Oracle® Identity Manager

Design Console Guide

Release 9.0

B25940-01

May 2006

ORACLE®

Oracle Identity Manager Design Console Guide, Release 9.0

B25940-01

Primary Authors: Vimmika Dinesh, Don Gosselin

Contributors: Jatan Rajvanshi, Raj Kuchi, Semyon Shulman

Contents

5 User Management

6 Resource Management

7 Process Management

8 Oracle Identity Manager (Xellerate) Administration

9 Development Tools

C The Form Version Control Utility

Index

Preface

This preface introduces you to the *Oracle Identity Manager Design Console Guide* discussing the intended audience and conventions of this document. It also includes a list of related Oracle documents.

> **Note:** This is a transitional release following Oracle's acquisition of Thor Technologies. Some parts of the product and documentation still refer to the original Thor company name and Xellerate product name and will be rebranded in future releases.

Audience

Oracle Identity Manager Design Console Guide is intended for users of the Oracle Identity Manager Java Client application. This guide describes the basic functionality of Oracle Identity Manager for both daily and administrative operations. For information on Oracle Identity Manager 's development tools, refer to *Oracle Identity Manager Tools Reference Guide* and the Oracle Identity Manager SDK.

This guide contains information related solely to the behavior of the Java edition of Oracle Identity Manager. For information about the functions and usage of the Oracle Identity Manager Administrative and User Console, refer to the *Oracle Identity Manager Administrative and User Console Guide*.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at

http://www.oracle.com/accessibility/

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an

otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

TTY Access to Oracle Support Services

Oracle provides dedicated Text Telephone (TTY) access to Oracle Support Services within the United States of America 24 hours a day, seven days a week. For TTY support, call 800.446.2398.

Related Documents

This guide assumes that you have read and understood the following documents:

For more information, see the following documents in the Oracle Identity Manager documentation set:

- *Oracle Identity Manager Installation and Upgrade Guide for JBoss*
- *Oracle Identity Manager Installation and Upgrade Guide for WebLogic*
- *Oracle Identity Manager Installation and Upgrade Guide for WebSphere*
- *Oracle Identity Manager Administrative and User Console Customization Guide*
- *Oracle Identity Manager Design Console Guide*
- *Oracle Identity Manager Tools Reference Guide*
- *Oracle Identity Manager Audit Report Developer Guide*
- *Oracle Identity Manager Best Practices Guide*

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager 9.0 documentation set, visit Oracle Technology Network at

`http://www.oracle.com/technology/documentation/index.html`

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Online Help

To access online help for the Oracle Identity Manager Design Console, select Administrator's Guide from the Help menu.

1

The Oracle Identity Manager Architecture

This chapter describes the architecture, benefits, and key features of Oracle Identity Manager. It contains the following topics:

Overview

The Oracle Identity Manager platform automates access rights management, security, and provisioning of IT resources. Oracle Identity Manager instantly connects users to resources they need to be productive and revokes and restricts unauthorized access to protect sensitive corporate information.

Benefits and Key Features

The architecture of Oracle Identity Manager is designed for rapid integration within your business enterprise. It provides the following features:

Scalable Architecture: The J2EE application server model of Oracle Identity Manager provides scalability, fail-over, and load-balancing, and inherent Web deployment. Based on an open, standards-based technology, and featuring a three-tier architecture (the Client application, Oracle Identity Manager supported J2EE-compliant Application Server and ANSI SQL-compliant database), Oracle Identity Manager can provision both LDAP and non-LDAP enabled applications.

Extensive User Management: Oracle Identity Manager includes unlimited user organizational hierarchies and user groups with inheritance, customizable User ID policy management, password policy management, and user access policies that reflect customers' changing business needs. Oracle Identity Manager also provides a resource allocation history, and the ability to manage application parameters and entitlements. Delegated administration is also a key element of user management with comprehensive permission settings.

Web-based User Self-Service: Oracle Identity Manager contains a customizable Web-based user self-service portal with the ability to manage user information, change and synchronize passwords, reset forgotten passwords, request available applications, review and edit available entitlements, and effect or react to workflow tasks.

Powerful and Flexible Process Engine: With Oracle Identity Manager, you can create business and provisioning process models in easy-to-use applications, such as Microsoft Project and Microsoft Visio. Process models include support for approval

workflows and escalations. You can track the progress of each provisioning event, including the current status of the event and error code support. Oracle Identity Manager provides support for complex, branching, self-healing processes, and nested processes with data interchange and dependencies. The process flow is fully customizable and does not require programming.

Comprehensive Reporting for Audit-Trail Accounting: Oracle Identity Manager provides real-time reporting, and up-to-the-minute status reports on all processes with full-state information. In addition, the complete OLAP capability of Oracle Identity Manager supports even the most complex reports, analysis, and dynamic queries.

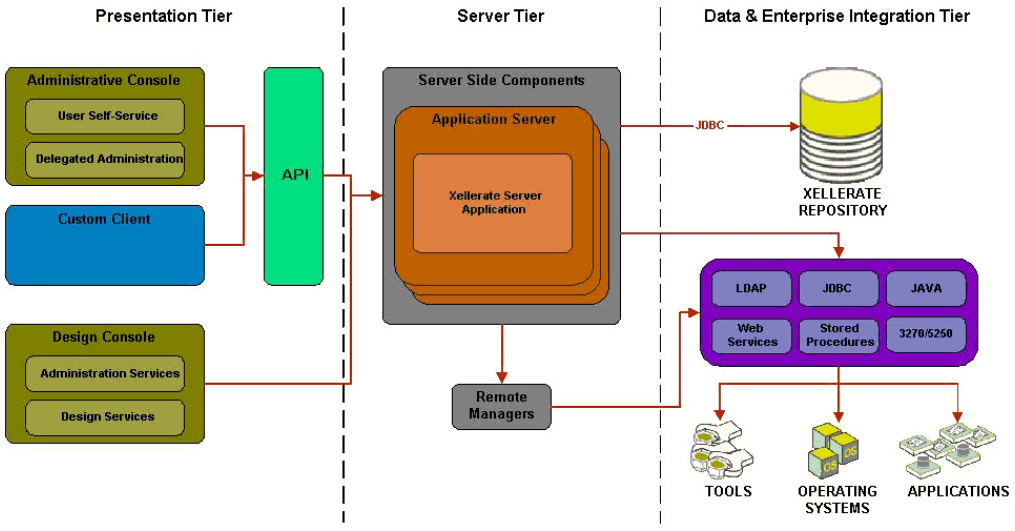
Integration Using the Adapter Factory™: Attempting to support all systems with hand-coded adapters is impractical. Thus, Oracle has developed an automated tool for adapter generation. This tool, the Adapter Factory, supports a wide range of interfaces and virtually any application or device. These adapters run on the Oracle Identity Manager server, and do not require agents to be installed or updated on target platforms. In situations where the target application resource does not have a network-enabled interface, you can create remote integration by using UDDI/SOAP-based support. With the Adapter Factory, integrations that take months to implement can now be accomplished in a few days. Numerous adapters can be generated instantly. With the Adapter Factory, not only can you keep existing integrations updated, you can also support new integration needs quickly. Oracle Identity Manager has the ability to run programs on external third-party systems using the remote managers.

Built-in Change Management: Oracle Identity Manager enables you to package new processes, import and export existing ones, and move packages from one system to another.

The Three Tiers of Oracle Identity Manager

The Oracle Identity Manager architecture consists of three tiers, as shown in Figure 1–1.

Figure 1–1 Oracle Identity Manager Three-Tier Architecture



Tier 1: Client

The first tier provides two distinct interfaces, the Java Administrative and User Console applications.

> **Note:** This guide contains information related solely to the behavior of the Design Console edition of the Oracle Identity Manager product. For information on the functions and usage of the Oracle Identity Manager Administrative and User Console, refer to the *Oracle Identity Manager Administrative and User Console Guide*.

The Oracle Identity Manager application GUI component reside in this tier. Users login by using the Oracle Identity Manager client. By doing so, the Oracle Identity Manager client interacts with the Oracle Identity Manager server, providing it with the user's login credentials. The Oracle Identity Manager server then validates these credentials. In addition, through the Oracle Identity Manager client, you can submit requests to search for information in the database as well as save, edit, or delete that information.

Tier 2: Application Server

The second tier implements the business logic, which resides in the Java Data Objects that are managed by the supported J2EE application server (JBoss application server, BEA WebLogic, and IBM WebSphere). The Java Data Objects implement the business logic of the Oracle Identity Manager application, however, they are not exposed to any methods from the outside world. Therefore, to access the business functionality of Oracle Identity Manager , you can use the API layer within the J2EE infrastructure, which provides the lookup and communication mechanism.

The Oracle Identity Manager supported J2EE-compliant application server is the only component that interacts with the database and is responsible for:

- **Logging into Oracle Identity Manager**: The Oracle Identity Manager supported J2EE-compliant application server connects the Oracle Identity Manager client to the database.
- **Handling Client Requests**: The Oracle Identity Manager supported J2EE-compliant application server processes requests from the Oracle Identity Manager client. It then sends the appropriate information from these requests to the database. The Server also delivers responses from the database to the client.
- **Scalability (Connection Pooling/Sharing)**: The Oracle Identity Manager supported J2EE-compliant Application Server supports single- or multi-application usage in a manner that is transparent to Oracle Identity Manager clients. Connection pooling improves database connectivity performance and dynamically resizes the **connection pool** by optimizing resources for usage scalability.
- **Securing System-Level Data (Metadata)**: Oracle Identity Manager employs **row-level** security to prevent unauthorized access by users who might otherwise accidentally delete or modify system-level information (system metadata).

Note: If an unauthorized user attempts to add, modify, or delete system-level information, the following message is displayed:

"**The security level for this data item indicates that it cannot be deleted or updated.**"

Tier 3: Database

The third tier consists of the database. This is the layer that is responsible for managing the storage of data within Oracle Identity Manager.

2

Starting Oracle Identity Manager

This chapter describes the procedure to start Oracle Identity Manager. It contains the following topics:

Overview

This section describes the steps to start Oracle Identity Manager.

Starting Oracle Identity Manager

1. Double-click the **Oracle Identity Manager** icon on the desktop. The Login window is displayed.

   Note: Your user ID and password cannot have special characters, such as: % + = , \ ‘ “ < > / |

2. Enter your user ID and password.

   Note: Your password appears as asterisks (****) for security purposes.

3. Click **Login**. The Oracle Identity Manager main screen is displayed.

   Note: You can also access the basic features of Oracle Identity Manager by using the Oracle Identity Manager Administrative and User Console. For more information on what features are available through the Oracle Identity Manager Administrative and User Console, refer to the *Oracle Identity Manager Administrative and User Console Guide.*

After you log in to Oracle Identity Manager, configure the system settings. These settings control the system-wide behavior of Oracle Identity Manager and affect its users. For a description of each of these settings and instructions on how to set it, refer to Chapter 8, the "The System Configuration Form" section.

3

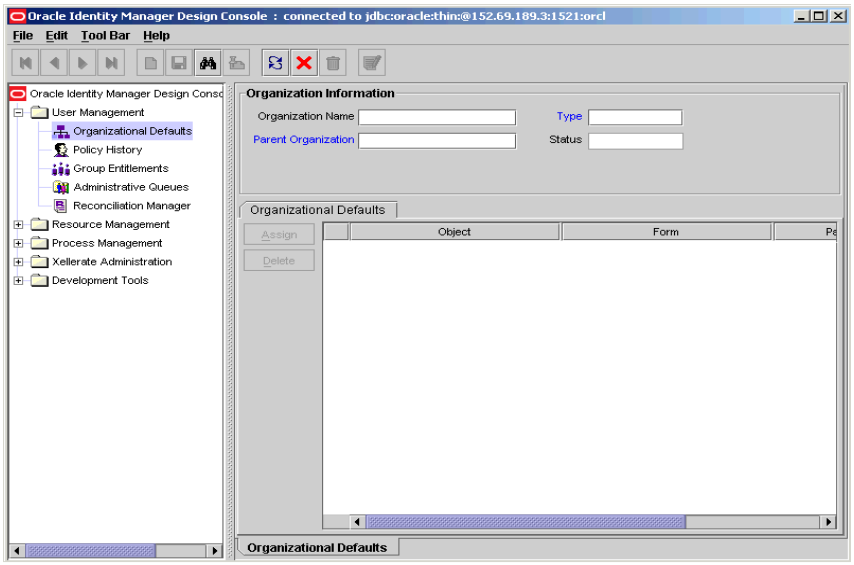
The Oracle Identity Manager Main Screen

This chapter describes the main screen in Oracle Identity Manager. It contains the following topics:

Overview

You can create, track, and analyze a business process by using the main screen in Oracle Identity Manager, as shown in Figure 3–1.

Figure 3–1 Oracle Identity Manager Main Screen



The Oracle Identity Manager main screen consists of four regions:

- "The Oracle Identity Manager Menu Bar" on page 3-2
- "The Oracle Identity Manager Toolbar" on page 3-3

- "The Oracle Identity Manager Explorer" on page 3-5
- "The Oracle Identity Manager Workspace" on page 3-6

Each of these regions is covered in greater detail in the sections that follow.

The Oracle Identity Manager Menu Bar

The Oracle Identity Manager Menu Bar is located at the top of the Oracle Identity Manager main screen. It contains the menus that enable you to perform all operations within the Oracle Identity Manager GUI.

To select a menu, click it. Once a menu is selected, a list of menu items is displayed. By selecting a menu item, you can perform the action associated with that menu item. For example, to print the contents of the active form, you select the **Print** item from the **File** menu.

As an alternative to the mouse, you can use either keyboard shortcuts (for example, **ALT+F** for the **File** menu) or shortcuts keys (for example, **Ctrl+P** to print the active form). The keyboard shortcuts and shortcut keys that are available are displayed in black, and disabled shortcuts and keys appear in gray.

The Oracle Identity Manager Menu Bar provides 4 menus: File, Edit, Toolbar, and Help. This section describes the following topics:

- "File Menu" on page 3-2
- "Edit Menu" on page 3-2
- "Toolbar Menu" on page 3-3
- "Help Menu" on page 3-3

File Menu

The **File** menu provides the following menu options:

Menu Item	Action
Print	Print the active form
Login	Log out of Oracle Identity Manager, and then log in again
Exit	Exit Oracle Identity Manager

Edit Menu

The **Edit** menu provides the following clipboard options:

Menu Item	Action
Cut	Cut selected text from editable fields, and copy it to the system Clipboard.
Copy	Copy the selected text to system Clipboard.
Paste	Paste text from the system Clipboard to the selected field.
Clear	Clear the selected text.

Toolbar Menu

The **Toolbar** menu is made up of menu items that comprise the Oracle Identity Manager Toolbar.

Menu Item	Action
New	Clear the contents of the active form.
Save Changes	Save all changes made to the active form.
Query	Execute a query on the active form.
Notes	Display any notes that may be attached to the active form.
Refresh	Refresh the record of the active form.
Close	Close the active form.
Delete	Delete the current record.
Next	Display the next record, when you have queried more than one record.
Previous	Display the previous record, when you have queried more than one record.
First	Display the first record, when you have queried more than one record.
Last	Display the last record, when you have queried more than one record.
Close All	Close all open forms, and clear the Oracle Identity Manager Workspace.

Help Menu

The **Help** menu provides access to the Oracle Identity Manager Design Console online Help system and about the copyright information.

Menu Item	Action
Administrator Guide	Display the online Help equivalent of the *Oracle Identity Manager Administrative and User Console Guide*.
About	Display the copyright information about Oracle Identity Manager Design Console.

Note: By accessing the **Help** menu of the Oracle Identity Manager Web Application, and selecting the **User Guide** command, you can see the online Help equivalent of the *Oracle Identity Manager Administrative and User Console Guide*.

The Oracle Identity Manager Toolbar

Figure 3–2 displays the Oracle Identity Manager Toolbar.

Figure 3–2 Oracle Identity Manager Toolbar

The Oracle Identity Manager Toolbar is a series of buttons, located below the Oracle Identity Manager Menu Bar. These buttons always provide single-click access to frequently used actions. The Toolbar buttons are always applied to the active form.

> **Tip:** When you hold the mouse over a Toolbar button for a few seconds, a tooltip appears, containing a description of that button.

The following table provides a list of the buttons that comprise the Oracle Identity Manager Toolbar, along with descriptions of the actions these buttons perform.

Button	Action
First	Display the first record, when you have queried more than one record.
Previous	Display the previous record, when you have queried more than one record.
Next	Display the next record, when you have queried more than one record
Last	Display the last record, when you have queried more than one record.
New	Clear the active form.
Save	Save all changes made to the active form.
Query	Execute a query on the active form.
Notes	Display any notes that may be attached to the active form.
Refresh	Refresh the active form.
Close	Close the active form.
Delete	Delete the current record.
Prepopulate	Populate designated fields with data. These fields are user-defined, and have prepopulate adapters attached to them. **Note**: For more information on prepopulate adapters, refer to the *Tools Reference Guide*.

Oracle Identity Manager Shortcuts

Besides the Oracle Identity Manager Toolbar and Oracle Identity Manager Menu Bar, Oracle Identity Manager provides the following keyboard shortcuts that perform functions quickly or provide you with easy access to menus.

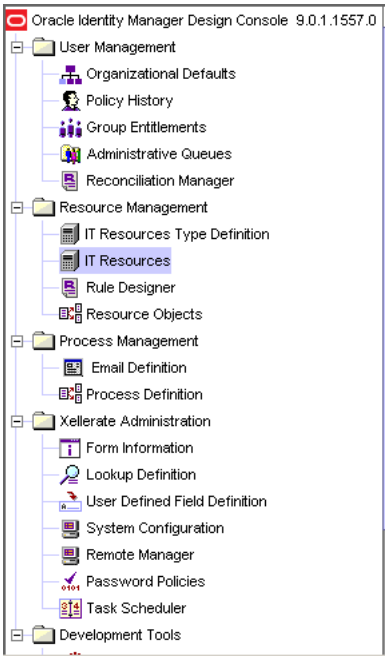
Shortcut Name	Keystroke Combination	Description
File Menu	ALT+F	Activate the **File** Menu.
Edit Menu	ALT+E	Activate the **Edit** Menu.
Toolbar Menu	ALT+T	Activate the **Toolbar** Menu.
Help Menu	ALT+H	Activate the **Help** Menu.
Print	CTRL+P	Print the active form.
Cut	CTRL+X	Cut selected text from editable fields, and copy it to the system Clipboard.
Copy	CTRL+C	Copy the selected text to system Clipboard.

Shortcut Name	Keystroke Combination	Description
Paste	CTRL+V	Paste text from the system Clipboard to the selected field.
Clear	CTRL+DEL	Clear the selected text.
New	CTRL+N	Clear the active form.
Save Changes	CTRL+S	Save all changes made to the active form.
Query	CTRL+Q	Execute a query on the active form.
Notes	CTRL+SHIFT +N	Display notes that are attached to the active form.
Refresh	CTRL+R	Refresh the active form.
Close	CTRL+W	Close the active form.
Delete	CTRL+D	Delete the current record.
Next	Numpad + (plus)	Display the next record, when you have queried more than one record.
Previous	Numpad - (minus)	Display the previous record, when you have queried more than one record.
First	CTRL+F	Display the first record, when you have queried more than one record.
Last	CTRL+L	Display the last record, when you have queried more than one record.
Prepopulate	CTRL+U	Populate designated fields of a customized form with data.
Help	F1	Launch context-sensitive Help for the active form.
Explorer	F3	Highlight the Oracle Identity Manager icon, which appears at the top of the Oracle Identity Manager Explorer.
Lookup	F4	Display the Lookup window for the selected lookup field.
Menu	F10	Activate the **File** menu.

The Oracle Identity Manager Explorer

Figure 3–3 describes the Oracle Identity Manager Explorer.

