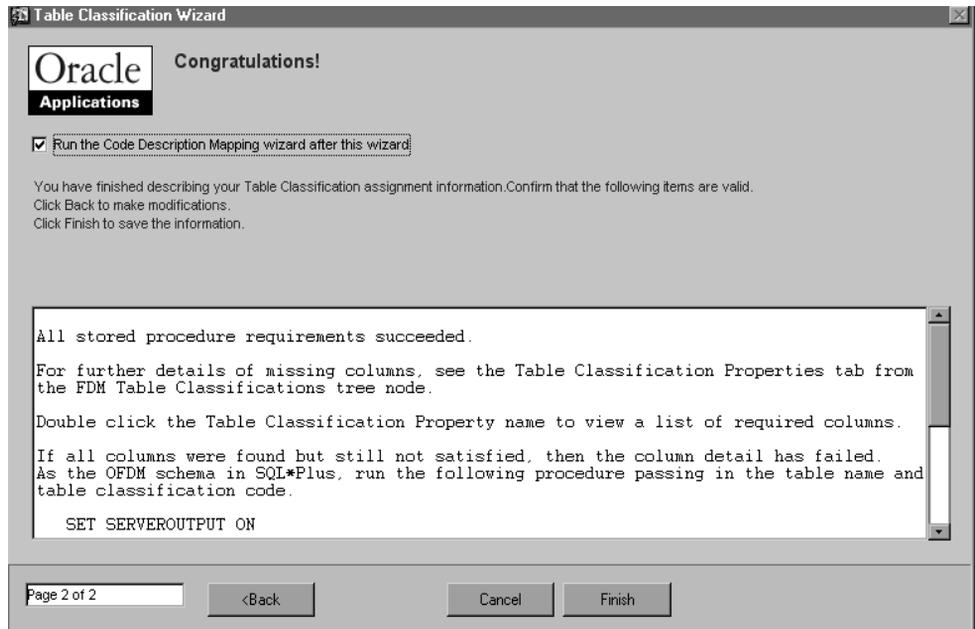
4. If the report states "one or more stored procedures failed," then follow the instructions on the screen to run the logic check manually. Doing so enables you to determine why the classification was not accepted.

5. To deselect one or more of the rejected classifications, click the Back button; then click the classifications to be deselected.

6. To run the next wizard in the sequence (Code Description Mapping), click the checkbox.

7. To exit the wizard, click Close.

Step Four: Mapping Code Descriptions

Code columns store numeric or alphanumeric codes. Each code has a written description, which the FDM database stores in a separate data structure.

To view code descriptions (instead of the codes themselves) within an FDM report, you need to provide a code description mapping for certain columns. This enables the description *US Dollar*, for example, to appear in place of the code *USD*.

> **Note:** You only need to map columns having FDM Data Type Code.

Following is the procedure for mapping a column in a new object.

How to Map Code Descriptions

1. To access the wizard for this step, do one of the following:

   - From the preceding wizard (Assigning Table Classifications), select the Code Description Mapping wizard.

   - From one of the FDM Description Tables tab pages, click Add New Mapping.

   - From the Maintenance menu, select Code Description Mappings.

2. In the New Mappings section, go to the field labeled "Columns From This Table" and select the first column you want to map.

3. In the Description Table Name field, select the object that provides the written description for the code column.

4. From the Description Join Column Name list, select the column you want to map to by specifying the Join Column name. This establishes a link between the desired code and its corresponding description.

5. From the list labeled Values Column Name, designate the column to store the description values to be shown in place of code.

6. Click Add New Mapping.

7. Repeat steps 2 through 6 for all mappings you want to make for this column.

8. After creating all desired mappings, click Apply.

All new mappings appear under Current Mappings.

9. Click Close.

Viewing, Modifying, and Deleting Registered Objects

Once an object is registered, you can view the data you entered in wizards, and in some cases edit and delete it by going to the FDM Administration navigation tree and using the appropriate tab pages.

Working With Object Identification Data

Besides viewing the identification data you entered in Step One, you can do the following:

- Edit such things as the display name and DBF name.

- Add one or more columns to an object and reregister it.

- Remove a column or object from the FDM metadata by unregistering it.