Figure 3–3 Oracle Identity Manager Explorer



The Oracle Identity Manager Explorer contains a list of form icons. These icons represent the Oracle Identity Manager forms that you have permission to access. To launch a form, click the plus icon, which appears to the left of the folder that contains the desired form. Then, double-click the appropriate icon, and the corresponding form appears in the Oracle Identity Manager Workspace.

Note: The Oracle Identity Manager Explorer is customizable by your System Administrator. Depending on the permissions you were given, different icons appear in the Oracle Identity Manager Explorer. If you do not see a particular form icon, then contact your System Administrator.

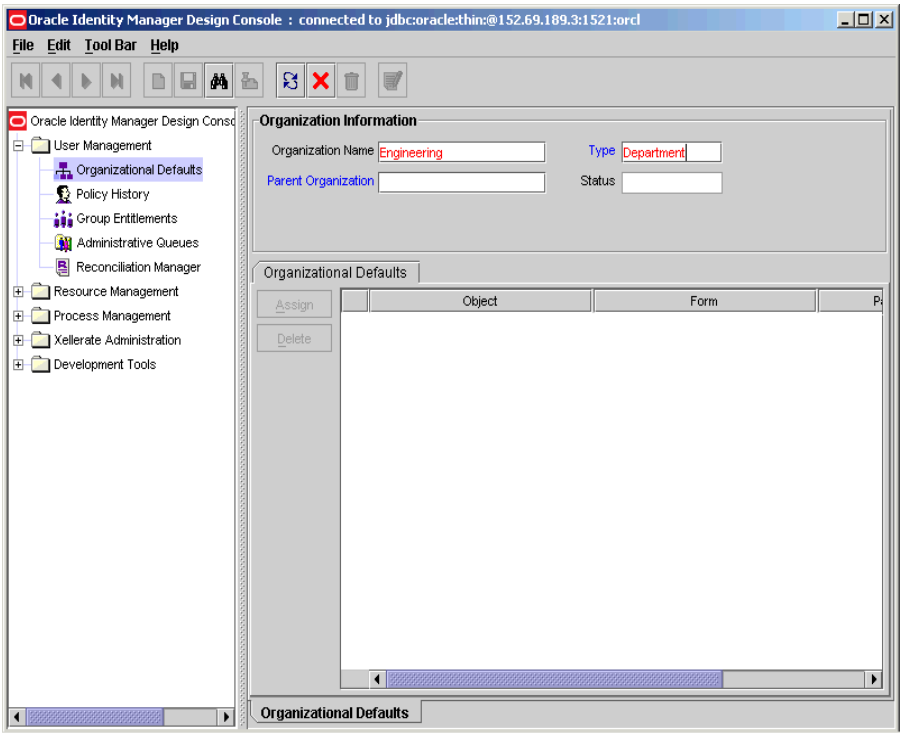
Tip: When you right-click the Oracle Identity Manager logo at the top of the Oracle Identity Manager Explorer, the **Refresh Explorer** menu command appears within a pop up window. When you click this command, Oracle Identity Manager updates and refreshes the Oracle Identity Manager Explorer with all forms to which you have access. This is useful when the System Administrator has changed your permissions.

Tip: You can adjust the size of the Oracle Identity Manager Explorer by dragging the Split Bar to the right or left. The Split Bar is the vertical line separating the Oracle Identity Manager Explorer from the Oracle Identity Manager Workspace.

The Oracle Identity Manager Workspace

Figure 3–4 describes the Oracle Identity Manager Workspace.

Figure 3–4 Oracle Identity Manager Workspace



The Oracle Identity Manager Workspace is the region of the Oracle Identity Manager main screen in which all forms accessed using the Oracle Identity Manager Explorer appears. If multiple forms are accessed, then Oracle Identity Manager places the active form on top and layers the remaining forms on readily accessible tabs (located along the bottom edge of the main screen). To switch between forms, click the desired form's tab, located at the bottom of the form.

Oracle Identity Manager is capable of displaying each form as two distinct views: a form view and a table view. The differences between the information presented in each view are explaing below:

Form View

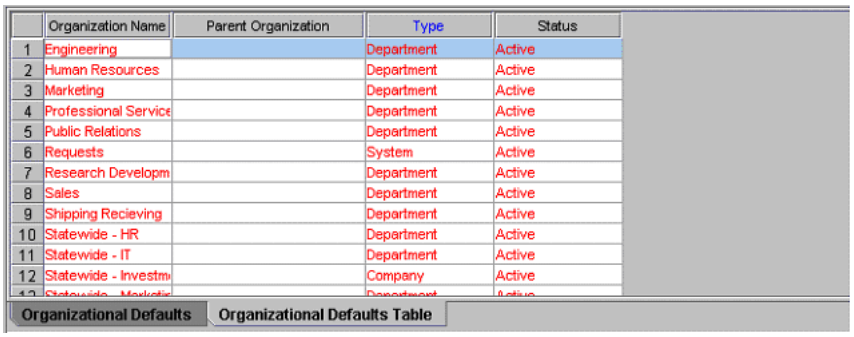
A form view provides detailed information about a single record. The form view is the view displayed whenever a form is initially accessed using the Oracle Identity Manager Explorer (for example, before a query has been performed).

Table View

A table view lists general information related to multiple records of a form. When a user submits a query, and that query produces more than one result, Oracle Identity Manager automatically displays a table containing all records that match the criteria of the search.

In the example below, a query of the **Organizations** form has returned a result containing several records. Notice that both the form and table view tabs of the **Organizations** form are displayed. Figure 3–5 displays the Table View of Oracle Identity Manager.

Figure 3–5 Table View



There are several standard usage and display conventions that apply to all table views:

- To select any record in a table view, click it.
- The data associated with any given record is displayed in cells. These cells are also referred to as fields.
- Oracle Identity Manager forms contain **column headers** (a gray box with a label above each column) that display the name of the column. If a particular column is equipped with a Lookup dialog box, the column header text appears in blue.
- Oracle Identity Manager forms contain **row headers** (a gray box with a numeric label at the beginning of each row). To view the detailed form view of any given record, double-click its row header. You can also display a record within the form view by selecting the desired record in the table view, and then clicking the applicable form tab at the bottom of the Oracle Identity Manager Workspace.
- If a query returns more records than can be displayed within the Oracle Identity Manager Workspace, a vertical scrollbar appears along the right edge of the table view. Click the **Up** or **Down** arrows in the vertical scrollbar to scroll through the records of the table.
- If the table view contains more columns than can be displayed within the Oracle Identity Manager Workspace, a horizontal scrollbar appears along the bottom edge of the table view. Click the **Left** or **Right** arrows in the horizontal scrollbar to reveal additional columns not initially visible within the Oracle Identity Manager Workspace.
- The record information presented within the individual cells (fields) of the table view may be edited by the user. To edit the information in a particular field, click it, and make the desired changes. For fields that are equipped with Lookup dialog boxes (i.e. text appears in blue), double-click the field to access its Lookup dialog box. Then, select the desired value. When you edit the value in any field of a record, the row header for that record changes to **black**. This indicates that data in that field has been changed and must be saved to the database.
- To select multiple, consecutive record rows simultaneously, use the **SHIFT** key.
- To select multiple, non-consecutive record rows simultaneously, use the **CTRL** key.
- To export a record, right-click its row header (to select more than one record, use the **SHIFT** key first). A popup dialog box is displayed.
- If you select **Copy to Clipboard**, then it copies the selected records to the Clipboard. You can then paste the selected records into an MS Excel spreadsheet or an MS Word document.

- If you select **Copy to File**, the this option allows you to save the record(s) as a 'tab' delimited file.
- The order in which the records in a table view are displayed can be controlled using the sort feature. To adjust the sort order of displayed records, click the header of the column by which you wish the records to be sorted. Notice that a small triangle appears beside the column header text. This indicates the direction (ascending or descending order) in which the records were sorted.

4

Basic Functionality of Oracle Identity Manager

This chapter describes how to use several features of Oracle Identity Manager. The behavior of these features is standard for all forms. It is therefore recommended that you review and understand this section before proceeding on to further sections. This chapter contains the following sections:

Special Field/Form Types

Oracle Identity Manager forms are designed to utilize standard conventions so that they are easy to use. As a number of these conventions may be unfamiliar to new users, they have been presented here for reference. In addition, there are a number of field and window types employed throughout the Oracle Identity Manager main screen, which have specific capabilities or behavior for displaying data.

Data Fields

Data fields are display areas within Oracle Identity Manager forms used to present text information related to a given record (for example, the First Name field on the Users form).

The *label* of a particular field may be displayed in one of two colors (black or blue).

- A **black** label denotes that this field is a standard field. You can perform a query, or create, modify, or delete information within this type of field.
- A **blue** label denotes that the data in this field is derived from a pre-defined list of values supplied using a Lookup or Date & Time window. When you double-click this type of field, the applicable Date & Time window or Lookup window is displayed. You can then select a date, time, or a lookup value.

The *value* of a particular field may be displayed in one of two colors (black or red) to denote the type of data being displayed in it.

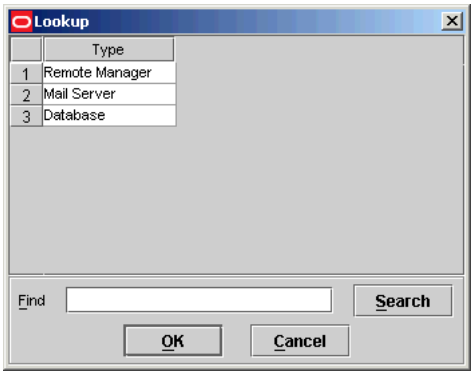
- If the field value is displayed in **black**, then it signifies that the data in this field is provided by the user. You can perform queries on or edit the information in these types of fields.
- If the field value is displayed in **red**, then it signifies that the data in this field is system-generated and auto-provided by Oracle Identity Manager. In addition,

values of this type are read-only. This preserves data integrity and prevents users from accidentally overwriting critical information.

Lookup Fields

Figure 4–1 displays the Lookup dialog box. From the Lookup dialog box, select a value (by clicking it), and click **OK**. Or, click **Cancel** to close the Lookup window without selecting anything.

Figure 4–1 The Lookup Dialog Box



Note: You can display the Lookup window for a lookup field by selecting the field and pressing the **F4** key.

When the Lookup dialog box displays a long list of values, you can search the list by entering the first few characters of the value you need, followed by a wildcard (*) in the **Find** box. Then, click **Search** to refresh the Lookup dialog box with the results matching your search.

Date And Time Fields

The Date & Time window is available for fields, which require a calendar date or time value. This window is activated automatically whenever you double-click a field equipped with it. When displayed, it allows the user to select a month, year, date, and time.

Note: You can display the Date & Time window by selecting the desired field and pressing the **F4** key.

To select a Date and Time, perform the following steps:

1. Double-click the field into which you want to enter a date and time. The Date & Time window is displayed.
2. Click the combo box. From the pull-down menu that is displayed, select the desired month.
3. From the **Date** scroll box, select the desired year
4. Click the desired date on the calendar.
5. From the Time scroll box, select the desired time

6. Click **OK** to save your changes to the database. The Date & Time window disappears. The field that you double-clicked in Step 1 now displays the date and time you selected.

Note: Click **Cancel** to exit without saving changes to the database.

Combo Box

Certain fields are equipped with pull-down menus, known as combo boxes. Combo boxes contain a list of pre-defined values. When you click a combo box, its values are displayed. If the list contains more values than can be displayed at one time, a vertical scrollbar appears to the right of the list.

When you select a value, the list disappears, and the selected value is displayed within the combo box.

Note: Combo boxes are similar to Lookup windows, except there are no querying capabilities and the values appear only within one column.

Notes Window

The Notes window contains additional data related to the current record. In addition, when used with adapters, this window displays the code Oracle Identity Manager generated while compiling the adapter.

Note: For more information on adapters, refer to *Oracle Identity Manager Tools Reference Guide*.

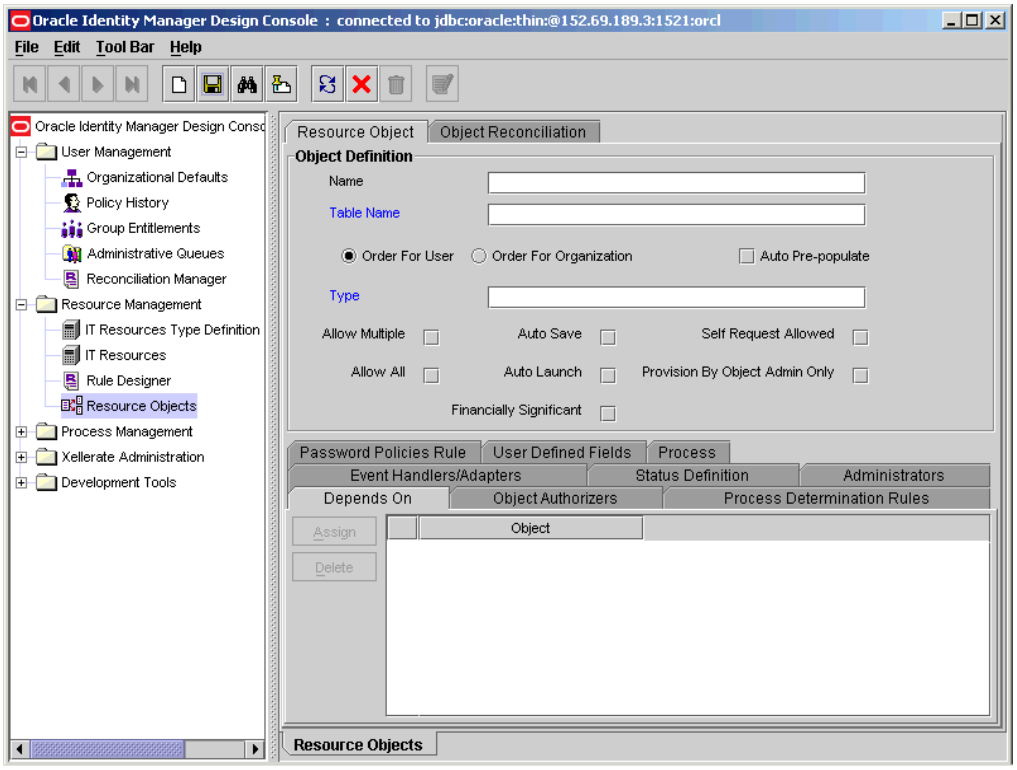
To use the Notes window to enter supplemental information for a record, perform the following steps:

1. Query for the desired record.
2. Click the **Notes** button. The Notes window is displayed.
3. Enter the information into the text area of the Notes window.
4. Click the icon that represents a man to store your information into the Notes window. Or, click **Close** to close the Notes window without storing your information.
5. From the Toolbar, click the **Save** button. The information you entered into the Notes window is saved to the database.

Note: If the Notes button is red, the current record already has additional information associated with it. To view this information, click the button. You may also enter supplemental information. Each entry receives a unique date, time, and user stamp, which allow the history of entries to be tracked.

Tabs On Forms

Figure 4–2 Oracle Identity Manager Design Console - Tab on Forms



Most Oracle Identity Manager forms are comprised of multiple tabs. The tabs are generally located in the lower region of the form, and are used to display additional information related to a particular record (for example, the users who are employed at an organization), as shown in Figure 4–2.

In addition, each tab is often equipped with its own tables and function buttons (generally, the buttons on a tab are not enabled until the information in the upper portion of the form is saved). The table displayed on the tab is used to view and edit records associated with that tab item. To modify information within a row of a tab's table, you may either double-click the field that contains the information you wish to edit, or double-click the associated row header.

Assignment Windows

The User Form Assignment window allows the easy selection and assignment of available entities to a given record. The Assignment window is displayed whenever the you click the **Assign** button.

The left panel of this dialog box lists all items that can be assigned to the record (for example, Organization). The right panel lists all items that have already been assigned to the record. In this example, the Assigned Forms objects is available for assignment.

- To select multiple non-consecutive items simultaneously (for example, the User Group, IT Resource Type Definition, and Form Information objects, but not the Process Definition object), hold down the **CTRL** key while selecting items with the mouse.

- To select multiple items that are listed consecutively (for example, the Organization, Users, and User Group objects), hold down the **SHIFT** key and select the first and last items with the mouse.
- To assign one or more items, select it (so that it is highlighted), and click

- To unassign one or more items that have been assigned already, select it, and click

When you have assigned and/or unassigned items, click **OK**. If you click **Cancel**, all assignment changes you made are discarded.

Although the values available for selection in the left and right panels are unique to what is being assigned or unassigned, the buttons and general use of this dialog box are consistent throughout the application.

Querying Capabilities

Oracle Identity Manager provides users with the ability to perform searches (also referred to as "queries") for records that have been stored in the database. Every form within Oracle Identity Manager comes equipped with the search feature. The search feature is invoked by clicking the

on the Toolbar. Searching is also available from within lookup fields.

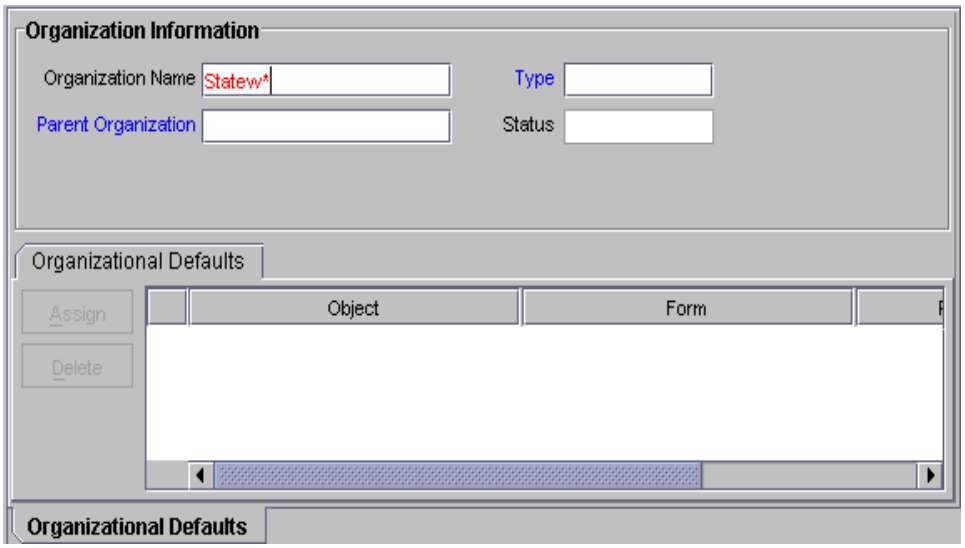
Constructing a Search Query

You can also filter the search criteria in a form field. This causes Oracle Identity Manager to limit the results returned to those records, which match the criteria you entered. If you leave all form fields blank prior to conducting the search, all records in the table are returned.

To further control the records that are retrieved, you can fine-tune the search criteria by using a wildcard. The asterick (*) wildcard character is used to represent unspecified portions of search criteria. You can use this character at the beginning, middle, or end of the value you are entering within a given field. For example, if you enter B* in the Location field of an Oracle Identity Manager form and execute a search, you retrieve all records with locations that begin with the letter B (for example, Burbank, Boston, Bristol, etc.). If the * character is placed in the middle or a search value, as in Br*on, you retrieve all records that begin with BR and end with ON (for example, *Brighton, Boston*, etc.) If you place the * character at the end of the search value, as in *A, you retrieve all records that end in A (for example, *Philadelphia, Tampa*, etc.).

In the example below, a query is being performed on the Organizational Defaults form and the Organization Name field is being used to filter the search criteria. The limiting criteria being specified are "*Statew*;" therefore, only those organizations with names that begin with Statew are retrieved from the database, as shown in Figure 4–3.

Figure 4–3 Displaying the Results of a Search Query



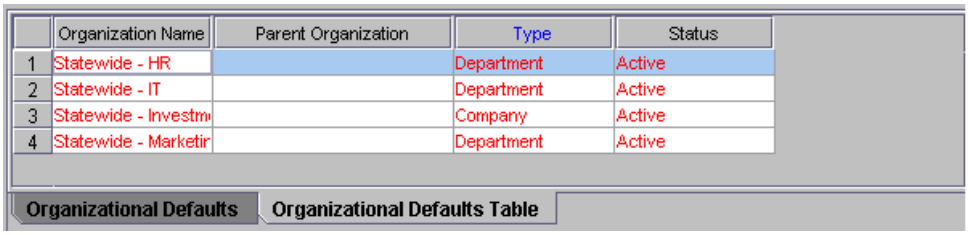
Executing the Search

After all of the desired criteria have been entered in the various fields on which the query is being performed, click

(or press Ctrl+Q).One of the following actions occurs:

- **No records are returned**. No records in the database matched your search criteria for this form. Modify your search criteria. This result may also signify that the record for which you are searching no longer exists in the database
- **One record is returned.** Only one record in the database has matched your search criteria. The Form view displays that record.
- **More than one record is returned.** Multiple records in the database have matched your search criteria. A Table view, containing all records that meet your search criteria, is displayed. In addition, the first record in the retrieved set of records appears in the Form view, as shown in Figure 4–4.

Figure 4–4 Multiple Records Returned



Query Results Set

If you perform a query, and multiple records in the database match your search criteria, you may wish to see detailed information about each record. When this occurs, Oracle Identity Manager provides you with several directional buttons, which

can assist you when viewing these records within the Form view. These directional buttons, referred to as VCR buttons, are located in the Toolbar. They are described below:

Buttons	Description
	When clicked, Oracle Identity Manager displays the first record in the result set in the Form view.
	When clicked, Oracle Identity Manager displays the preceding record (according to the display sequence in the Table view) in the result set in the Form view.
	When clicked, Oracle Identity Manager displays the next record (according to the display sequence in the Table view) in the result set in the Form view.
	When clicked, Oracle Identity Manager displays the last record in the result set in the Form view

Optimizing Query Performance

As certain queries may retrieve an exceptionally large result set, and thus require significant time to execute and/or consume your computer's resources, it is important to optimize query performance. To optimize performance, employ the following search techniques:

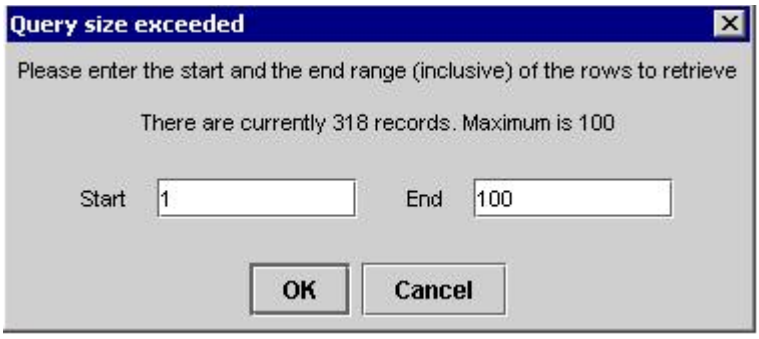
- Define the scope of a search strategy as precisely as possible. Enter the most specific information needed to retrieve the desired record(s) when constructing your query. For example, if the first name of a contact is JOHN and his last name is JACKSON, be sure to enter both pieces of information when defining the search criteria (rather than merely entering a search for all contacts with the last name JACKSON).
- Employ the * wildcard character wherever possible (for example, on specific fields to refine the scope of your search). If you place the * wildcard in front of an alphabetical character (for example, "*A"), a particular field reduces the number of records retrieved (as opposed to leaving the value in a given field blank).

Note: For more information on indexes, consult your System Administrator.

Result Set Exceeds Limit

If you have both read- and write-access to all forms and record within Oracle Identity Manager (i.e., the System Administrator) in the System Configuration form, then this enables you to set the maximum number of records that may appear in the result set for a search. If the set of records retrieved for a search exceeds this value, Oracle Identity Manager displays the Query Size Exceeded dialog box, as shown in Figure 4–5.

Figure 4–5 The Query Size Exceeded Dialog Box



You are then prompted to enter a specific range or subset of the result set to be viewed. In the example above, the maximum result set of 100 has been exceeded, though it is specified that only records 1 through 100 are to be displayed.

Note: For more information on the System Configuration form, refer to "The System Configuration Form" on page 8-14.

5

User Management

This chapter describes the details of managing the user in Oracle Identity Manager. It contains the following topics:

Overview

The User Management folder provides System Administrators with the tools necessary to create and manage information pertaining to your company's organizations, users, user groups, requests, form templates, locations, process tasks, and reconciliation events.

This folder contains the following forms:

- **Organizational Defaults**: This form is used to view the organization records that reflect the internal structure of your enterprise as well as designate other information related to these entities.
- **Policy History**: This form is used to view the user records that your employees require.
- **Group Entitlements**: This form is used to view the records of collections of users to whom you may assign some common functionality. These collections of users are known as **user groups**.
- **Administrative Queues**: This form is used to create and manage mass-assignment privileges of user groups for other Oracle Identity Manager forms.
- **Reconciliation Manager**: This form is used to manage reconciliation in Oracle Identity Manager.

Organizational Defaults Form

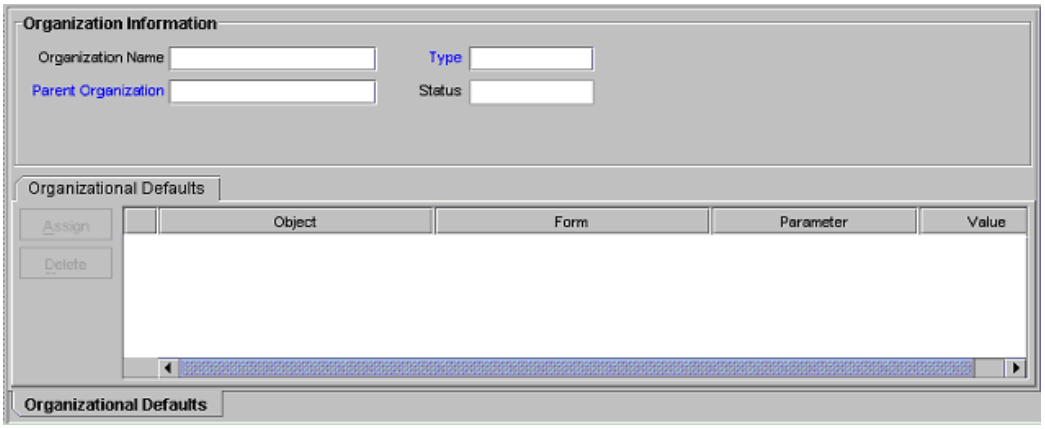
The Organizational Defaults form is located in the User Management folder. It is used to view the organization records that reflect the internal structure of your enterprise as well as designated other information related to these entities. An organization record contains information related to an organizational unit within an enterprise's hierarchy,

such as a company, department, or branch. A sub-organization is an organization, which is a member of another organization, (for example, a department within a company). The organization to which the sub-organization belongs is also referred to as a Parent Organization.

The Organizational Default tab is used to specify default values for parameters on the custom process form of resources that can be provisioned for the current organization. Each process form is associated with a resource object that has either been allowed for the organization or has the Allow All check box on the associated Resource Objects form selected.

The values specified in the Process Defaults tab are used as the default values for all users within the organization.

Figure 5–1 The Organizational Defaults Form



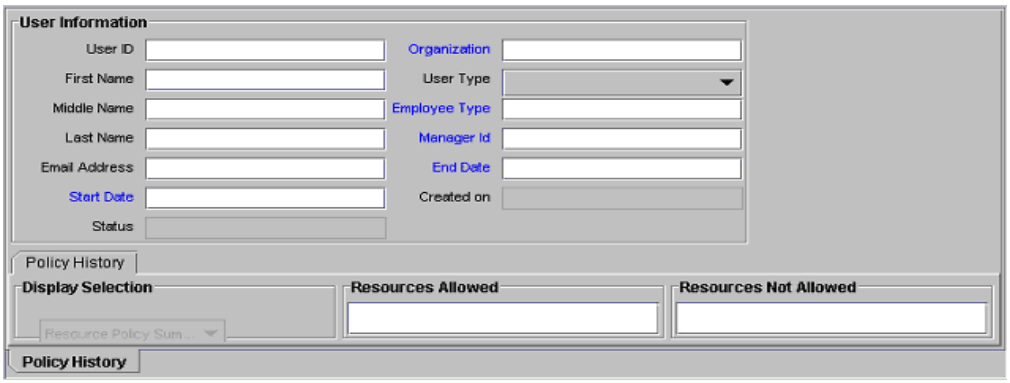
Now that we have reviewed organizations, you will learn about the data fields of the Organizational Defaults form. The following table describes the data fields of this form.

Field Name	Description
Organization Name	Name of the organization.
Type	The classification type of the organization (for example, *Company*, *Department*, *Branch*).
Status	The current status of the organization (*Active*, *Disabled*, or *Deleted*).
Parent Organization	The organization of which this organization is a member. If an organization appears in this field, this organization appears on the Sub Organizations tab of that parent organization. When no value is specified in this field, this organization does not belong to any other organization (i.e., it is a top-level organization).

The Policy History Form

The Policy History form is used to view information related to user records. Specifically, the resources that are allowed or disallowed for the user.

Figure 5–2 The Policy History Form



There are two types of users within Oracle Identity Manager:

- **End-User Administrators**. Users with this type of Oracle Identity Manager account are able to access both editions of the Oracle Identity Manager interface (for example, the Java Client and the Administrative and User Console). Based on the permissions assigned by the System Administrator, End-User Administrators have access to a subset of the forms available within the Java Client.
- **End-Users**. Users with this type of Oracle Identity Manager account are able to access only the Administrative and User Console edition of the Oracle Identity Manager interface and generally have a lesser set of permissions than End-User Administrators. Only those resource objects that are defined as self-serviceable on the Objects Allowed tab of the user's organization will be available for provisioning requests using the Administrative and User Console.

Now that we have reviewed about users, you will learn about the data fields of the Policy History form. The following table describes the data fields of this form.

Field Name	Description
User ID	The user's Oracle Identity Manager login ID.
First Name	The user's first name.
Middle Name	The user's middle name.
Last Name	The user's last name.
Email	The user's e-mail address.
Start Date	The date on which the user's account will be activated.
Status	The current status of the user (Active, Disabled, or Deleted).
Organization	The organization to which the user belongs.
User Type	The user's classification status. Valid options are End-User Administrator and End User. Only End-User Administrators have access to the Java Client edition of the Oracle Identity Manager interface.
Employee Type	The employment status of the user at the parent organization (for example, Full-Time, Part-Time, Intern, etc.).
Manager ID	The user's manager
End Date	The date on which the user's account will be deactivated.
Created on	The date and time that the user record was first created.

Policy History Tab

This tab is used to view the resource objects that are allowed or disallowed for the user based on:

- The access policies that are applicable to the user group to which they belong.
- The resource objects that have been allowed by the organization of which they are a member.

The Policy History tab has a Display Selection region. By accessing the upper-most combo box from this region, and selecting one of its menu items, you can determine how Oracle Identity Manager will organize the contents that appear within this tab.

If you select the Resource Policy Summary menu item, the resource objects that are allowed and/or disallowed based on a combination of the user's organization and applicable access policies is displayed.

By selecting the Not Allowed by Org menu item, the only resource objects that appear are those that are disallowed, based on the user's organization.

If you select the Resources by Policy menu item, a second combo box is displayed. This combo box contains the access policies that apply to the user groups of which the user is a member. By selecting an access policy from this combo box, the resource objects that are allowed or disallowed for the user, based on this access policy, is displayed.

Oracle Identity Manager also provides you with a tracking system, designed to see the resources that have been allowed or disallowed for a user, based on the organizations of which the user is a member, and/or the access policies that apply to the user.

The resource objects that are allowed for the user appear in the Resources Allowed list. The resource objects that are disallowed for the user are displayed in the Resources Not Allowed list. Resource objects that are displayed in the Resources Allowed list merely represent the resource objects with which the user can be provisioned. It does not represent the resource objects with which the user is provisioned.

To view this tracking system, click the Policy History button (which appears within the Display Selection region of the Policy History tab). The User Policy Profile History window is displayed.

From this window, by selecting:

- The desired date (from the History Date combo box);
- Whether you want Oracle Identity Manager to display resources with which has been allowed or disallowed, based on the organizations of which the user is a member, the access policies that apply to the user, or both (from the Display Type combo box); and
- The specific access policy, which determines the resource objects that are allowed and/or disallowed for the user (from the Policy combo box),

You can see the resources that have been allowed or disallowed for a user for the date and time you selected.

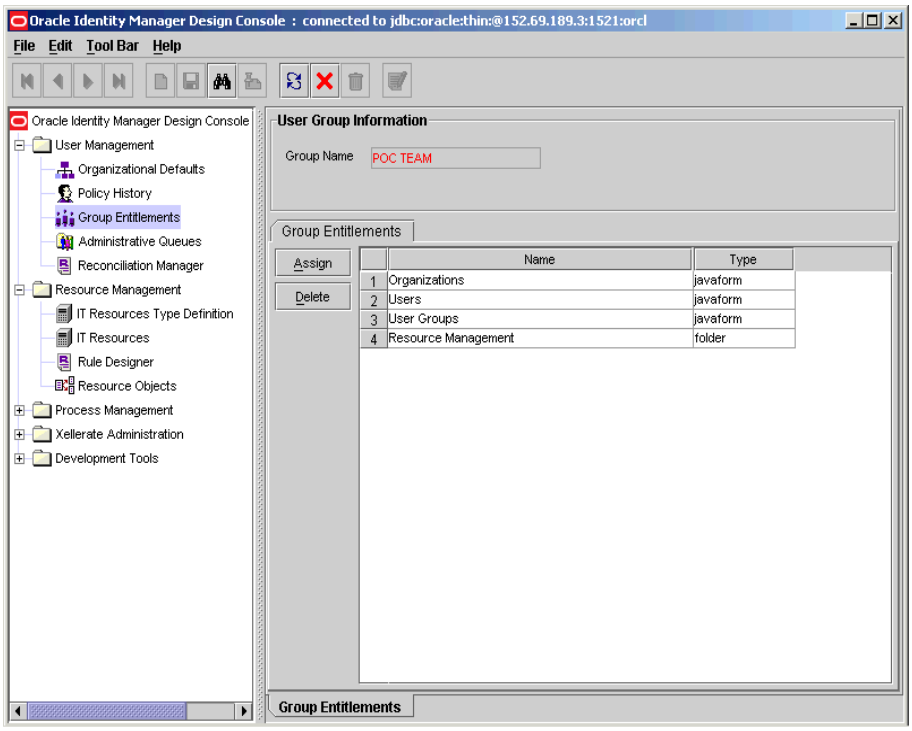
Group Entitlements Form

The Group Entitlements form is located in the User Management folder. It is used to designate the Oracle Identity Manager forms and folders that members of a user group can access through the Oracle Identity Manager Explorer.

Assigning Group Entitlements

> **Note:** You can use the Group Entitlements form to create and move forms.

1. Open the Group Entitlements form. The User Group Information dialog box is displayed.
2. In the **Group Name** field, enter the name of the user group.
3. Click **Assign**. The User Form Assignment lookup table is displayed.
4. From the lookup table, select the user form for this user group. Use the **Arrow** button(s) to either add or delete from the **Assigned Forms** list.
5. Click **OK** when completed. The User Group Information dialog box is displayed.



Note that the newly added user forms are listed in the Group Entitlement display table. This display table shows the name of the user form and the type. In this example, there are two distinct types, javaform and folder. A javaform is a java-based, graphical interface. A folder is a container of one or many javaforms.

> **Note:** The Group Entitlement Table displays all available user groups.

Pre-Existing Groups

Oracle Identity Manager provides four default user group definitions:

- System Administrators
- Operators

- Self Operators
- All Users

You may modify the permissions associated with these user groups. In addition, you can create additional user groups, as needed.

The System Administrators User Group

Members of the *System Administrators* user group have full permissions to create, edit, and delete records within Oracle Identity Manager (except for system records).

Note: When using the Oracle Identity Manager Administrator's Console (Administrative and User Console), a user assigned to a particular process task can change its status.

The Operators User Group

Members of the Operators user group have access to the Organizational Defaults and Policy History forms. These users can perform limited functionality within these forms.

The All Users User Group

Members of the All Users user group have minimal permissions, which include, but are not limited to, the ability to access one's own user record. By default, each user automatically belongs to the All Users user group.

Note: A user cannot be removed from the *All Users* group.

Important: There is a fourth user group definition, SELF OPERATORS, which is added to Oracle Identity Manager, by default. This user group contains one user, XELSELFREG, who is responsible for modifying the privileges that users have when performing self-registration actions within the Oracle Identity Manager Administrative and User Console.

Do not modify the permissions associated with the SELF OPERATORS user group, or assign any users to this group.

The Administrative Queues Form

Oracle Identity Manager allows you to designate that specific groups of users are collectively responsible for managing a provisioning request. These groups are assigned to a request using an entity called a Queue. A queue is merely a collection of existing group definitions, which functions as a mega-group.

Note: Queues can also be nested within other queues, further enhancing the ability to create mega-collections of groups for streamlined assignment.

Once defined, queues can then be attached to requests, thereby making the members of the groups (of which the queue is comprised), responsible for managing the request.

For example, your might create a queue that contained three user groups. Once the queue was assigned to a request, the members of these three groups would have administrative privileges on that request. The administrative privileges that each group has on a particular request are specified within the request (i.e., each group may have distinct privileges within the queue). For instance, the first user group might be able to read, modify, and delete the request. The second user group might be able to read and modify the request, while the third user group might only be able to read and delete the request.

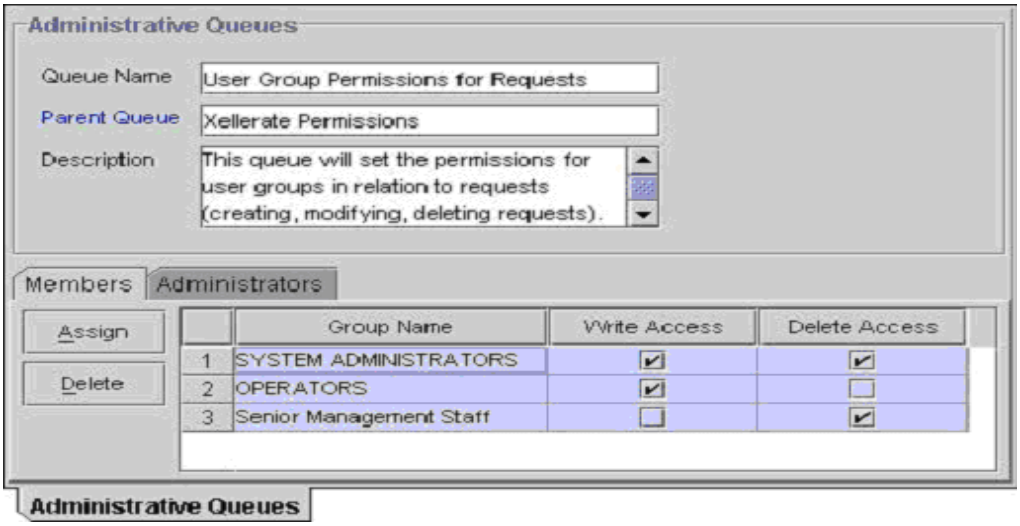
Once defined, a queue is assigned to a request using the Queues tab on the Requests form.

Assigning administrative queues to a form increases your efficiency as a user. Queues also enhance the manageability of requests across an enterprise.

By using an administrative queue, you can accomplish the same goal with only a few mouse clicks. In addition, the queue that you assign to one request can be reused for other requests.