From the FDM Administration tree, select one of the following tab pages in FDM Objects:

Objects The Objects page lists all registered objects. These are viewable by table or by table classification. You can change the Display Name value, DBF name, or whether an object appears in OFS applications.

Columns The Columns tab page lists all columns in a given object. Through this page you can change the Display Name value, DBF name, FDM Data Type, or whether or not a column appear in OFS applications.

Object Description This page enables you to enter or modify the description of a specified object.

Column Description This enables you to enter or modify the description of a given column.

> **Note:** Be sure to confirm any changes you make by clicking the Apply button.

How to Add a Column

When you add a column to an object you must identify the object again. This enables the FDM metadata to recognize the new column. All other data (column properties, object classifications, and code mappings) remain as you previously defined them.

To identify an object after a column has been added, do the following:

1. From the Wizards menu, select Register -> Reregister Object.

   The first page of the wizard appears.

2. Select a user name from the pull-down list. Do likewise for the object name.

3. Enter a display name for the object. This name will appear in lists of data values within OFS applications.

4. Indicate whether or not you want the object displayed in OFS applications.

5. Optional: enter a description of the object.

6. Click Next.

   The second page of the wizard appears. This page contains the following column information:

   ■ A display name

   ■ FDM Data Type

   ■ Database file name

   ■ A detailed description of the column, if one was entered

7. If necessary, modify the following data:

   ■ Database file (DBF) name

   ■ Column display names that appear as defaults

   ■ FDM Data Types

8. For each column, choose whether or not to display it in OFS applications.

9. Optional: enter a description for each column.

10. Click Next.

    A report appears, describing the object and columns as you have defined them. If you want to make any changes, click the Back button.

11. When you are satisfied with the object definition, choose one of the following options:

    ■ To continue the registration process, click the checkbox for the Column Properties Assignment wizard. Then click Finish.

      If you proceed to the Column Properties Assignment wizard, the first screen appears. Otherwise the main tree of FDM Administration returns to your screen.

    ■ To save the identification and exit the wizard, click Finish.

You can view your changes on the FDM Objects tab pages.

> **Note:** At the conclusion of this process, only the column or columns you have added will be displayed. Previously-registered columns will not be displayed.

How to Remove an Object

If you want to remove an object from the FDM metadata, you can unregister it through the Objects page.

To unregister an object, do the following:

1. In the FDM Administration tree, double-click FDM Objects. Select the Objects tab.

2. Locate the object you want to unregister. Click in the box to the left of it.

3. Click Unregister.

Working With Column Property Assignments

You can add or remove column properties through the Column Properties tab page in FDM Objects. This page lists the properties you assigned in Step Two.

How to Add Column Properties

To add column properties, follow "How to Assign Column Properties" in this chapter.

How to Remove Column Properties

In the Column Properties tab page, do the following:

1. Select the object you want in the Tables field.

2. Select the column property in the Column Properties field.

3. Click the entries you want to remove.

4. Click the Remove Assignment button.

Working With Object Classifications

You can access object classification data through the following FDM Table Classification tab pages. Be sure to click the Apply button to confirm your changes.

Table Classifications This page lists all classifications, including codes and descriptions.

Table Classification Assignments This page enables you to review table classification assignments in the following dimensions:

- All tables assigned to a specified classification
- All classifications assigned to a given table

Table Classification Properties This page lists object classifications and their requirements (where applicable) and table properties. You can review, but not modify, the data.

How to Add an Object Classification Assignment

To add an assignment, see "How to Classify an Object" in this chapter.

How to Remove an Object Classification Assignment

To remove an object classification assignment, do the following:

1. From the Table Classification Assignment tab page, select the object or classification you want to change.
2. Click the checkbox by the classification you want to remove.
3. Click Remove Assignment.

   The assignment is removed from the FDM metadata and the screen is refreshed.

Working With Code Description Mappings

You can view code description mapping data on the FDM Description Tables tab pages. Choose the type of display you want:

Description Tables by Column Name This page lists all code description mappings for the column name you specify.

Description Tables by Table Name This page lists all code description mappings for the specified table name.