The Administrative Queues form is located in the User Management folder. It is used to create and manage the administrative queues that will be assigned to requests.

Figure 5–3 The Administrative Queues Form



You will now learn about the data fields of the Administrative Queues form. The following table describes the data fields of this form.

Field Name	Description
Queue Name	The name of the administrative queue.
Parent Queue	The queue to which this administrative queue belongs.
Description	Explanatory information about the administrative queue.

Now that we have reviewed administrative queues and the data fields of the Administrative Queues form, you are ready to create an administrative queue.

Create an Administrative Queue

To create an administrative queue, perform the following steps:

1. Open the Administrative Queue form.
2. In the **Queue Name** field, enter the name of the administrative queue.
3. Double-click the **Parent Queue** lookup field. From the lookup dialog box that appears, select the queue of which this administrative queue is a member.

   Note: If the administrative queue you are creating does not belong to another administrative queue (it is a parent administrative queue), proceed to Step 4.

4. In the **Description** field, you can enter explanatory information about the administrative queue.
5. Click **Save**. The administrative queue is created.

Tabs on the Administrative Queues Form

Once you launch the Administrative Queues form, and create an administrative queue, the tabs of this form become functional.

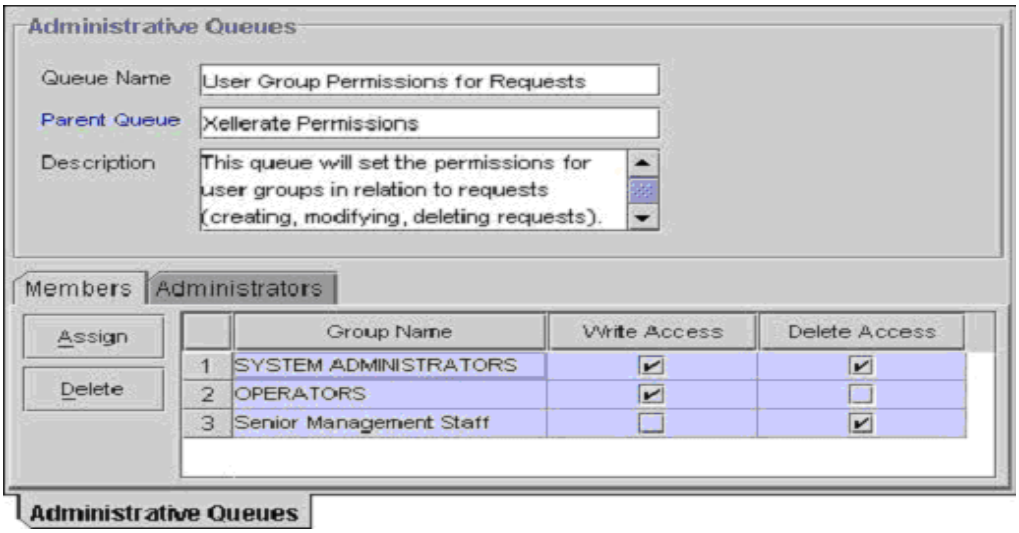
The Administrative Queues form contains the following tabs:

- "Members" on page 5-8
- "Administrators" on page 5-10

Each of these tabs is covered in greater detail in the following sections.

Members

Figure 5–4 The Members Tab of the Administrative Queues Form



This tab is used to select the user groups that will be members of the current administrative queue. In addition, the **Write Access** and **Delete Access** check boxes are visual indicators of the privileges that a user group will have on the requests to which this queue is assigned.

When the **Write Access** check box is selected, the corresponding user group can create and modify information on the request (to which the administrative queue is

assigned). If this check box is cleared, the user group will not be able to create or edit data on requests to which the queue is assigned.

Similarly, when the **Delete Access** check box is selected, it signifies that the associated user group can delete any requests (to which the administrative queue is assigned). If this check box is cleared, the user group cannot delete requests to which the queue is assigned.

For this example, if the User Groups Permissions for Requests queue was assigned to a particular request:

- The SYSTEM ADMINISTRATORS user group would be able to read, modify, and delete information within the request.
- The OPERATORS user group would be able to read and modify information within the request. However, since the **Delete Access** check box is cleared, this user group would not be able to delete the request.
- The Senior Management Staff user group would be able to delete the request. However, because the **Write Access** check box is cleared, this user group would not be able to modify information the within the request.

Just as you can assign a user group to an administrative queue, you must also remove a user group from the administrative queue when that user group can no longer read, modify, or delete information on requests to which this administrative queue is assigned.

Now that we have reviewed the **Members** tab, you will learn how to assign a user group to an administrative queue, and remove a user group from an administrative queue.

Assign a User Group to an Administrative Queue

To assign a user group to an administrative queue, perform the following steps:

1. Click **Assign**. The Assignment dialog box is displayed.
2. Select the user group, and assign it to the administrative queue.
3. Click **OK**. The user group is displayed in the **Members** tab.
4. If you do not want this user group to be able to modify information on requests to which the administrative queue is assigned, clear the corresponding **Write Access** check box. Otherwise, proceed to Step 5.
5. If you do not want this user group to be able to delete the requests to which this administrative queue is assigned, clear the associated **Delete Access** check box. Otherwise, proceed to Step 6.
6. Click **Save**. The user group is assigned to the administrative queue.

> **Note:** By default, any group listed on the **Members** tab will have read privileges on the requests to which the queue is assigned.

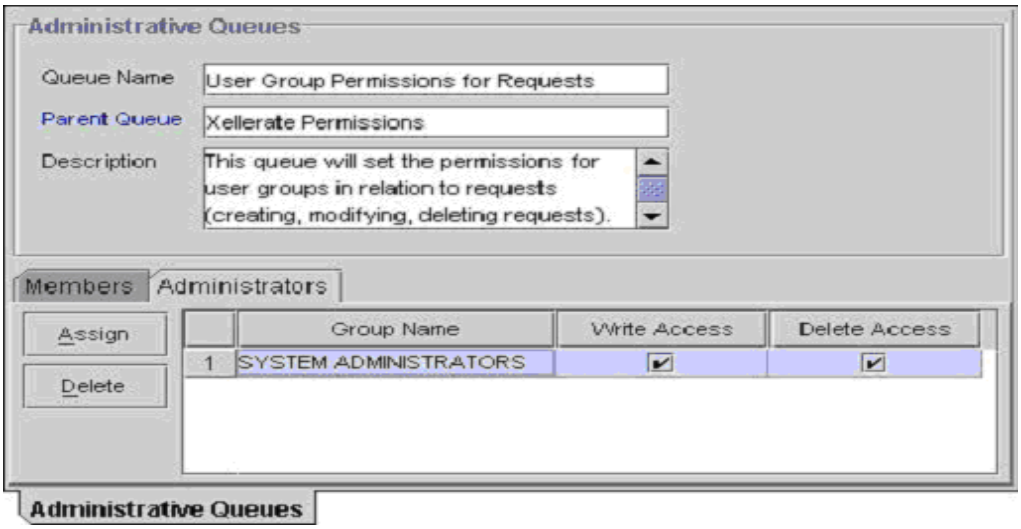
Remove a User Group From an Administrative Queue

To remove a user group to an administrative queue, perform the following steps:

1. Highlight the user group that you want to remove.
2. Click **Delete**. The user group is removed from the administrative queue.

Administrators

Figure 5–5 The Administrators Tab of the Administrative Queues Form



This tab is used to select the user groups that can read, modify, and delete the current administrative queue.

In addition, the **Write Access** and **Delete Access** check boxes are visual indicators of the privileges that a user group has with an administrative queue. When the **Write Access** check box is selected, the corresponding user group can read and modify the current administrative queue. If this check box is cleared, the user group cannot create or edit the administrative queue.

Similarly, when the **Delete** check box is selected, the associated user group can delete the current administrative queue. If this check box is cleared, the user group cannot delete the administrative queue.

For this example, both the **Write Access** and **Delete Access** check boxes are selected for the SYSTEM ADMINISTRATORS user group. As a result, this user group can read, modify, and delete the User Groups Permissions for Requests administrative queue.

Just as you can assign a user group to an administrative queue, you must also remove a user group from an administrative queue when the user group can no longer read, modify, or delete the current administrative queue.

Now that we have reviewed the **Administrators** tab, you will learn how to designate a user group as an administrator to an administrative queue. You will also learn how to remove an administrator user group from an administrative queue.

Designate a User Group as an Administrator of an Administrative Queue

To designate a user group as an administrator of an administrative queue, perform the following steps:

1. Click **Assign**. The Assignment dialog box is displayed.
2. Select the user group, and assign it to the administrative queue.
3. Click **OK**. The user group is displayed in the **Administrators** tab.
4. If you do not want this user group to be able to modify the current administrative queue, clear the corresponding **Write Access** check box. Otherwise, proceed to Step 5.

5. If you want this user group to be able to delete the current administrative queue, clear the associated **Delete Access** check box. Otherwise, proceed to Step 6.
6. Click **Save**. The user group is now an administrator to the administrative queue.

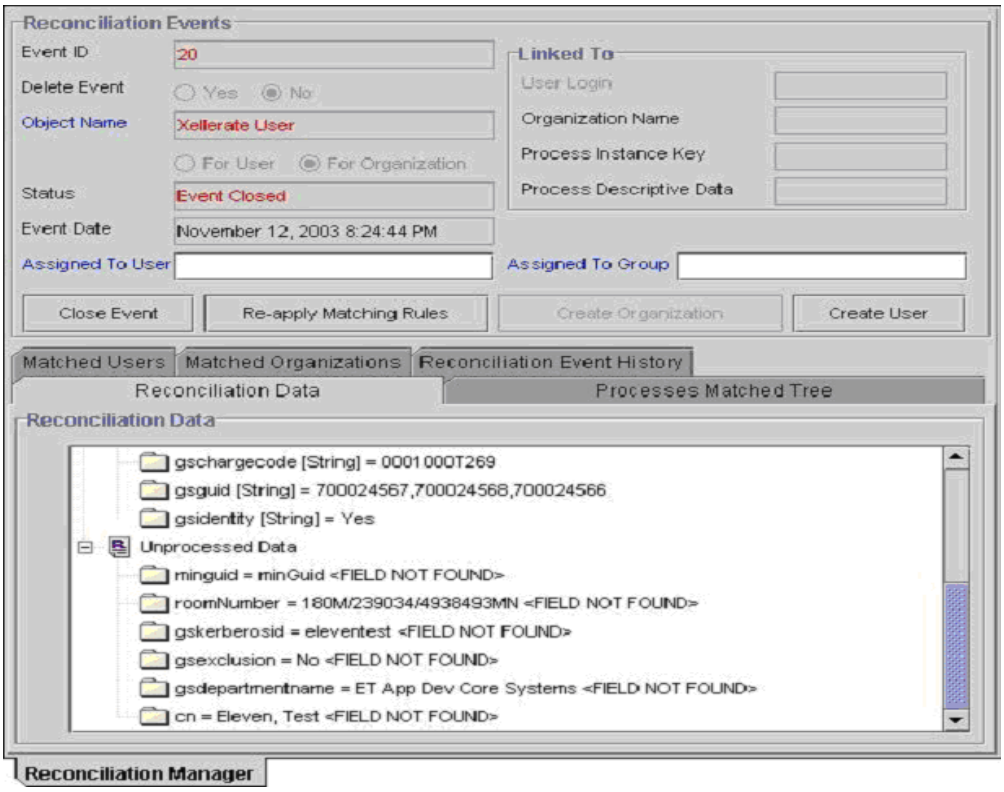
Remove an Administrator User Group From an Administrative Queue

To remove an administrator user group from an administrative queue, perform the following steps:

1. Highlight the user group that you want to remove.
2. Click **Delete**. The administrator user group is removed from the administrative queue.

The Reconciliation Manager Form

Figure 5–6 The Reconciliation Manager Form



This form is located in the User Management folder. As the reconciliation classes you have defined periodically poll your target resources and trusted source, changes occurring on those systems will cause reconciliation events to be generated. Once these events are generated, they are written directly to the Reconciliation Manager where Oracle Identity Manager begins analyzing the information contained within them (according to the mappings defined in the relevant provisioning process). Oracle Identity Manager can be configured to take automated action (based on any action rules you may have defined) if the information in the event is ultimately determined to be associated with an existing record or to represent a new account or it can allow the linking of the information in the event to be manually initiated.

Note: You can use Oracle Identity Manager Task Scheduler form to define a schedule and set the timing parameters that will govern how often your reconciliation class is run or use a third party scheduling tool to set the polling frequency.

This form allows users to view, analyze, correct, link, and manage information contained in reconciliation events received from your target resources and trusted source. The analysis and linking of information contained within your reconciliation events can be conducted manually by a designated individual or performed automatically by Oracle Identity Manager based on information available to it.

More specifically:

- If the information in the reconciliation event is related to an existing user or organization record, this form can be used to manually link the data contained in the reconciliation event to the relevant user's (or organization's) record or review the information that was automatically linked to the user (or organization).
- If the reconciliation event represents the creation of a new employee on a trusted source (i.e., user discovery) or the provisioning of an existing employee with a new resource (i.e., account discovery), this form can be used to manually update Oracle Identity Manager with new data or review the information that was automatically linked to a user. For trusted sources, the data in the reconciliation event will be used to create a new user account. For target resources, the data in the reconciliation event will be used to populate the relevant resource-specific process form.
- If the reconciliation event represents the creation of a new organization on a trusted source (i.e., organization discovery) or the provisioning of an existing organization with a new resource (i.e., account discovery), can be is used to manually update Oracle Identity Manager will that new data or review the information that was automatically linked to a organization.
- If the reconciliation event represents the deletion of an account on a target system or trusted source, this form can be used to instruct Oracle Identity Manager to delete a particular account or review the account that was automatically deleted. For trusted sources, this will result in the deletion of the user's Oracle Identity Manager account (and the revocation of all accounts with which that user may have been provisioned on any target resources). For target resources, this will result in Oracle Identity Manager recognizing that the user's account on that system has been revoked.

The upper portion of the Reconciliation Manager form contains the following fields and buttons:

Field Name	Description
Event ID	The numeric ID of the reconciliation event.

Field Name	Description
Delete Event (Yes/No flag)	This display-only field is used to indicate whether the classification type of the current reconciliation event is a delete event (i.e., the corresponding record has been deleted from either the target resource or the trusted source).If the reconciliation event is a delete event, Oracle Identity Manager selects the Yes option. If this event is ultimately associated with a user's account on a target resource, that account will be marked as revoked. If the event is ultimately associated with a particular user's account, that user's account will be deleted. If the current reconciliation event is not a delete event, Oracle Identity Manager selects the No option. **Note**: This field is set by Oracle Identity Manager. A user cannot set it.
Object Name	The resource object (target resource/trusted source) associated with this reconciliation event. For trusted sources, this will be the user.
For User/For Organization	Option designating whether the reconciliation event related to a resource object is associated with a user or organization record.

Field Name	Description
Status	The current status of the reconciliation event. Possible statuses are: ■ **Event Received**: A notification that information has changed has been received from the target resource/trusted source (for example, the CreateReconciliationEvent method has been called). The reconciliation event has not yet been received its actual data from the target resource/trusted source. ■ **Data Received**: The information from the target resource/trusted source has been received. ■ **Users Matched**: The information in the reconciliation event has been matched to one or more user records (using the application of reconciliation user-matching rules). ■ **Organizations Matched**: The information in the reconciliation event has been matched to one or more organization records (using the application of reconciliation organization-matching rules). ■ **Processes Matched**: The information in the reconciliation event has been matched to one or more provisioning processes (for example, all the values of key fields in the reconciliation event have matched the values of those fields on the process' form). ■ **No Match Found**: Neither the values of key fields (on provisioning process forms) or the criteria of any user/organization-matching rules matched the information in the reconciliation event. The reconciliation event has not been associated with any user or organization record. ■ **Rules Reapplied**: The **Reapply Matching Rules** button was clicked (previous matches may be removed) and the logic of the latest edition of all matching rules (associated with this resource) were applied. ■ **Event Linked**: The information in the reconciliation event has been matched and linked to a particular user or organization record. ■ **Event Closed**: A user manually closed the reconciliation event (by click the Close Event button) without its data being linked to a record within Oracle Identity Manager. Once closed, a reconciliation event cannot be reopened and no addition m·Required Data Missing - At least one required data element is missing. If the data for any fields that have been set as required on the resource definition is not available in the reconciliation event, this message is displayed. atching logic can be applied to it.
Event Date	The date and time on which this reconciliation event was received.
Assigned to User	The user to whom this reconciliation event has been assigned.
Assigned to Group	The user group to which this reconciliation event has been assigned.

Field Name	Description
Linked To (region)	The fields in this section of the form are described below.
User Login	The Oracle Identity Manager ID of the user record to which the reconciliation event has been linked.
Organization Name	The Oracle Identity Manager ID of the Oracle Identity Manager organization record to which the reconciliation event has been linked. If you are conducting organization discovery with a trusted source, it is recommended that this be done prior to performing user discovery (since every user record in Oracle Identity Manager must be associated with an organization record).
Process Instance Key	Numeric instance of the provisioning process to which the reconciliation event has been linked.
Process Descriptive Data	Instance-specific descriptive data for the provisioning process (that is defined in the Map Descriptive Field pop-up window within the Process Definition form)
Close Event	This button is used to close the reconciliation event. If the reconciliation event is closed, no additional matching attempts or linking can be performed on it.
Re-apply Matching Rules	This button is used to reapply the reconciliation matching rules (i.e., both process data and user/organization-matching rules) associated with the resource object. If Oracle Identity Manager is not generating satisfactory matches, the resource's reconciliation matching rules can be amended and reapplied (alternately, you might also amend the mappings on the provisioning process). Re-applying these rules after they have been edited may cause different records to be appearing on the Processes Matched, Matched Users or Matched Organizations tabs. Reconciliation rules are only applied to target resource reconciliation events when no provisioning process matches are generated (since the process matches are considered to be of better quality and therefore more likely accurate).
Create Organization (Only available on events related to the trusted source)	This button is used to create an organization record in Oracle Identity Manager based on the information provided in the reconciliation event. This button should only be used when you are certain that the reconciliation event represents the creation of a new organization on the trusted source.
Create User(Only available on events related to the trusted source)	This button is used to create a user record in Oracle Identity Manager based on the information provided in the reconciliation event. This button should only be used when you are certain that the reconciliation event represents the creation of a new user on the trusted source.

View and Manage Reconciliation Events

To view and manage reconciliation events, perform the following steps:

1. Access the Reconciliation Manager form.
2. Use the query feature to locate the desired reconciliation event.

Note: Reconciliation events can also be queried by their associated resource (in the Object Name field) or Status (in the Status field).

If the reconciliation event for which you are querying is a delete event (i.e., the corresponding record has been deleted from either the target resource or the trusted source), the Yes option for the Delete Event flag will be selected. Otherwise, the No option will be selected.

3. Once the desired reconciliation event has been located, use the tabs of this form to:
   - Correct any unprocessed data.
   - Browse and link to matching provisioning process form instances or user/organization record candidates.
   - View the audit history of the event.

Note: Depending on how you have defined your reconciliation action rules, Oracle Identity Manager may automatically link data in a reconciliation event to a user or organization record when only one match is found (or when no matches are found for the trusted source).

The information displayed on each tab is described in the Tabs on the Reconciliation Manager form section. When evaluating the matches Oracle Identity Manager has generated you can either:

- Link the reconciliation event to a particular provisioning process, user or organization (this denotes that the event is associated with an existing user or organization record). To do this, click the **Link** button on the applicable tab. Alternately, you may have defined rules that instruct Oracle Identity Manager to automatically link the data when only a single match is found.
- **[For user-based reconciliation with the trusted source]** Create a new user in Oracle Identity Manager (this denotes that the event represents the creation of a new user on the trusted source). To do this, click the **Create User** button. Alternately, you may have defined action rules that instruct Oracle Identity Manager to automatically create the user when no match is found.
- **[For organization-based reconciliation with the trusted source]** Create a new organization in Oracle Identity Manager (this denotes that the event represents the creation of a new organization on the trusted source). To do this, click the **Create Organization** button. Alternately, you may have defined action rules that instruct Oracle Identity Manager to automatically create the organization when no match is found.
- Refine the reconciliation rules associated with this resource and then re-apply the rule to generate more accurate matches. To do this, first refine the applicable reconciliation rule, save it and then click the **Re-apply Matching Rules** button.

Note: If you refine a reconciliation rule and reapply it or choose to create/link a user/provisioning process/organization, these actions will be logged on the **Reconciliation Event History** tab. To view a log of the actions that have been performed on the reconciliation event, click the **Reconciliation Event History** tab.

Tabs on the Reconciliation Manager Form

Once the reconciliation event you wish to examine has been located, you can use these tabs to view any processed/unprocessed data in that event, view any provisioning process/ user/organization matches that have been generated and link the event to the appropriate record (or create a new user).

Reconciliation Data

The data displayed on this tab appears under one of two branches: Processed Data and Unprocessed Data.

Processed Data

The fields listed within the Processed Data branch are those fields (as defined on the Reconciliation Fields tab of the associated resource) within the reconciliation event that have been successfully processed (for example, have not violated any data types requirements). For each successfully processed field, the following information will be provided:

- Name of the field as defined on the Reconciliation Fields tab of the associated resource (for example, *field1*).
- Data type associated with the field that was reconciled (for example, *string*). Possible values are *Multi-Valued*, *String*, *Number*, *Date*, *IT resource*.
- Value of the field that was received in the reconciliation event (for example, *Newark*). This may be one of several values that changed on the target resource/trusted source and initiated the reconciliation event.

An example of a processed data field might appears as follows:

```
Location [String] = Newark
```

> **Note:** If a field is of type multi-value (only allowed for target resources, not trusted sources), it will not have a value. Instead, its component fields (contained within it's sub-branch) will each have their own individual values.

Unprocessed Data

The fields listed within the Unprocessed Data branch are those fields within the reconciliation event that were unable to be processed (for example, due to not being defined or having a conflict with the data type set on the Reconciliation Fields tab of the associated resource). For each unprocessed field, the following information will be provided:

- Name of the field (for example, *user_securityid*).
- Value of the field that was received in the reconciliation event (for example, *capital*). This may be one of several values that changed on the target resource/trusted source and initiated the reconciliation event.
- Reason why the data received from the target system was unable to be automatically processed (for example, <*Not Numeric*>). One of the following reason codes appears next to the unprocessed field:

Error code	Reason generated
NOT MULTI-VALUED ATTRIBUTE	A value was specified for a field that is defined as a multi-valued attribute. Only the component fields of a multi-value attribute (not the multi-value field itself) can accept values.
NOT NUMERIC	The value specified for a numeric field was non-numeric.
DATE PARSE FAILED	The system failed to recognize the value of a date field as a valid date.
SERVER NOT FOUND	The value specified for a field of type *IT Resource* was not recognized as the name of an existing IT Resource instance.
FIELD NOT FOUND	The name of the field specified in the event has not been defined on the resource.
PARENT DATA LINK MISSING	The parent data field (of type multi-value) is not yet linked to a reconciliation field. As a result, this component field cannot be linked to a child reconciliation field.
FIELD LINKAGE MISSING	The corresponding reconciliation field is not defined on the Reconciliation Fields tab of the associated resource.
ATTRIBUTE LINKAGE MISSING	[Only for fields of type multi-value.] The multi-value reconciliation field cannot be processed as one or more of its component (child) fields' data is not linked to reconciliation fields.
TABLE ATTRIBUTE LINKAGE MISSING	[Only for fields of type multi-value.] The multi-value field cannot be processed as some of its component (child) fields of type *Multi-Valued Attribute* are not linked to a reconciliation field of type *Multi-Valued Attribute*.

- The name of the resource field this reconciliation event field was ultimately mapped to (if the unprocessed field is successfully mapped to a resource field).

An example of an unprocessed data field might appears as follows:

```
user_securityid = capital <Not Numeric>
```

> **Note:** Oracle Identity Manager will not attempt to match processes (for target resources) or user/organizations (for trusted sources) until all fields that have been set as required (on the Reconciliation Fields tab of the associated resource) have been successfully processed.

To Map or Correct Unprocessed Fields

This procedure is used to correct and/or map unprocessed fields within the reconciliation event to the relevant fields as defined on the applicable resource.

1. Double-click the unprocessed field.

   If the unprocessed field is of type multi-value, you may need to map it to the appropriate child process form and/or check the individual component field (for multi-value fields, double-click and correct the component fields).

   The Edit Reconciliation Field Data dialog box is displayed.

Note: To map an unprocessed multi-value component field to one of the multi-value fields defined on the Reconciliation Fields tab of the associated resource, double-click the **Linked to** field, select the desired field and click **OK**. Then click **Save** and close the Edit Reconciliation Field Data dialog box.

2. To map the unprocessed field to one of the fields defined on the Reconciliation Fields tab of the associated resource, double-click the **Linked To** field, select the desired field, and click **OK**. Then click **Save** and close the Edit Reconciliation Field Data dialog box.

   To correct the value of the unprocessed field, enter the correct value in the **Corrected Value** field, click **Save** and close the Edit Reconciliation Field Data dialog box.

If the field's data is successfully processed, the entry within the Unprocessed Data branch will be updated to reflect the field to which it was linked. A new entry for the field will be added to the Processed Data branch.

Once all the required data elements (as set as on the Object Reconciliation tab of the applicable resource definition) within the reconciliation event have been marked as processed on the Reconciliation Data tab, Oracle Identity Manager will display:

- For trusted sources:

All user or (organization) records that match the relevant data (as specified within the logic of all applicable user/organization-matching reconciliation rule associated with the resource) in the reconciliation event. These candidates represent any accounts on the trusted source for which a potential owner was found in Oracle Identity Manager (i.e., user update) based on the application of user-matching rules. If no matches are found, the reconciliation event represents the creation of a new user account on the trusted source (i.e., user creation).

- For target resources:

All provisioning process form instances where the values of all key fields (as set on the Reconciliation Field Mappings tab of the applicable process definition) match the values for all key fields within the reconciliation event. This represents an account in the target system for which a possible matching account was found within Oracle Identity Manager (i.e., account update). If no processes instances are found to match these values, Oracle Identity Manager will proceed to evaluate the applicable user- (or organization-) matching reconciliation rules and display any users (or organizations) that match relevant data in the reconciliation event. These matches represent accounts on the target system for which the reconciliation engine did not find a matching account record within Oracle Identity Manager (i.e. Oracle Identity Manager is not aware that the user has been provisioned with an account on that system) but did find potential owners of the account (i.e., account creation). If more than one matching candidate is found, you will generally want to have an administrator examine the records and decide which Oracle Identity Manager account to link it to. If no matches are found, it could mean that there has been a possible mismatch between the data in your trusted source and the target application, that this event represents a "rogue" account on the target system or that an existing employee has been provisioned with a new account on the target system but Oracle Identity Manager is unable to decide which user that account is associated with.

Processes Matched Tree (for target resources only)

Once all required fields (as defined on the Reconciliation Fields tab of the associated resource) have been processed, this tab will display all provisioning process form instances where the values of all key fields match the values for all key fields within the reconciliation event.

> **Note:** This will only occur for reconciliation events associated with target resources. Since the trusted source is linked to the user resource (or *Organization*) and it's provisioning process, cannot have a custom process form and therefore, cannot possess the matches required to populate this tab. As a result, for trusted sources, once all required fields have been processed, Oracle Identity Manager will proceed immediately to evaluating user\organization matching rules.

For each matched provisioning process, the follwing is displayed:

- The name of provisioning process associated with the process form instance that matched the values of the key fields in the reconciliation event (for example, windows2000_prov).
- The numeric ID of the particular process instance (for example, 445)
- The User ID (for example, jdoe) or Organization Name (for example, Finance) associated with this process instance (i.e., the user who was provisioned with the resource by that instance of the provisioning process).

An example of a matched provisioning process might appears as follows:

```
Windows2000_prov [445] for User=jdoe
```

If no provisioning processes are listed on this tab, it denotes that Oracle Identity Manager was unable to match any of the values in the key fields in the reconciliation event to any of the values for those fields within process form instances associated with that resource. If this occurs, Oracle Identity Manager will then attempt to apply any user\organization-matching rules that have been defined for the resource (if matches are found, they appears on the **Matched Users or Matched Organizations** tab accordingly).

Link a Provisioning Process Instance to the Reconciliation Event

To link a provisioning process instance to the reconciliation event, perform the following steps:

1. Once you have determined which provisioning process instance to link to the reconciliation event, select it and click **Establish Link**.
2. Oracle Identity Manager will then update the relevant process form instance with the information in the reconciliation event according to the mappings defined on the relevant provisioning process (and insert the Reconciliation Update Received task within that process).

Matched Users

This tab displays the user records that match the relevant data within the reconciliation event (as specified in the criteria of the resource's reconciliation rules).

For trusted sources, Oracle Identity Manager will evaluate these rules and display any matching user records as soon as all required fields (as defined on the **Reconciliation Fields** tab of the associated resource) have been processed.

For target resource, Oracle Identity Manager will evaluate these rules and display any matching user records only after all required fields (as defined on the **Reconciliation Fields** tab of the associated resource) have been processed and no matches have been generated on the **Processes Matched Tree** tab.

> **Note:** If matching records are present on the **Processes Matched Tree** tab, no records appears on the **Matched Users** tab (since the process matches are considered to be of better quality and therefore more likely accurate).

For each matching record, Oracle Identity Manager will display the User's ID, First Name, and Last Name.

Link a User Record to the Reconciliation Event

1. Once you have determined which user to link to the reconciliation event, select it and click **Link**.
2. If you click Link and the reconciliation event is for a target resource, then Oracle Identity Manager:
   - Creates an instance of the resource's provisioning process (for the selected user), suppress any adapters associated with the process' tasks, auto completes the process and inserts the Reconciliation Insert Received task.
   - Creates an instance of the resource's process form with the data from the reconciliation event according to the mappings defined on the provisioning process.

   If you click Link and the reconciliation event is for a trusted source, then Oracle Identity Manager:
   - Updates the user record with the data from the reconciliation event according to the mappings defined on the "user" provisioning process.
   - Inserts the Reconciliation Insert Received task in the existing instance of the "user" provisioning process for the user record to which the reconciliation event has been linked.

   > **Note:** Alternately, for trusted sources, if you determine that the reconciliation event represents the creation of a new user on the trusted source, click the **Create User** button (this will create a new user record with the information contained in the reconciliation event).

Matched Organizations

This tab displays the Oracle Identity Manager organization records that match the data within the reconciliation event (as specified in the criteria of the resource's reconciliation rules).

For trusted sources, Oracle Identity Manager will evaluate these rules and display any matching organization records as soon as all required fields (as defined on the Reconciliation Fields tab of the associated resource) have been processed.

For target resources, Oracle Identity Manager will evaluate these rules and display any matching organization records only after all required fields (as defined on the

Reconciliation Fields tab of the associated resource) have been processed and no matches have been generated on the Processes Matched Tree tab.

> **Note:** If matching records are present on the Processes Matched Tree tab, no records appears on the Matched Organizations tab (since the process matches are considered to be of better quality and therefore more likely accurate).

For each matching record, Oracle Identity Manager will display the User's ID, First Name, and Last Name.

Link an Organization Record to the Reconciliation Event

1. Once you have determined which organization to link to the reconciliation event, select it and click **Link**.
2. If you click **Link** and the reconciliation event is for a target resource, Oracle Identity Manager:
   - Creates an instance of the resource's provisioning process (for the selected organization), suppress any adapters associated with the process' tasks, auto completes the process and inserts the Reconciliation Insert Received task.
   - Creates an instance of the resource's process form with the data from the reconciliation event according to the mappings defined on the provisioning process.

   If you click **Link** and the reconciliation event is for a trusted source, Oracle Identity Manager:
   - Updates the organization record with the data from the reconciliation event according to the mapping defined on the "*Oracle Identity Manager Organization*" provisioning process.
   - Inserts the Reconciliation Insert Received task in the existing instance of the "*Oracle Identity Manager Organization*" provisioning process for the organization record to which the reconciliation event has been linked.

   > **Note:** Alternately, for trusted sources, if you determine that the reconciliation event represents the creation of a new organization on the trusted source, click the **Create Organization** button (this will create a new organization record with the information contained in the reconciliation event).

Reconciliation Event History

This tab displays a history of the actions performed on this reconciliation event. For each action, the date and time on which it took place will be listed. Oracle Identity Manager will track and log the following reconciliation event actions:

- **Event Received**: The action is logged when a reconciliation event is received by Oracle Identity Manager.
- **Data Sorted**: The action is logged when the data within a reconciliation event has been sorted into processed and unprocessed fields.
- **Rules Reapplied**: The action is logged when a user has clicked the **Re-apply Matching Rules** button.

- **Processes Matched**: The action is logged when one or more process form instances (and their associated provisioning process) have been matched to the values of key fields within the reconciliation event.
- **Users Matched**: The action is logged when one or more user records have been matched with the data in the reconciliation event (using the invocation of a user-matching reconciliation rules).
- **Organization Matched**: The action is logged when one or more Oracle Identity Manager organization records have been matched with the data in the reconciliation event (using the invocation of a organization-matching reconciliation rules).
- **Linked to User**: The action is logged when the data in the reconciliation event has been linked to a particular user.
- **Linked to Organization**: The action is logged when the data in the reconciliation event has been linked to a particular organization.

6

Resource Management

This chapter describes the resource management in Oracle Identity Manager. It contaisn the following topics:

Overview

The Resource Management folder provides System Administrators with the tools necessary to manage Oracle Identity Manager resources. This folder contains the following forms:

- **IT Resources Type Definition**: This form is used to create the resource types that appear as lookup values on the IT Resources form.
- **IT Resources**: This form is used to define and manage IT resources.
- **Rule Designer**: This form is used to create rules that can be applied to password policy selection, auto-group membership, provisioning process selection, task assignment, and prepopulate adapters.
- **Resource Objects**: This form is used to create and manage resource objects. These objects represent the resources that you wish to make available to users and organizations.

Note: Throughout this chapter, you will read about prepopulate adapters and Java tasks. To learn more about adapters and adapter tasks, refer to *Oracle Identity Manager Tools Reference Guide*.

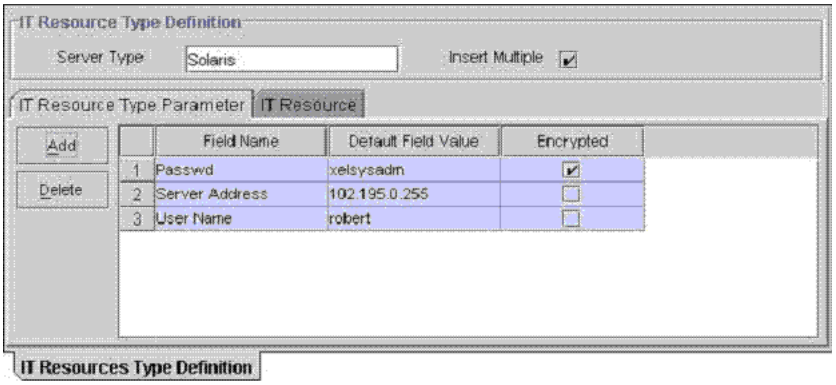
The IT Resources Type Definition Form

The IT Resources Type Definition form, as shown in Figure 6–1, is located in the Resource Management folder. It is used to specify the types of IT resources that are to be associated with the resource objects that can be provisioned to target users and organizations.

The IT resource types defined here will be available for selection (using the **Type** field) when defining IT resources in the IT Resources form. IT resource types serve as a template for all IT resource definitions that reference them.

Note: Each IT resource definition must be associated with an IT resource type.

Figure 6–1 The IT Resources Type Definition Form



Note: If the IT resource you are defining must access an external resource but cannot reach that resource using the network, you must associate it with a remote manager. For more information on defining remote managers (and their association with IT resources), refer to *Oracle Identity Manager Tools Reference Guide*.

As mentioned, the IT Resources Type Definition form is used to classify the IT resource types (for example, *AD*, *MS Exchange*, *Solaris*) that Oracle Identity Manager can associate with the resources objects it will be provisioning. The IT resource type serves as the general IT classification (such as Solaris), whereas the IT resource designates a particular instance of that resource type (*Solaris for Statewide Investments*). The parameters and values defined for an IT resource type are inherited by all IT resource definitions that reference it.

Now that we have reviewed IT resource types, you will learn about the data fields of the IT Resources Type Definition form. The following table describes the fields of this form.

Field Name	Description
Server Type	The name of the IT resource type.
Insert Multiple	This checkbox is used to specify whether this IT resource type may be referenced by more than one IT resource.

Now that we have reviewed about types of IT resources, you are ready to define a template for IT resources.

Define a Template for IT Resources

To define a template for the IT Resouces, perform the following steps:

1. Enter the name of the IT resource type in the **Server Type** field (for example, *Solaris*).
2. When you want this IT resource type to be available for multiple IT resources, select the **Insert Multiple** checkbox.

   If you wish this IT resource type to be available for only one IT resource, clear the **Insert Multiple** checkbox.
3. Click **Save**. The IT resource template is defined. It can now be selected (using the **Type** field) when defining IT resources from within the IT Resources form.

Tabs on the IT Resource Type Definition Form

Once you save the preliminary information for a new IT resource type, or query for an existing IT resource type, the fields within the tabs of the IT Resources Type Definition form's lower region are enabled.

The IT Resources Type Definition form is comprised of the following tabs:

- IT Resource Type Parameter
- IT Resource

Each of these tabs is covered in greater detail in the sections that follow.

IT Resource Type Parameter

IT Resource Type Parameter tab is used to specify the default values and encryption settings for all connection parameters that are associated with the IT resource type, as shown in Figure 6–1. Any parameters specified on this tab will automatically be inherited by all IT resources that reference this IT resource type.

Note: The default values and encryption settings supplied for these parameters may be customized within each IT resource.

Now that we have reviewed about the **IT Resource Type Parameter** tab, you will learn how to add a parameter to an IT resource type, and remove a parameter from an IT resource type.

Add a Parameter to an IT Resource Type

To add a parameter to an IT Resource Type, perform the following steps:

1. Click **Add**. A new row is displayed within the **IT Resource Type Parameter** tab.
2. Enter the name of the parameter in the **Field Name** field.
3. Enter a value into the **Default Field Value** field. This default value will be inherited by all IT resources that reference this IT resource type.
4. Select or clear the **Encrypted** checkbox. This checkbox is used to specify whether this parameter's value should be masked (i.e., represented with **** symbols) within any form fields.

When you want this parameter's value to be visible within Oracle Identity Manager fields, clear the **Encrypted** checkbox. Otherwise, if you want this parameter's value to be masked within Oracle Identity Manager form fields, select this checkbox.

5. Click **Save**. The specified parameter, along with its associated values and encryption settings, are added to the current IT resource type. As a result, this parameter will now be added to any new or existing IT resource definitions that reference this IT resource type. In other words, for that resource definition, the parameter you added appears within the **Parameters** tab of the IT Resources form.

Remove a Parameter From an IT Resource Type

To remove a parameter from an IT Resource Type, perform the following steps:

1. Highlight the parameter you want to remove.
2. Click **Delete**. The parameter and its associated value will be removed from both the IT resource type, and any IT resource definitions that reference this type.

IT Resource

This tab displays all of the IT resources that reference the selected IT resource type. All IT resources listed here share the same set of parameters (although the values may be uniquely set for each IT resource).