How to Remove a Code Description Mapping

To remove a mapping, do the following:

1. Click the check boxes of all mappings you want to remove.

2. Click Remove Mapping.

The mapping is removed from the FDM metadata and the screen is refreshed.

Leaf Management

In the context of OFS applications, a Leaf Column is an attribute which provides data dimensionality. Leaf Columns enable data categorization via hierarchies (Tree Rollups) in the OFS applications. They are special columns within FDM, used for a variety of purposes within the OFS applications, including Performance Analyzer, Risk Manager and Transfer Pricing processing operations. Generally, Leaf Columns are defined for use with Instrument and client data tables, including the LEDGER_ STAT table.

Leaf management refers to the identification of physical column names as Leaf Columns. as well as the definition of their characteristics. This is a separate concept from the management of the individual Leaf Values (Leaf Nodes) for registered Leaf Columns. The management of these Leaf Values is completed within the Leaf Setup screen of the individual OFS applications.

See the *Oracle Financial Services Installation and Configuration Guide* for more information on leaf management.

Registering a Leaf Column

To register a leaf column, do the following:

1. From the Wizards menu, select Register -> Leaf.

   The first page of the wizard appears.

2. Type in the Leaf Column Name.

3. Enter a description for the Leaf Column.

4. Select a Registration Type.

   Available Registration Types are All or Ledger Stat Only. Leaf Columns registered as Ledger Stat Only are only required to exist on the LEDGER_STAT table and a few other specific tables. Leaf Columns registered as All are required to exist on a much larger set of objects. Refer to Step 1 above for information regarding these options.

5. For Key Leaf, click Yes or No.

FDM requires that Leaf Columns designated as Key are a component of the primary key for certain designated tables. Leaf Columns that are not key are never a component of the primary key for tables.

6. Click Next.

The confirmation page of the wizard appears.

7. Click Finish.

When you click the Finish button, the wizard validates all of the requirements for the new Leaf Column (described in the steps above). If these requirements are met, the FDM Administration application registers the Leaf Column in the FDM Metadata. The new Leaf Column is then available within the OFS applications for use.

If the requirements are not met, the wizard displays an appropriate error message.

Modifying Registered Leaf Columns

Once a Leaf Column is registered, you can view the data you entered in the wizard, and modify description information for it, by selecting FDM Leaves from the FDM Administration navigation tree.

All the information about the Leaf Column, except for the Leaf Description, is protected from update. To modify the Leaf Description, go to the Leaf Descriptions tab page. Type in the new Description for the Leaf Column, and click the Apply button.

You can also unregister a Leaf Column. Unregistered Leaf Columns may still exist as registered columns on FDM objects. However, the Leaf Column is not identified in the FDM Metadata as such, and therefore does not appear in the OFS applications as a valid Leaf Column.

Unregistering a Leaf Column

To unregister a leaf column, do the following:

1. Go to the Leaves tab page.

2. Select the Leaf Column to Unregister.

3. Click the Unregister button.

The Leaf Columns seeded in the FDM database cannot be unregistered.

Caution: Once a Leaf Column is unregistered, modify the unique indexes and Column Property assignments for the affected Objects as appropriate. If the Unregistered Leaf Column is not removed from the appropriate unique indexes and Processing Key Column Property assignments, the OFS application will not operate correctly.

For more information on Leaf Column Unregistration, see the chapter on object management in the *Oracle Financial Services Installation and Configuration Guide, Release 4.5.*

5

Migrated Data

The new security framework in FDM Administration manages security differently from previous versions. User names migrated from a 3.5 or 4.0 database to the 4.5 database retain the same database and application privileges. However, because previous versions operated on a union-of-restrictions paradigm rather than the Version 4.5 union-of-privileges paradigm, the migrated data requires some realignment.

This chapter describes the workflow for migrated data by following an example of a Performance Analyzer user. For migrated users, this workflow replaces the workflows described in Chapter 2.

For the details necessary to work with migrated users and privileges, you should consult the *Oracle Financial Services Installation and Configuration Guide, Release 4.5*.