IT Resource Type Definition Table

The IT Resource Type Definition Table displays the following information:

Field Name	Description
Server Type	This is the name of the resource asset type (as defined in the IT Resource Type Definition form).
Insert Multiple	This checkbox indicates whether multiple instance of this IT Resource Definition can be created or not.

The IT Resources Form

The IT Resources form is located in the Resource Management folder. It is used to display (and specify the parameter values for) the IT resources that you wish to make available within Oracle Identity Manager.

IT resource definitions generally represent the hardware (i.e., a Server or a machine) on which one or more resources reside. These IT resource definitions are then referenced by your resource objects during the execution of provisioning processes. A resource object cannot be provisioned without an association with an IT resource definition, which specifies where that resource is located and how to connect to it.

In addition, the variables of an Oracle Identity Manager adapter can be mapped to the values of any parameters defined for an IT resource. These parameters can represent information pertaining to the hardware itself (for example, a Server's domain name) or other information, such as the ID of the user who accesses this IT resource.

Note: For more information about adapters and their mappings, refer to *Oracle Identity Manager Tools Reference Guide*.

Each IT resource definition represents a particular instance of an IT resource type. In the above example, the *ramone* definition belongs to the IT resource type named *Database*.

Now that we have reviewed IT resources, you will learn about the data fields of the IT Resources form. The following table describes the fields of this form.

Field Name	Description
Name	The name of the IT resource.
Type	This classification type of the IT Resource (as defined in the IT Resources Type Definition form).
Remote Manager	When the IT resource can be accessed using a remote manager, this field displays the name of the remote manager. Otherwise, this field is empty.

Now that we have reviewed about IT resources, you are ready to define an IT resource.

Define an IT Resource

To define an IT Resource, perform the following steps:

1. Enter the name of the IT resource in the **Name** field.
2. Double click the **Type** lookup field. From the Lookup dialog box that is displayed, select the IT resource type that is to be associated with this IT resource. Click **OK**.

   Note: IT resource types are defined using the IT Resource Type definition form.

   The IT resource will inherit the parameters and values that were defined for the IT resource type you select.
3. If the IT resource is to be accessed using a remote manager (i.e., the IT resource type has been defined as a remote manager), double-click the **Remote Manager** lookup field. From the Lookup dialog box that is displayed, select the desired remote manager. Click **OK**.

   If the IT resource will not be accessed using a remote manager, proceed to Step 4.
4. Click **Save**. The IT resource is defined. The parameters and default values associated with this IT resource classification type appear within the **Parameters** tab. In addition, this IT resource will now be displayed on the **IT Resource** tab of the IT Resources Type Definition form for the associated IT resource type.
5. *Optional*. To specify IT resource-specific values for the parameters that are listed on the **Parameters** tab, select the **Value** field for the parameter you wish to edit, and enter the desired value. Then, click **Save**.

Setting Access Permissions to an IT Resource Instance Parameter

Use the Administrators tab to set the access permissions to specified administrative groups and have a level of security for the IT Resource APIs.

1. Click the **Administrators** tab. By default, administrator group associated with this IT Resource Instance is displayed automatically.
2. Click **Assign** to add a new administrative group.

In this example, *G2* is assigned as a administrative group for the *ramone* IT Resource instance.

3. Click the desired checkbox to give **Read**, **Write**, or **Delete** permissions.

Name	Description
Read	When the **Read** check box is selected, the corresponding Group Name can read the current IT Resource Instance. If this check box is cleared, the administrative group cannot access the IT Resource Instance.
Write	When the **Write** check box is selected, the corresponding Group Name cannot read and modify the current IT Resource Instance parameter values. If this check box is cleared, the administrative group cannot edit the IT Resource Instance parameters.
Delete	When the **Delete** check box is selected, the associated administrative group can delete the current IT Resource Instance. If this check box is cleared, the administrative group cannot delete the IT Resource Instance.

4. Click the **Save** button.

The Rule Designer Form

Rules are criteria that enable Oracle Identity Manager to match conditions and take action based on them.

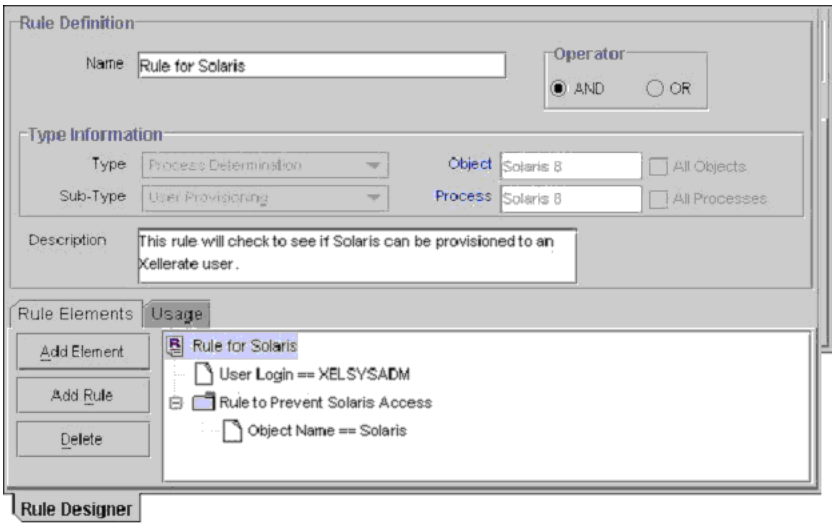
Rules can be used for various purposes, such as:

- Determining which password policy will be applied to a resource object of type **Application**.
- Enabling users to be added to user groups automatically.
- Specifying which approval and provisioning processes will be selected for a resource object, once that resource object is assigned to a request.
- Determining how a process task will be assigned to a user.
- Specifying which prepopulate adapter will be executed for a given form field.

Note: To learn more about prepopulate adapters and their usage with form fields, refer to *Oracle Identity Manager Tools Reference Guide*.

The Rule Designer form, as shown in Figure 6–2, is located in the Resource Management folder. It is used to create and manage the rules that are used with the resources in Oracle Identity Manager.

Figure 6–2 Rule Designer Form



There are four types of rules:

General. This type of rule enables Oracle Identity Manager to add a user to a user group automatically. It can also be used to determine the password policy that will be assigned to a resource object.

Process Determination. This type of rule determines the standard approval process that will be associated with a request, as well as the approval and provisioning processes that will be selected for a resource object.

Task Assignment. This type of rule specifies which user and/or user group will be assigned to a process task.

Prepopulate. This type of rule determines which prepopulate adapter will be executed for a given form field.

Note: A rule can be assigned to either a specific resource object or process, or it can be applied to all resource objects or processes.

A rule can be comprised of the following items:

A rule element. A rule element consists of an attribute, an operator, and a value. For this example, the attribute is *User Login*, the operator is ==, and the value is *XELSYSADM*.

A nested rule. Sometimes, for logic purposes, one rule must be contained inside of another rule. The internal rule is known as the **nested rule**. In this example, the *Rule to Prevent Solaris Access* rule is nested inside of the *Rule for Solaris* rule.

An operation. When a rule is comprised of multiple rule elements or nested rules, an operation is needed to show the relationship among the rule elements and/or nested rules. For this example, the **AND** operation is selected, signifying that the *User Login==XELSYSADM* rule element and the *Rule to Prevent Solaris* Access nested rule must both be true for the rule to be successful.

You will now learn about the data fields of the Rule Designer form. The following table describes the data fields of this form.

Field Name	Description
Name	The rule's name.
AND/OR	These radio buttons are used to specify the operation for the rule. To stipulate that a rule will be successful only when all of its outer rule elements and/or nested rules are *TRUE*, select the **AND** radio button. To indicate that a rule is to be successful if any of its outer rule elements and/or nested rules are *TRUE*, select the **OR** radio button. **Important**: These radio buttons do not reflect the operations for rule elements that are contained within nested rules. For the above graphic, the **AND** operation applies to the *User Login == XELSYSADM* rule element and the *Rule to Prevent Solaris Access* nested rule. However, this operation has no bearing on the *Object Name != Solaris* rule element (which is contained within the *Rule to Prevent Solaris Access* rule).
Type	The rule's classification status. A rule can belong to one of four types: ■ **General**: This type of rule enables Oracle Identity Manager to add a user to a user group automatically. It also determines the password policy that will be assigned to a resource object. ■ **Process Determination**: This type of rule determines the standard approval process that will be associated with a request, as well as the approval and provisioning processes that will be selected for a resource object. ■ **Task Assignment**: This type of rule is used to determine which user and/or user group will be assigned to a process task. ■ **Prepopulate**: This type of rule is used to determine which prepopulate adapter will be executed for a given form field.
Sub-Type	For organizational purposes, when a rule's type is **Process Determination**, **Task Assignment**, or **Prepopulate**, it can be further categorized into one of four sub-types: ■ **Organization Provisioning**: This sub-type further classifies the rule as a provisioning rule. It is used to determine the organization for which a process will be provisioned, a task will be assigned, or the prepopulate adapter will be applied. ■ **User Provisioning**: This sub-type further classifies the rule as a provisioning rule. It is used to determine the user for which a process will be provisioned, a task will be assigned, or a prepopulate adapter will be applied. ■ **Approval**: This sub-type further classifies the rule as an approval rule. It is used to approve the provisioning of resources to users or organizations. ■ **Standard Approval**: This sub-type further classifies the rule as a standard approval rule. It is used to approve a request. **Note**: If a rule's type is **Task Assignment** or **Prepopulate**, the Approval and Standard Approval items will not appear within the **Sub-Type** combo box. Furthermore, when a rule's type is **General**, the **Sub-Type** combo box will be disabled.
Object	The resource object to which this rule is assigned.
All Objects	By selecting this check box, the rule can be assigned to all resource objects.
Process	The process to which this rule is assigned.
All Processes	By selecting this check box, the rule can be assigned to all processes.
Description	Explanatory information about the rule.

Now that we have reviewed the data fields of this form, you will learn how to create a rule.

Create a Rule

To create a rule, perform the following steps:

1. Open the Rule Designer form.
2. In the **Name** field, enter the name of the rule.
3. If you want to stipulate that a rule will be successful only when all of its rule elements and/or nested rules are *TRUE*, select the **AND** radio button. If you want to indicate that a rule is to be successful if any of its rule elements and/or nested rules are *TRUE*, select the **OR** radio button.

   Caution: These radio buttons do not reflect the operations for rule elements that are contained *within* nested rules. Figure 6–2 the **AND** operation applies to the *User Login == XELSYSADM* rule element and the *Rule to Prevent Solaris Access* nested rule. However, this operation has no bearing on the *Object Name != Solaris* rule element (which is contained within the *Rule to Prevent Solaris Access* rule).

4. Click the **Type** combo box. From the custom menu that appears, select the classification status (**General**, **Process Determination**, **Task Assignment**, or **Prepopulate**) that will be associated with the rule.
5. If you select **Process Determination** from the **Type** combo box, click the **Sub-Type** combo box. From the drop-down menu that is displayed, select the specific classification status (**Organizational Provisioning**, **User Provisioning**, **Approval**, or **Standard Approval**) that will be associated with the rule.

   If you select **Task Assignment** or **Prepopulate** from the **Type** combo box, click the **Sub-Type** combo box. From the drop-down menu that is displayed, select the specific classification status (**Organization Provisioning** or **User Provisioning**) that will be associated with the rule.

   If you select **General** from the **Type** combo box, proceed to Step 8.
6. If you want to associate the rule with a single resource object, double-click the **Object** lookup field. From the Lookup dialog box that is displayed, select the resource object that will be associated with the rule.

   If you want the rule to be accessible with all resource objects, select the **All Objects** check box.
7. When you want to assign the rule to one process, double-click the **Process** lookup field. From the Lookup dialog box that is displayed, select the process that will be associated with the rule.

   Caution: The only processes that appears within this Lookup window are ones that are associated with the resource object you selected in Step 6.

   If you want the rule to be accessible with all processes, select the **All Processes** check box.

Caution: If you have selected a resource object in Step 6, by selecting the **All Processes** check box, this rule will be accessible with every process that is associated with the selected resource object.

8. In the **Description** field, enter explanatory information about the rule.
9. Click **Save**. The rule is created. In addition, the tabs of this form are now functional.

Tabs on the Rule Designer Form

Once you launch the Rule Designer form, and create a rule, the tabs of this form become operational.

The Rule Designer form contains the following tabs:

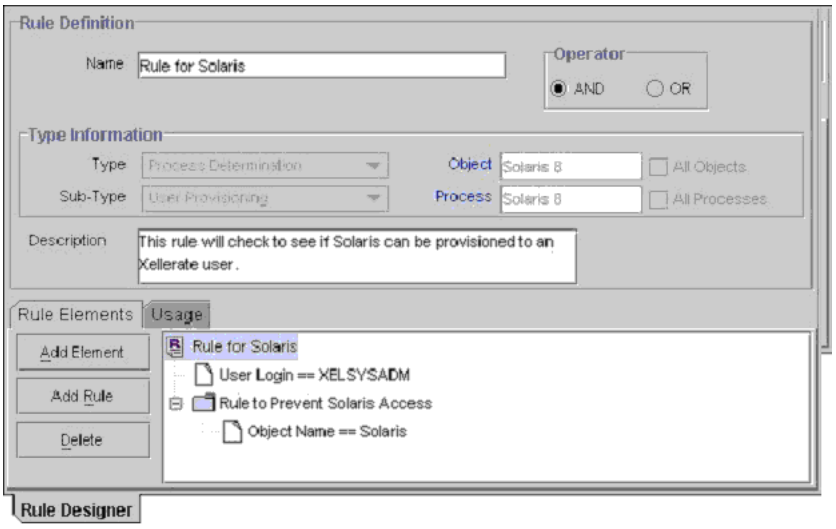
- Rule Elements
- Usage

Each of these tabs is covered in greater detail in the following sections.

Rule Elements

Figure 6–3 displays the Rule Elements tab of the Rule Designer form.

Figure 6–3 The Rule Elements Tab of the Rule Designer Form



Within this tab, you can create and manage the rule elements and/or the nested rules for a rule. For this example, the *Rule for Solaris* rule contains the *User Login==XELSYSADM* rule element. It also has the *Rule to Prevent Solaris Access* rule nested within it.

This rule is to be applied to a provisioning process that is associated with the *Solaris* resource object. Once this resource object is assigned to a request, the rule will be triggered. If the target user's login is *XELSYSADM*, and the name of the resource object is *Solaris*, the Solaris resource object will be provisioned to the user. Otherwise, the user will not be able to access Solaris.

When a rule element or nested rule is no longer valid, you need to remove it from the rule.

The following procedures will demonstrate how to:

- Add a rule element to a rule
- Add a nested rule to a rule
- Remove a rule element or nested rule from a rule

Add a Rule Element to a Rule

To add a rule element to a rule, perform the following steps:

1. Click **Add Element**. The Edit Rule Element dialog box is displayed.

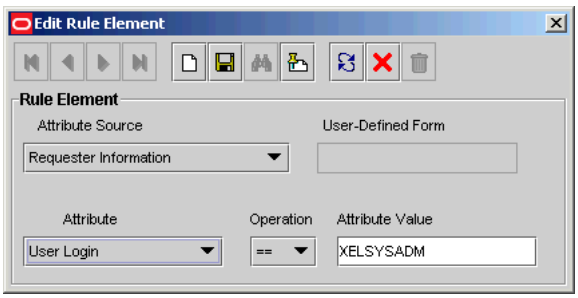
   The following table will help you understand the various data fields of the Edit Rule Element dialog box.

Name	Description
Attribute Source	From this combo box, select the source of the attribute. For example, if the attribute you wish to select is Object Name, the attribute source to select would be *Object Information*.
User-Defined Form	This field displays the user-created form that is associated with the attribute source that appears within the adjacent combo box. **Note**: If *Object Data* or *Process Data* do not appear within the **Attribute Source** combo box, the **User-Defined Form** field will be empty.
Attribute	From this combo box, select the attribute for the rule.
Operation	From this combo box, select the relationship between the attribute and the attribute value (== or !=)
Attribute Value	In this text box, enter the value for the attribute. **Note**: The attribute's value is case-sensitive.

> **Note:** The custom menus of the combo boxes of the Edit Rule Element dialog box will reflect the items that appear in the **Type** and **Sub-Type** combo boxes of the Rule Designer form.

2. Set the parameters for the rule you are creating, as shown in Figure 6–4.

Figure 6–4 Edit Rule Element Window -- Filled



For this example, if the Login ID of the target user is equal to *XELSYSADM*, the rule element is *TRUE*. Otherwise, it is *FALSE*.

Note: For more information on which parameters to select, refer to the "Rule Elements" on page 6-10.

3. From the Toolbar of the Edit Rule Element dialog box, click **Save**. Then, click **Close**. The rule element you created is displayed within the **Rule Elements** tab of the Rule Designer form.
4. From the main screen's Toolbar, click **Save**. The rule element is added to the rule.

Add a Nested Rule to a Rule

To add a nested rule to a rule, perform the following steps:

1. Click **Add Rule**. the Select Rule dialog box is displayed.
2. Select the desired nested rule and Click **Save**.

Caution: Only rules that are of the same type and sub-type, as the parent rule appears within the Select Rule window.

3. Then, click **Close**. The nested rule you selected appears within the **Rule Elements** tab of the Rule Designer form.
4. From the main screen's Toolbar, click **Save**. The nested rule is added to the rule.

Remove a Rule Element or Nested Rule From a Rule

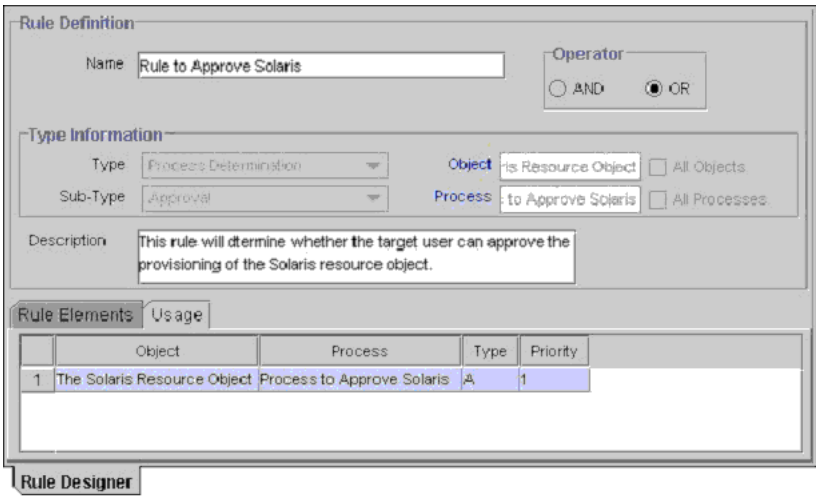
To remove a rule elemenet or nested rule from a rule, perform the following steps:

1. Highlight the rule element or nested rule that you want to remove.
2. Click **Delete**. The rule element or nested rule is removed from the rule.

Usage

Figure 6–5 displays the Usage tab of the Rule Designer form.

Figure 6–5 Usage Tab of the Rule Designer Form



Within this tab, you can see the following:

- The password policy, resource object, process, process task, auto-group membership criteria, user group, Oracle Identity Manager form field, and/or pre-populate adapter with which a rule is associated.
- A one-letter code, signifying the rule's classification type (A=Approval; P=Provisioning). This code appears for process determination rules only.
- The rule's priority number.

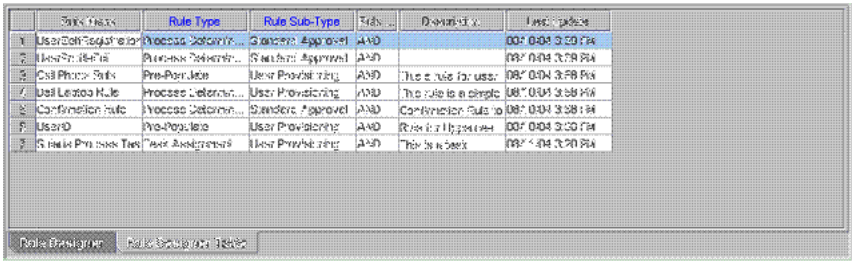
> **Note:** The type of information you can see within the **Usage** tab reflects the rule's classification type. For example, if the rule's type is **Pre-Populate**, the user-created field to which this rule is applied appears within this tab.

For this example, the *Rule to Approve Solaris* rule has been assigned to *The Solaris Resource Object* and the *Process to Approve Solaris*. Since this is an approval rule, its classification type is *A*. Lastly, the priority of this rule is *1*, indicating that it was the first approval rule that Oracle Identity Manager was scheduled to evaluate, once the corresponding resource object was assigned to a request.

Rule Designer Table

The Rule Designer Table, as shown in Figure 6–6, displays all available rules that were defined in the Rule Designer form.

Figure 6–6 The Rule Designer Table



The Rule Designer Table displays the following information:

Field Name	Description
Rule Name	This is the name of the rule.

Field Name	Description
Rule Type	The rule's classification status. A rule can belong to one of four types: ■ **General**: This type of rule enables Oracle Identity Manager to add a user to a user group automatically. It also determines the password policy that will be assigned to a resource object. ■ P**rocess Determination**: This type of rule determines the standard approval process that will be associated with a request, as well as the approval and provisioning processes that will be selected for a resource object. ■ T**ask Assignment**: This type of rule is used to determine which user and/or user group will be assigned to a process task. ■ **Pre-Populate**: This type of rule is used to determine which pre-populate adapter will be executed for a given form field.
Rule Sub-Type	For organizational purposes, when a rule's type is **Process Determination**, **Task Assignment**, or **Pre-Populate**, it can be further categorized into one of four sub-types: ■ **Organization Provisioning**: This sub-type further classifies the rule as a provisioning rule. It is used to determine the organization for which a process will be provisioned, a task will be assigned, or the pre-populate adapter will be applied. ■ **User Provisioning**: This sub-type further classifies the rule as a provisioning rule. It is used to determine the user for which a process will be provisioned, a task will be assigned, or a pre-populate adapter will be applied. ■ **Approval**: This sub-type further classifies the rule as an approval rule. It is used to approve the provisioning of resources to users or organizations. ■ **Standard Approval**: This sub-type further classifies the rule as a standard approval rule. It is used to approve a request.
Rule Operator	This is the relationship between the attribute and the attribute value (== or !=)
Description	Explanatory information about the rule.
Last Updated	This is the date when the rule was last updated.

The Resource Objects Form

The Resource Objects form is located in the Resource Management folder. It is used to create and manage the resource objects that represent the Oracle Identity Manager resources you want to provision for organizations or users.

Note: These definitions serve as templates to be used when provisioning the resource. How the resource is actually approved and provisioned will depend on the design of the approval and provisioning processes that you link to it.

Note: For more information on requests, and their relationship with resource objects, refer to "The Administrative Queues Form" on page 5-6.

The following table describes the data fields of the Resource Objects form.

Field Name	Description
Name	The resource object's name.
Table Name	The name of the resource object form (i.e. the name of the table which represents that form) associated with this resource.
Order For User/Order For Organization	These radio buttons are used to specify whether the resource object can be requested for users or organizations. To request the resource object for a user, select the **Order For User** radio button. To request the resource object for an organization, select the **Order For Organization** radio button.
Auto Pre-Populate	This check box designates whether a custom form, which: ■ Is associated with the resource object ■ Contains fields that have pre-populate adapters attached to them Will be populated by Oracle Identity Manager or a user. If the **Auto Pre-Populate** check box is selected, once the associated custom form appears, the fields that have pre-populate adapters attached to them will be populated by Oracle Identity Manager. When this check box is cleared, these fields must be populated by a user (by clicking the **Pre-Populate** button on the Toolbar). **Important**: This setting does not control the triggering of the pre-populate adapter. It merely determines whether the contents resulting from the execution of the adapter appear within the associated field because of Oracle Identity Manager or a user. For more information on pre-populate adapters, refer to *Oracle Identity Manager Tools Reference Guide*. **Note**: Setting this checkbox is only relevant if you have created a form that is to be associated with the resource object.
Type	The resource object's classification status. A resource object can belong to one of three types: ■ **Application**: Classifies this resource object as an application. ■ **Generic**: This type of resource object is comprised of business-related processes. ■ **System**: Oracle Identity Manager uses this type of resource object internally. A System Administrator should not modify system resource objects without first consulting Oracle.
Allow Multiple	This check box is used to designate whether the resource may be provisioned more than once to any given user or organizations. If it is selected, the resource object can be provisioned more than once per user or organization.

Field Name	Description
Auto Save	By selecting this check box, Oracle Identity Manager saves the data in any resource-specific form, created using the Form Designer form, without first displaying the form. If you select this checkbox, you must supply system data, a rule generator adapter, or an entity adapter to populate the form with the required data (since the user will not be able to access the form). **Note**: Setting this checkbox is only relevant if you have created a form for the provisioning of the resource object.
Self Request Allowed	By selecting this check box, users as well as the System Administrator can request the resource object for him/herself. **Note**: This functionality currently exists only for the Java version of Oracle Identity Manager. It is not applicable for the Oracle Identity Manager Administrative and User Console.
Allow All	By selecting this check box, the resource object can be requested for all Oracle users. This setting takes precedence over whether the organization to which a user belongs has allowed the resource to be requestable for its users.
Auto Launch	By default, this checkbox is checked at the time of object creation. Oracle Identity Manager will automatically initiate the provisioning process once the resource's approval process has achieved a status of *Completed*. Oracle Identity Manager automatically makes all resource objects set to Auto Launch, even though this checkbox is cleared.
Provision by Object Admin Only	This check box is used to designate who may provision this resource (either using direct provisioning or by manually initiated the provisioning process when the **Auto Launch** check box is cleared). If this check box is selected, only users who are members of the groups listed on the **Object Administrators** tab will be allowed to provision this resource object (either directly or by manually initiating the provisioning process from the request). If this check box is cleared, no restriction will be placed on who can direct provision this resource.

Now that we have reviewed the data fields of this form, you will learn how to create a resource object.

Create a Resource Object

To create a resource object, perform the following steps:

1. Open the Resource Objects form.
2. In the **Name** field, enter the name of the resource object.
3. Double-click the **Table Name** lookup field. From the Lookup dialog box that is displayed, select the table, which represents the form that will be associated with the resource object.
4. If you want to request the resource object for a user, then select the **Order For User** radio button. If you want to request the resource object for an organization, select the **Order For Organization** radio button.

Note: A resource object can be requested for either one user *or* one organization.

5. If a custom form is to be associated with the resource object, this form contains fields that have pre-populate adapters attached to them, and you want these fields to be populated automatically by Oracle Identity Manager, select the **Auto Pre-Populate** check box.

   If the fields of this form are to be populated manually (by a user clicking the **Pre-Populate** button on the Toolbar), clear the **Auto Pre-Populate** check box.

   Note: If the resource object has no custom form associated with it, or this form's fields have no pre-populate adapters attached to them, clear the **Auto Pre-Populate** check box. For more information on pre-populate adapters, refer to *Oracle Identity Manager Tools Reference Guide*.

6. Double-click the **Type** lookup field. From the Lookup dialog box that is displayed, select the classification status (**Application**, **Generic**, or **System**) that will be associated with the resource object.
7. If you want multiple instances of the resource object to be requested for a user or an organization, select the **Allow Multiple** check box. Otherwise, proceed to Step 8.
8. When you want Oracle Identity Manager to save the data in any resource-specific form (created using the Form Designer form) without first displaying the form, select the **Auto Save** check box. Otherwise, proceed to Step 9.

   Caution: If you select this check box, you must supply system data, a rule generator adapter, or an entity adapter to populate the form with the required data (since the user will not be able to access the form).

   Setting this checkbox is only relevant if you have created a form for the provisioning of the resource object.

9. If you want the System Administrator to be able to request the resource object for him/herself, select the **Self Request Allowed** check box. Otherwise, proceed to Step 10.
10. When you want the resource object to be provisioned for all users, regardless of whether the organization to which the user belongs has the resource object assigned to it, select the **Allow All** check box. Otherwise, proceed to Step 11.
11. If you want Oracle Identity Manager to automatically initiate the provisioning process when the resource object's approval process has achieved a status of *Completed*, select the **Auto Launch** check box. Otherwise, proceed to Step 12.

    Caution: By default, Oracle Identity Manager automatically makes all resource objects set to Auto Launch, even though this checkbox is cleared.

12. When you want to restrict the user groups that can provision this resource object, either directly or by assigning it to a request, to those groups that appear within the **Object Authorizers** tab of the Resource Objects form, select the **Provision by Object Admin** Only check box. Otherwise, proceed to Step 13.
13. Click **Save**. The resource object is created.

Tabs on the Resource Objects Form

Once you launch the Resource Objects form, and create a resource object, the tabs of this form become functional.

The Resource Objects form contains the following tabs:

Each of these tabs is covered in greater detail in the following sections.

Depends On

From this tab, you can select other resource objects that Oracle Identity Manager will need to provision before the current resource object can be provisioned. In addition, when Oracle Identity Manager can provision the current resource object without first provisioning the resource object that appears in the **Depends On** tab, you need to remove that resource object from the tab.

The following procedures will demonstrate how to:

- Select a resource object on which the current resource object is dependent
- Remove the dependent resource object

Select a Dependent Resource Object

To select a dependent resource object, perform the following steps:

1. Click **Assign**. The Assignment dialog box is displayed.
2. Select the resource object, and assign it to the request.
3. Click **OK**. The dependent resource object is selected.

Remove a Dependent Resource Object

To remove a dependent resource object, perform the following steps:

1. Highlight the dependent resource object you want to remove.
2. Click **Delete**. The resource object has been removed from the **Depends On** tab.

Object Authorizers

This tab is used to specify the user groups that are the Object Authorizers for this resource. The users who are members of these Object Authorizers groups can be selected as targets for task assignments. If you no longer want a user group to be an Object Authorizer, delete it from the list.

Each user group that appears within the **Object Authorizers** tab has a priority number assigned to it. The priority number is evaluated when Oracle Identity Manager is determining the user to whom to assign a task (when the task assignment target is *Object Authorizer user with highest priority*). Alternately, the priority value can be referenced when a task assigned to a group is escalated due to lack of action. You can also increase or decrease the priority number for any user group that is displayed within this tab.

As an example, assume that members of the *SYSTEM ADMINISTRATORS* user groups have been specified as Object Authorizers. If a process task associated with this resource object has a task assignment rule attached to it, and the assignment criteria is **Object Authorizer User with Highest Priority**, the first user who is authorized to complete this process task is the user with the highest priority who belongs to the *SYSTEM ADMINISTRATORS* user group (since its priority number is *1*). If this user does not complete this process task within a user-specified time, Oracle Identity Manager will reassign the task to the user in the *SYSTEM ADMINISTRATORS* group who has the next highest priority.

> **Note:** For more information on task assignment rules and their relationship with completing process tasks, refer to "The Rule Designer Form" and "Assignment" on page 7-29.

The following procedures will show how to:

- Assign a user group to a resource object
- Remove a user group from a resource object
- Change the priority number for a user group

Assign a User Group to a Resource Object

To assign a user group to a resource object, perform the following steps:

1. Click **Assign**. The Assignment dialog box is displayed.
2. Select a user group, and assign it to the resource object.
3. Click **OK**. The user group is selected.

Remove a User Group From a Resource Object

To remove a user group from a resource object, perform the following steps:

1. Highlight the desired user group.
2. Click **Delete**. The user group is removed from the **Object Authorizers** tab.

Change a User Group's Priority Number

To change a user group's priority number, perform the following steps:

1. Highlight the user group whose priority number you wish to change.

2. To raise the selected user group's priority number by one, click **Increase**. To lower this user group's priority by one, click **Decrease**.

   Note: To increase or decrease a user group's priority number by more than one, click the appropriate button repeatedly. As an example, to raise the priority number of a user group by two, click the **Increase** button *twice*.

3. Click **Save**. The user group's priority number is now changed to the value you selected.

Process Determination Rules

A request is one mechanism used to provision Oracle Identity Manager resources to users or organizations. Through a request, a user can approve the provisioning of these resources to the target users or organizations. However, a request cannot be acted on until a resource object is assigned to it. Each resource object is comprised of one (or more) provisioning process and potentially one (or more) approval process.

As mentioned, the resource object definition serves as a template to be referenced when the resource is being provisioned to users or organizations. Since the resource definition may be linked to multiple approval and provisioning processes, Oracle Identity Manager must know which approval process and provisioning process to execute when the resource is requested or direct provisioned to users or organizations. This determination is made using the use of process determination rules.

Process determination rules are criteria. These rules are used by Oracle Identity Manager to determine which:

- Approval and provisioning process to select when a resource is requested
- Provisioning process to select when a resource is direct provisioned

Usually, each approval process and provisioning process has a process determination rule associated with it. In addition, every rule/process combination has a priority number, which indicates the order in which Oracle Identity Manager will evaluate it.

For this example, when the resource is requested or direct provisioned, Oracle Identity Manager will evaluate the *Rule to See if Solaris is Needed* and *Rule to Check Provisioning of Solaris for IT Dept*. rules (since they both have the highest priority). If the conditions of these rules were **TRUE**, Oracle Identity Manager will execute the processes associated with them (the *Check if Solaris is Needed* approval process and the *Provision Solaris for IT Dept*. provisioning process).

If the condition of a rule is **FALSE**, Oracle Identity Manager will then evaluate the rule with the next highest priority. If that rule is **TRUE**, Oracle Identity Manager will execute the process associated it.

So, in this example, if the resource was requested or direct provisioned and the *Rule to Check Provisioning of Solaris for IT Dept*. rule FALSE, Oracle Identity Manager would evaluate the *Rule to Check Provisioning of Solaris for Developers* rule. If this rule were TRUE, Oracle Identity Manager would execute the process associated with that rule (the *Provision Solaris for Devel*. provisioning process).

Now that we have reviewed process determination rules, you will learn how to add a process determination rule to a resource object. In addition, when an existing rule is no longer valid, you will learn how to remove it from the resource object.

Add a Process Determination Rule to a Resource Object

To add a process determination rule to a resource object, perform the following steps:

1. Click **Add** in either the **Approval Processes** or **Provisioning Processes** region, depending on the rule/process combination you intend to create.
2. From the row that is displayed, double-click the **Rules** lookup field.
3. From the Lookup dialog box that is displayed, select a rule, and assign it to the resource object only rules of type *Process Determination* is available for selection).
4. Click **OK**.
5. Within the adjacent column, double-click the **Processes** lookup field.
6. From the Lookup dialog box that is displayed, select the desired process, and assign it to the rule.
7. Click **OK**.
8. Enter a numeric value in the **Priority** field. This will determine the order in which Oracle Identity Manager evaluates the rule/process combination.
9. Click **Save**. The rule/process combination is added to the resource object.

Remove a Process Determination Rule From a Resource Object

To remove a process determination rule from a resource object, perform the following steps:

1. Highlight the desired rule/process combination.
2. Click **Delete**. The rule/process combination is removed from the resource object.

Event Handlers/Adapters

Sometimes, a resource object may have data that needs to be handled in a particular fashion. For example, a resource object's provisioning process may contain tasks, which must be completed automatically.

When this occurs, you must assign either an event handler or an adapter to the resource object. An event handler is a software routine that provides the processing of this specialized information. An adapter is a specialized type of event handler that generates the Java code, which enables Oracle Identity Manager to communicate and interact with external resources.

Also, when an event handler or adapter, which has been assigned to a resource object, is no longer valid, you must remove it from the resource object.

For this example, the *adpAUTOMATEPROVISIONINGPROCESS* adapter has been assigned to the *Solaris* resource object. Once this resource object is assigned to a request, Oracle Identity Manager will trigger the adapter, and the associated provisioning process is executed automatically.

The following procedures demonstrate how to assign an event handler or adapter to a resource object, and remove an event handler or adapter from a resource object.

Assign an Event Handler or Adapter to a Resource Object

To assign an event handler or adapter to a resource object, perform the following steps:

1. Click **Assign**. The Assignment dialog box is displayed.
2. Select an event handler, and assign it to the resource object.
3. Click **OK**. The event handler is assigned to the resource object.

Remove an Event Handler or Adapter From a Resource Object

To remove an event handler or adapter from a resource object, perform the following steps:

1. Highlight the desired event handler.
2. Click **Delete**. The event handler is removed from the resource object.

Status Definition

This tab is used to set the provisioning statuses for a resource object. A **provisioning status** indicates the status of the resource object throughout its entire lifecycle, until it is provisioned to the target user or organization. Once this occurs, you can see the provisioning status of the resource object from within the Status region of the **Currently Provisioned** tab.

Every provisioning status of a resource object is associated with a task status of the relevant provisioning process (which Oracle Identity Manager selects when the resource object is assigned to a request). For example, if the *Provision for Developers* process is selected, and a task within this process achieves a status of *Completed*, the corresponding status of the resource object can be set to Provisioned. This way, you can see how the resource object relates to the provisioning process, quickly and easily.

Currently, a resource object has eight pre-defined statuses:

- **Waiting**: Oracle Identity Manager has checked and has found that there are other resource objects upon which this resource object depends. However, these resource objects have not yet been provisioned.
- **Revoked**: The resources, represented by the resource object, have been provisioned to the target users or organizations. However, these users or organizations have been permanently de-provisioned from using the resources.
- **Ready**: Oracle Identity Manager has checked and has found that [a] this resource object is not dependent upon any other resource objects; or [b] all resource objects, upon which this resource object depends, have been provisioned.

  Once the resource object's status is *Ready*, it evaluates the process determination rules to determine the approval and provisioning processes once the resource object is assigned to a request. When this happens, the status of the resource object changes to *Provisioning*.
- **Provisioning**: The resource object has been assigned to a request, and an approval process and a provisioning process have been selected.
- **Provisioned**: The resources, represented by the resource object, have been provisioned to the target users or organizations.
- **Provide Information**: Additional information is required before the resources, represented by the resource object, can be provisioned to the target users or organizations.
- **None**: This status does not represent the provisioning status of the resource object. Rather, it signifies that a task, which belongs to the provisioning process that Oracle Identity Manager selects, has no effect on the status of the resource object.
- **Enabled**: The resources, represented by the resource object, have been provisioned to the target users or organizations. In addition, these users or organizations have access to the resources.

- **Disabled**: The resources, represented by the resource object, have been provisioned to the target users or organizations. However, these users or organizations have temporarily lost access to the resources.

Each provisioning status has a corresponding **Launch Dependent** check box. If a check box is selected, and the resource object achieves that provisioning status, Oracle Identity Manager enables other, dependent resource objects to launch their own provisioning processes.

For this example, the *Exchange* resource object has the **Launch Dependent** check box selected for the *Provisioned* and *Enabled* provisioning statuses. Once the provisioning status of this resource object changes to *Provisioned* and *Enabled*, Oracle Identity Manager checks to see if there are other resource objects, upon which the *Exchange* resource object depends. If this is so, Oracle Identity Manager first launches the approval and provisioning processes of these dependent objects. Then, Oracle Identity Manager selects an approval and provisioning process for the *Exchange*.

You may want to add additional provisioning statuses to a resource object to reflect the various task statuses of a provisioning process. For example, when the status of a task that belongs to a provisioning process is *Rejected*, you may want to set the corresponding provisioning status of the resource object to *Revoked*.

Similarly, when an existing provisioning status is no longer valid, you need to remove it from the resource object.

The following procedures demonstrate how to add a provisioning status to a resource object, and remove a provisioning status from a resource object.