How Data Was Migrated: An Example

Assume, for example, that a group of Performance Analyzer users in your pre-migrated data, Grp A, had unrestricted access to Performance Analyzer. The following table shows how Grp A appears in Release 4.5 of FDM Administration:

In Release 4.0, Appeared As:	In Release 4.5, Appears As:
Grp A—unrestricted access to Performance Analyzer	G_GrpA—unrestricted access to Performance Analyzer
■ The Performance Analyzer application and menu privileges of Grp A	S_GrpA—a security profile with all Performance Analyzer functions
■ The ID grouping of Grp A	GrpA—an ID folder for Performance Analyzer IDs

Also assume that your pre-migrated data includes User A, who has Performance Analyzer privileges, but is restricted from running Allocation IDs. After migration, User A has the same Performance Analyzer privileges that were assigned pre-migration. The difference is that all these privileges are assigned directly to the user, an undesirable outcome, rather than originating from a security profile or user group assignment.

In this example, S_GrpA should ideally be assigned to G_GrpA automatically in the migration, but then User A will have Allocation ID privileges, from which he was restricted pre-migration. Therefore, part of the workflow for migrated data will be to create new security profiles and user groups for users like User A.

The following workflow assumes a migration scenario for Performance Analyzer User A. You will need to complete the steps in this workflow for each application at your site. Also, for each user, you will need to assess and note all needed privileges since you will not have visibility of the user requirements once you start.

Workflow for Migrated Data

```
┌─────────────────────────────────────────────┐
│      Remove Individual Privileges from User   │
└─────────────────────────────────────────────┘
                      │
                      ▼
┌─────────────────────────────────────────────┐
│               Create User Group               │
└─────────────────────────────────────────────┘
                      │
                      ▼
┌─────────────────────────────────────────────┐
│            Assign Users to User Group         │
└─────────────────────────────────────────────┘
                      │
                      ▼
┌─────────────────────────────────────────────┐
│              Create Security Profile          │
└─────────────────────────────────────────────┘
                      │
                      ▼
┌─────────────────────────────────────────────┐
│        Remove Alloc ID from the Security Profile │
└─────────────────────────────────────────────┘
                      │
                      ▼
┌─────────────────────────────────────────────┐
│        Assign Security Profile to User Group  │
└─────────────────────────────────────────────┘
                      │
                      ▼
┌─────────────────────────────────────────────┐
│          Assign Seeded Role to User Group     │
└─────────────────────────────────────────────┘
```
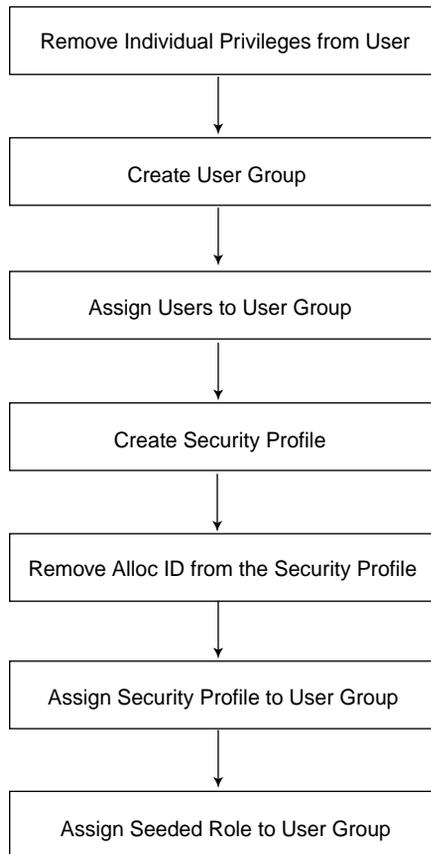
Remove Individual Privileges from User In the FDM Users metadata, double-click User A, the Performance Analyzer user restricted from Allocation IDs. Starting with the Application tab, remove the assignments to User A by checking all the boxes and clicking Remove Recipient. Continue removing all recipients for the rest of the tab pages.

Create User Group Using the User Group Creation wizard, create a user group, for example, G_PA_NO_ALLOC, for Performance Analyzer users restricted from Allocation IDs.

Assign Users to User Group Using the User Assignment wizard, assign User A to G_PA_NO_ALLOC.

Create Security Profile Using the Security Profile Creation wizard, create a security profile, for example S_PA_NO_ALLOC, for Performance Analyzer users restricted from Allocation IDs. Check Base Features on Existing Security Profile and select the seeded Performance Analyzer security profile, OFDM_S_PA.

Remove Allocation ID from the Security Profile Double-click FDM Applications in the metadata. Click the Function Recipients tab and query by S_PA_ NO_ALLOC. Check Allocation ID for all actions—View, Update, Run, Create, and Delete—and click Remove Recipient.

Assign Security Profile to User Group Using the Security Profile Assignment wizard, assign S_PA_NO_ALLOC to G_PA_NO_ALLOC.

Assign Seeded Role to User Group Using the Role Assignment wizard, assign the seeded role for Performance Analyzer, OFDM_R_PA, to G_PA_NO_ALLOC.

After completing the steps in the migrated data workflow, you can manage migrated users like other users in FDM Administration.

Glossary

As-of-Date

The date when the data is current.

Asset/Liability Management Committee

The Asset/Liability Management Committee (ALCO) is an organization within a financial institution whose charter is to manage interest rate risk.

At-Risk Period

The time period for value-at-risk. That is, the difference between the future date when portfolio loss is evaluated and the as-of-date.

Base Rates

A section in Oracle Risk Manager that stores the interest rates associated with the as-of-date of the data.

Basis Points

1/100th of a percent. Abbreviated as *bp*.

Breakage Charges

A charge assigned to an account whose actual cash flows are significantly different from the expected cash flows when the account funded.

Business Area

A conceptual grouping of tables or views represented as folders, items, conditions, filters, joins, and hierarchies. Each business area is grouped within the same End User Layer (EUL) that the current session is connected to.

Cash Flow Table

An instrument table that contains all of the Oracle Financial Services (OFS) cash flow columns.

Cash Flow Column

A column in an instrument table that is used by the OFS cash flow engine to perform cash flow analysis on a record.

Configuration ID

An ID that stores system default information that has been customized for the user and/or the institution.

CPR (Constant Prepayment Rate)

A method of measuring an annualized prepayment rate.

Credit Risk

The risk that a loan holder will not be able to repay some portion of a loan.

Current Rate Risk Profit

Component of funding center rate risk results attributed to current mismatches of assets and liabilities.

Data Correction Processing ID

An ID that enables you to simultaneously correct multiple columns in a database table in one pass through the database, using a previously defined Correction Rule ID.

DDA (Demand Deposit Account)

An account paying on demand, with no notice of withdrawal required, for example, a checking account.

De-annualize

To compute the monthly equivalent rate of an annual rate.

Duration

The rate of market value change with respect to discount rate changes. A measure of market value sensitivity: the lower the value, the less sensitive the market value to changes in interest rates.

Embedded Rate Risk Profit

A portion of funding center rate risk result attributed to prior rate bets.

End User Layer (EUL)

A metalayer that contains data about other tables in a database. Conceptually, the EUL shields the end user from the complexity of the database. The database tables are modified by the Oracle Discoverer Administration Edition and Oracle Financial Data Manager/Discoverer Integrator. Business areas are defined within the EUL and then used in the Oracle Discoverer End User Edition.

Floating Tree Bar

A window that enables you to choose the appropriate branch or leaf in the Tree ID that is currently active.

Funding Center

An area in a financial institution that receives the transfer pricing charge and credit for funds.

General Ledger (GL)

The main data source that defines the financial reality for an institution. The general ledger reflects all accounting entries.

Historical Rates Table

The OFS table that holds all historical actual interest rates.

Instrument

Legally enforceable agreements about types of financial security. See *Instrument Table.*

Instrument Table

A type of table in the Oracle Financial Data Manager (FDM) database that is used to store account-level information.

Instrument Records

Rows in the Oracle Financial Data Manager (FDM) database that contain account information for each customer. Examples are checking accounts, mortgage accounts, or installment debt accounts for a given customer.

Interest Rate Code

User-defined code to reference a yield curve or single rate index for historical analysis and transfer pricing and interest rate forecasting purposes.

Last Repricing Date

The date of the last rate change for an adjustable-rate instrument and the origination date for a fixed-rate instrument.

Leaf Fields

Oracle Financial Data Manager (FDM) database fields that are used to define hierarchical segmentations of data (trees). They also define the relationship between the instrument data and the general ledger data in the LEDGER_STAT table.

Leaf ID

A column in the Oracle Financial Data Manager (FDM) database that provides for the creation of hierarchical trees for use in assumptions and reporting. Leaf ID columns also define the relationship between instrument data and ledger data.

Leaf Values

Values that compose the leaf fields.

LEDGER_STAT

A table in the Oracle Financial Data Manager (FDM) database that stores all general ledger as well as statistical information for current and historical periods.

Liquidity Premiums

A charge levied on a long-term instrument to compensate for the illiquidity of the funds.

Long Run Rate

One of the user-defined parameters for the Vasicek (discrete-time) term structure model. It represents the equilibrium value of the one-month annually compounded rate.

Market Price of Risk

In financial economic theory, the market price of risk is a measure of intertemporal risk-aversion of the aggregate investor. For example, a high market price of risk during some future period means that investors will be more risk-averse, and that rates for that term should be higher to compensate for the risk. In practical terms, the market price of risk is the *plug* that makes the price of risk-free bonds correct.

Market Value

In Monte Carlo, the average of the (scenario specific) present values.

Matched Rate Transfer Pricing

A method of transfer pricing where all accounts have transfer rates that reflect their specific maturity and repricing characteristics.

Matched Spread

The interest profit margin for any account. For asset accounts, measured as the note rate minus the transfer rate and, for liability and equity accounts, the transfer rate minus the note rate.

Monthly Rate

The yield on a loan contracted at the beginning of the month for a period of one month, assuming a continuous compounding basis. The monthly rate is a function of time and scenario. The rate generator also computes rates for terms other than a month.

Next Repricing Term

The repricing frequency for an adjustable-rate instrument and the original term to maturity for a fixed-rate instrument

Operating Cost

The non-interest related cost of running a business.

Option Costs

The costs assigned to measure the value of any customer option on an instrument. For example, prepayments on a mortgage loan.

Portfolio Fields

Fields in the Oracle Financial Data Manager (FDM) database that are common to multiple instrument tables. Portfolio fields are determined by the OFS system administrator.

Prepayment

A reduction in the principal balance of a transaction record prior to the contracted schedule date.

Present Value

In Monte Carlo, the sum of cash flows paid by a security along a particular rate scenario, discounted by the stochastic discount factor.

Processing Filter ID

Filter ID used to define which data can go into a processing run.

PSA (Public Securities Association)

A prepayment specification method established by the Public Securities Association that relates a CPR to the age of an instrument.

Reconciliation

The process of comparing information in one data source to information in another data source.

Record

Usually a single account or transaction, or aggregation of accounts, stored in the database (also called a row).

Remote User

A user who is not connected to the client/server environment. A remote user needs to transmit information to the budget administrator using computer files.

Single Rate

An interest rate code with only one point defined. For example, prime rate or LIBOR.

Speed of Mean Reversion

One of the user-defined parameters for the Vasicek and Extended Vasicek (discrete-time) term structure models. Speed of mean reversion represents the long-run drift factor.

Spreadsheet Control Bar

A dialog box that facilitates the definition of a series of input values (dates or numbers) by providing several methods for defining structured patterns in the data.

SQL (Structured Query Language)

The standard method of accessing the Oracle Financial Data Manager (FDM) database.

Stochastic Discount Factor

Present value (along a rate scenario) of one dollar received at some future time. It is a function of future time, option adjusted spread (OAS), and scenario

Transfer Pricing

A method for valuing all sources and uses of funds for a balance sheet.

Transfer Pricing ID

An ID used to specify the method for transfer pricing all balance sheet accounts.

Transfer Pricing Table

An instrument table that contains all of the columns required to run transfer pricing.

Tree ID

Hierarchical structure for leaf fields in OFS products, for example, organization or product type.

UPR (Unscheduled Principal Runoff)

In addition to prepayments, a source of runoff in Risk Manager cash flow calculations. UPR is not applicable for Oracle Transfer Pricing.

Volatility

One of the user-defined term parameters of all (discrete-time) term structure models. It represents a standard deviation of the one-month annually compounded rate.

Yield Curve

The curve of annually compounded zero-coupon bond yield.

Index