Add a Provisioning Status to a Resource Object

To add a provisioning status to a resource object, perform the following steps:

1. Click **Add**.
2. Add a provisioning status in the **Status** field.
3. When you want other, dependent resource objects to launch their own approval and provisioning processes once the resource object achieves the provisioning status you are adding, select the **Launch Dependent** check box. Otherwise, proceed to Step 4.
4. Click **Save**. The provisioning status is added to the resource object.

Remove a Provisioning Status from a Resource Object

To remove a provisioning status from a resource object, perform the following steps:

1. Highlight the desired provisioning status.
2. Click **Delete**. The provisioning status is removed from the resource object.

Administrators

This tab is used to select the user groups that can view, modify, and delete the current resource object.

The **Write** and **Delete** check boxes are visual indicators of the privileges that a user group has with the resource object. When the **Write** check box is selected, the corresponding user group can modify the current resource object. If this check box is cleared, the user group cannot edit the resource object.

Similarly, when the **Delete** check box is selected, the associated user group can delete the current resource object. If this check box is cleared, the user group cannot delete the resource object.

For this example, the *SYSTEM ADMINISTRATORS* user group can view, modify, and delete the *Solaris* resource object. The *OPERATORS* user group can only view and modify this resource object (Its **Delete** check box is cleared.).

The following sections describe how to assign a user group to a resource object, and remove a user group from a resource object.

Assign a User Group to a Resource Object

To assign a user group to a resource object, perform the following steps:

1. Click **Assign**. The Assignment dialog box is displayed.
2. Select the user group, and assign it to the resource object.
3. Click **OK**. The user group appears in the **Administrators** tab. By default, all members of this group can view the active record.
4. If you want this user group to be able to modify the current resource object, double-click the corresponding **Write** check box. Otherwise, proceed to Step 5.
5. If you want this user group to be able to delete the current resource object, double-click the associated **Delete** check box. Otherwise, proceed to Step 6.
6. Click **Save**. The user group is assigned to the resource object.

Remove a User Group from a Resource Object

To remove a user group from a resource object, perform the following steps:

1. Highlight the user group that you want to remove.
2. Click **Delete**. The user group is removed from the resource object.

Password Policies Rule

If a resource object is of type **Application**, and you want to provision the resource object to a user or organization, you may want that user or organization to meet password criteria before accessing the resource object. This password criteria is created and managed in the form of password policies. These policies are created using the Password Policies form.

As the resource object definition is only a template for governing how a resource is to be provisioned, Oracle Identity Manager must be able to make determinations about how to provision the resource based on actual conditions and rules. These conditions may not be known until the resource is actually requested. Therefore, rules must be linked to the various processes and password policies associated with a resource to allow Oracle Identity Manager to decide which ones to invoke in any given context.

Oracle Identity Manager determines which password policy to apply to the resource when creating (or updating) a particular user's account by evaluating the password policy rules of the resource and applying the criteria of the policy associated with the first rule that is satisfied. Each rule has a priority number, which indicates the order in which Oracle Identity Manager will evaluate it.

For this example, Oracle Identity Manager will trigger the *Rule to Prevent Solaris Access* rule (since it has the highest priority). If this rule were **TRUE**, Oracle Identity Manager would apply the criteria of the *Restrict Solaris* password policy to the password of the account being created or updated.

If the rule is **FALSE**, Oracle Identity Manager will then evaluate the rule with the next highest priority. If this rule is **TRUE**, Oracle Identity Manager will apply the password policy associated with it to the password of the account being created or updated.

Now that we have reviewed about password policy rules, you will learn how to add a password policy rule to a resource object. In addition, when an existing rule is no longer valid, you will learn how to remove it from the resource object.

Add a Password Policy Rule to a Resource Object

To add a password policy rule to a resource object, perform the following steps:

1. Click **Add**.
2. From the row that appears, double-click the **Rule** lookup field.
3. From the Lookup dialog box that is displayed, select a rule, and assign it to the resource object.
4. Click **OK**.
5. Within the adjacent column, double-click the **Policy** lookup field.
6. From the Lookup dialog box that is displayed, select an associated password policy, and assign it to the resource object.
7. Click **OK**.
8. Add a numeric value in the **Priority** field. This field contains the rule's priority number.
9. Click **Save**. The password policy rule is added to the resource object.

Remove a Password Policy Rule From a Resource Object

To remove a password policy rule from a resource object, perform the following steps:

1. Highlight the desired password policy rule.
2. Click **Delete**. The password policy rule is removed from the resource object.

User-Defined Fields

This tab is used to view and access any user-defined fields that have been created for the Resource Objects form. Once a user-defined field has been created, it appears on this tab and be able to accept and supply data. For instructions on how to create user-defined fields on existing Oracle Identity Manager forms, refer to "The User Defined Field Definition Form" on page 8-7.

Process

The **Process** tab displays all of the approval and provisioning processes that are associated with the current resource object. In addition, this tab indicates (using the **Default** check boxes), which approval or provisioning processes have been designated as the default process of each type for the resource.

Note: Approval and provisioning processes are created and associated with a resource using the Process Definition form. Each process can then be linked to a process determination rule using the **Process Determination Rules** tab of the Resource Object form.

For this example, the *Solaris* resource object has one approval processes assigned to it. It also has the provisioning processes (*Provision Solaris for Devel.*) associated with it. The *Provision Solaris for Devel*. provisioning process has been designated as the default processes for this resource object.

Object Reconciliation

This tab contains two sub-tabs, Reconciliation Fields and Reconciliation Action Rules.

- The **Reconciliation Fields** tab is used to define the fields on the target resources/trusted sources that are to be reconciled with (for example, mapped to) information in Oracle Identity Manager
- The **Reconciliation Action Rules** tab is used to specify the actions Oracle Identity Manager is to take when particular matching conditions are met.

Reconciliation Fields Tab

This tab is used to define the fields on the target resources/trusted sources that are to be reconciled with (for example, mapped to) information in Oracle Identity Manager. For each field on the target system/trusted source, the following information will be listed:

- Name of the field on the target resource/trusted source that is to be reconciled with data in Oracle Identity Manager (for example, *targetfield1*)
- Data type associated with the field (for example, *String*). Possible values are *Multi-Valued*, *String*, *Number*, *Date*, *IT resource*
- Indicator designating whether this field is required within a reconciliation event

> **Note:** Oracle Identity Manager will not begin to match potential provisioning processes, users or organizations to the reconciliation event until all fields which have been set as required are processed on the **Reconciliation Data** tab of the Reconciliation Manager form.

An example of a target system field definition might appears as follows:

```
TargetField1 [String], Required
```

Add a Reconciliation Field

The following steps are used to add a field from the target system/trusted source to the list of fields that are to be reconciled with information within Oracle Identity Manager.

> **Note:** For a trusted source, this must be the *user* resource definition.

1. Click **Add Field**. The Add Reconciliation Field dialog box is displayed.
2. Enter the name of the field on the target resource/trusted source in the **Field Name** field. This is the name by which you wish to reference the target resource/trusted source field within Oracle Identity Manager.
3. Select one of the following values from the menu in the **Field Type** field:
   - Multi-Valued (for use with fields that contain one or more component fields)
   - String

- String
- Date
- IT resource (only to be used with fields that will reference the machine on the user account is provisioned)

4. Set the **Required** check box. If this checkbox is selected, this field must be processed on the **Reconciliation Data** tab of the Reconciliation Manager form before Oracle Identity Manager will begin attempting to match a provisioning process or user/organization to the reconciliation event. If this checkbox is cleared, the inability to process this field within a reconciliation event will not prevent matching from occurring.
5. Click **Save**. The field will be available for mapping within the resource's default provisioning process.

Note: Before Oracle Identity Manager can successfully perform reconciliation with an external target resource/target source, the fields you have defined on this tab must be mapped to the appropriate Oracle Identity Manager fields using the **Field Mappings** tab of the resource's default provisioning process.

Delete a Reconciliation Field

The following steps are used to remove a target system field from the list of fields that are to be reconciled with information within Oracle Identity Manager.

Note: For a trusted source, this must be the *user* resource definition.

1. Select the field you wish to remove.
2. Click **Delete Field**. The selected field will be removed from the list of fields with which Oracle Identity Manager attempts to reconcile data on the target system (this will have no affect on the data in the target system itself).

Reconciliation Action Rules Tab

This tab is used to specify the actions Oracle Identity Manager is to take when particular matching conditions are met. Oracle Identity Manager allows you to specify what action(s) it should automatically take when certain matches within reconciliation event records are encountered. Each record within this tab is a combination of:

- The matching condition criteria
- The action to take

The conditions and actions from which you may select are pre-defined. Depending on the matching conditions, certain actions may not be applicable. A complete list of the available options is provided below:

Rule Condition	Possible Rule Actions
No matches found	None
	Assign to Administrator with Least Load
	Assign to Authorizer with Highest Priority
	Assign to Authorizer with Least Load
	Assign to User
	Assign to Group
	Create User (only available with the trusted source)
One Process Match Found	None
	Assign to Administrator with Least Load
	Assign to Authorizer with Highest Priority
	Assign to Authorizer with Least Load
	Assign to User
	Assign to Group
	Establish Link
Multiple Process Matches Found	None
	Assign to Administrator with Least Load
	Assign to Authorizer with Highest Priority
	Assign to Authorizer with Least Load
	Assign to User
	Assign to Group
One Entity Match Found	None
	Assign to Administrator with Least Load
	Assign to Authorizer with Highest Priority
	Assign to Authorizer with Least Load
	Assign to User
	Assign to Group
	Establish Link
Multiple Entity Matches Found	None
	Assign to Administrator with Least Load
	Assign to Authorizer with Highest Priority
	Assign to Authorizer with Least Load
	Assign to User
	Assign to Group

Add a Reconciliation Action Rule

To add a reconciliation action rule, perform the following steps:

1. Click **Add Field**. The **Add a new Action Rule** dialog box is displayed.
2. Select the desired value from the **Rule Condition** menu. This is the matching condition that will cause the associated action to be executed. Each match condition can only be assigned to a single rule action.
3. Select the desired value from the **Rule Action** menu. This is the action that will be executed if the matching condition is satisfied.

4. Click **Save**, and close the Add a new Action Rule dialog box.

Delete a Reconciliation Action Rule

1. Select the matching condition/action combination you wish to delete.
2. Click **Delete**. The reconciliation action rule will be removed and the action associated with its condition will not be executed automatically.

Service Account Management

Oracle Identity Manager supports service accounts. Service accounts are general administrator accounts (for example, admin1, admin2, admin3, etc.) that are used for maintenance purposes, and are typically shared by a set of users. The model for managing and provisioning service accounts is slightly different from normal provisioning.

Service accounts are requested, provisioned, and managed in the same manner as regular accounts. They use the same resource objects, provisioning processes, and process/object forms as regular accounts. A service account is distinguished from a regular account by an internal flag.

When a user is provisioned with a service account, Oracle Identity Manager manages a mapping from the user's identity to the service account. When the resource is "revoked", or the user gets "deleted", the provisioning process for the service account does not get cancelled (which would cause the undo tasks to fire). Instead, a task is inserted into the provisioning process (the same way Oracle Identity Manager handles Disable/Enable actions). This task removes the mapping from the user to the service account, and returns the service account to the pool of available accounts.

This management capability is exposed through APIs.

7

Process Management

This chapter describes the process management in Oracle Identity Manager. It contains the following topics:

Overview

The Process Management folder provides System Administrators with the tools necessary to create and manage Oracle Identity Manager processes and e-mail templates. This folder contains the following forms:

This folder contains the following forms:

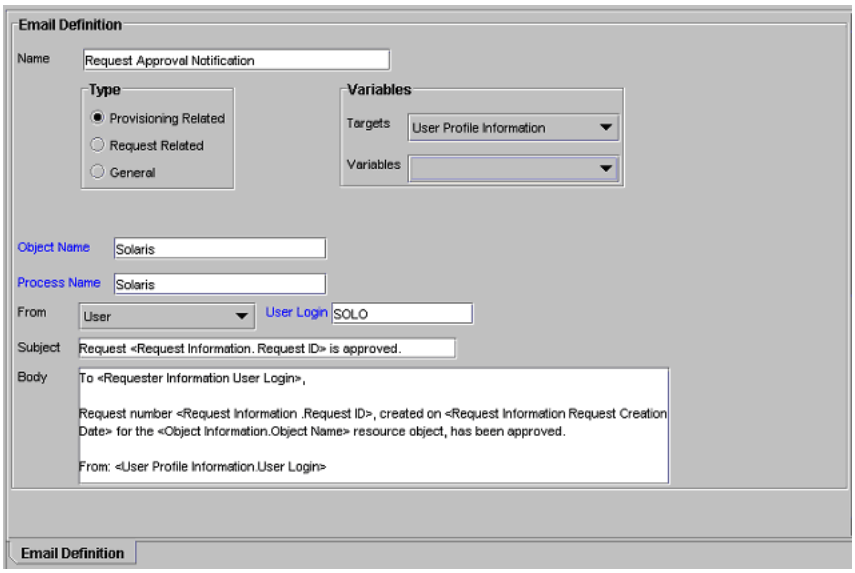
- **Email Definition**: Through this form, a System Administrator can create templates for e-mail notifications.
- **Process Definition**: This form is used to create and manage approval and provisioning processes. It also allows you to launch the Workflow Definition Renderer that displays your workflow definition in a graphical presentation.

The Email Definition Form

The Email Definition form, as shown in Figure 7–1, is located within the Process Management folder. It is used to create templates (or definitions) for e-mail notifications. These notifications can be set to be sent to the user when:

- A task is assigned to the user
- The task achieves a particular status
- A request is approved (the standard approval process has a status of Completed)

Figure 7–1 The Email Definition Form



For this example, an e-mail definition has been created. Once the request, which is represented by the Request ID e-mail variable, has been approved, an e-mail notification will be sent from User(SOLO) to the user who created the request (or the requester).

Important: Before using the E-mail Definition form, you must specify the address of the e-mail server that Oracle Identity Manager will use to send e-mail notifications to users

First, you need to launch the System Configuration form, query for the EMAILSERVER property, and ensure that it is set to the name of the resource asset instance that represents your e-mail server.

Next, you must open the IT Resources form and query for the EMAILSERVER IT resource (or whatever name of the resource asset is associated with your mail server.

Once this IT resource appears, you have to specify the IP address of the e-mail server, along with the name and password of the user who validates the usage of this server.

For more information, refer to "The System Configuration Form" on page 8-14, and "The IT Resources Form" on page 6-4.

Now that we have reviewed about e-mail definitions, you will learn about the data fields of the Email Definition form. The following table describes the fields of this form.

Field Name	Description
Name	The name of the e-mail definition.

Field Name	Description
Type	This region contains three radio buttons. These radio buttons are used to specify whether: ■ The e-mail definition is to be categorized as related to a request or a provisioning process. ■ A variable for the e-mail definition will be associated with a request or a provisioning process. ■ A variable for the email definition to be associated with a general process. If the e-mail definition is to be classified as a provisioning definition, or the e-mail variable is associated with a provisioning process, select the **Provisioning Related** radio button. When the e-mail definition will be categorized as a request definition, or the e-mail variable is associated with a request, select the **Request Related** radio button. If the e-mail definition is categorized as a general announcement, then select the **General** radio button.
Object Name	From this lookup field, select the resource object that is associated with the provisioning process to which the e-mail definition is related. **Note**: If you leave this lookup field empty, the e-mail definition will be available for use with all resource objects.
Process Name	From this lookup field, select a provisioning process that has been assigned to the selected resource object. This is the provisioning process to which the e-mail definition is to be related. **Note**: If the **Provisioning Related** radio button is not selected, both the **Object Name** and **Process Name** lookup fields are disabled.
Targets	From this combo box, select the source of the variable for the e-mail definition. For example, if the variable you wish to select were Request Name, the source to select would be Request Information. **Note**: The items that appear within this combo box reflect the radio button you select from the Type region.
Variables	From this combo box, select the variable for the e-mail definition (for example, Request Name). The variables, which appear within this combo box, reflect the items you select from the Targets box. **Note**: For more information on e-mail variables and their parameters, refer to "E-Mail Variables" on page A-8.
From	Currently, two types of users can be selected from this combo box: ■ **Requester**: The user who created the request. ■ **User**: Any Oracle User with an e-mail address, which appears in the **Contact Information** tab of their Users form.
User Login	The ID of the user who appears in the From region of the e-mail notification. **Note**: If the User item does not appear in the From combo box, the **User Login** field is disabled.
Subject	The title (or subject) of the e-mail definition.
Body	The content (or body) of the e-mail definition.

Now that we have reviewed e-mail definitions and the data fields of the E-mail Definition form, you are ready to create an e-mail definition.

Create an E-mail Definition

To create an e-mail definition, perform the following steps:

1. Open the Email Definition form.
2. In the **Name** field, type the name of the e-mail definition.
3. If the e-mail definition is to be used with a provisioning process, select the **Provisioning Related** radio button. When the e-mail definition is to be associated with a request, select the **Request Related** radio button.

   Important: If the **Request Related** radio button is selected, ensure that the name of the e-mail server appears in the **Value** field of the EMAILSERVER property for the System Configuration form.

4. Click **Save**. The remaining data fields of the Email Definition form are now operational.
5. Double-click the **Object Name** lookup field. From the Lookup dialog box that appears, select the resource object that is associated with the provisioning process to which this e-mail definition is related.

   Note: By leaving this lookup field empty, the e-mail definition will be available for use with all resource objects.

6. Double-click the **Process Name** lookup field. From the Lookup dialog box that is displayed, select a provisioning process that has been assigned to the resource object you selected in Step 5. This is the provisioning process to which this e-mail definition is to be related.

   Note: If the Provisioning Related radio button is not selected, both the Object Name and Process Name lookup fields are disabled.

7. Click the **From** combo box. From the custom menu that is displayed, select the type of the user (**Requester**, **User**, or **Manager of Provisioned User**) who appears in the From region of the e-mail notification.

   Note: If the **Provisioning Related** radio button is not selected in Step 3, the **Manager of Provisioned User** item will not appear in the **From** combo box.

8. *Optional*. If you selected the User option in the **From** combo box, double-click the **User Login** lookup field. From the Lookup dialog box that appears, select the ID of the user who appears in the From region of the e-mail notification.

   If you did not select the User item in the From combo box, the User Login field is disabled.

9. Add information in the **Subject** field. This field contains the title (or subject) of the e-mail definition.
10. Add information in the Body text area. This text area contains the content (or body) of the e-mail definition.

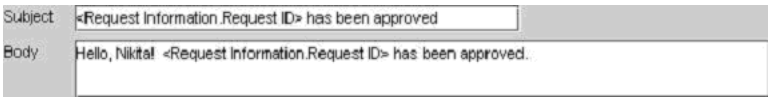
11. When necessary, populate the Subject field and Body text area with e-mail variables.

    The following table will help you understand the various radio buttons and combo boxes, which will enable you to customize an e-mail variable for the e-mail definition.

Name	Description
Type	These radio buttons are used to specify whether a variable for the e-mail definition will be related to a provisioning process or a request. When the e-mail variable is to be associated with a provisioning process, select the **Provisioning Related** radio button. If the variable is related to a request, select the **Request Related** radio button.
Targets	From this combo box, select the source of the variable for the e-mail definition. For example, if the variable you wish to select were Request Name, the source to select would be Request Information.
Variables	From this combo box, select the variable for the e-mail definition (for example, *Request Name*).

> **Note:** The items that appear in the custom menu of the **Targets** combo box reflect the selection of either the **Provisioning Related** or the **Request Related** radio button. Similarly, the items, which are displayed in the custom menu of the **Variables** combo box, correspond to the items that appear in the **Targets**, **Location Types**, and **Contact Types** combo boxes.

12. Create an e-mail variable for the Subject field or Body text area.



    For this example, the number of the request that has been approved (the *Request ID*) appears in both the **Subject** field and the **Body** text area.

13. Click **Save**. The e-mail definition is created. It can be applied through the **Assignment** tab of the Process Definition form.

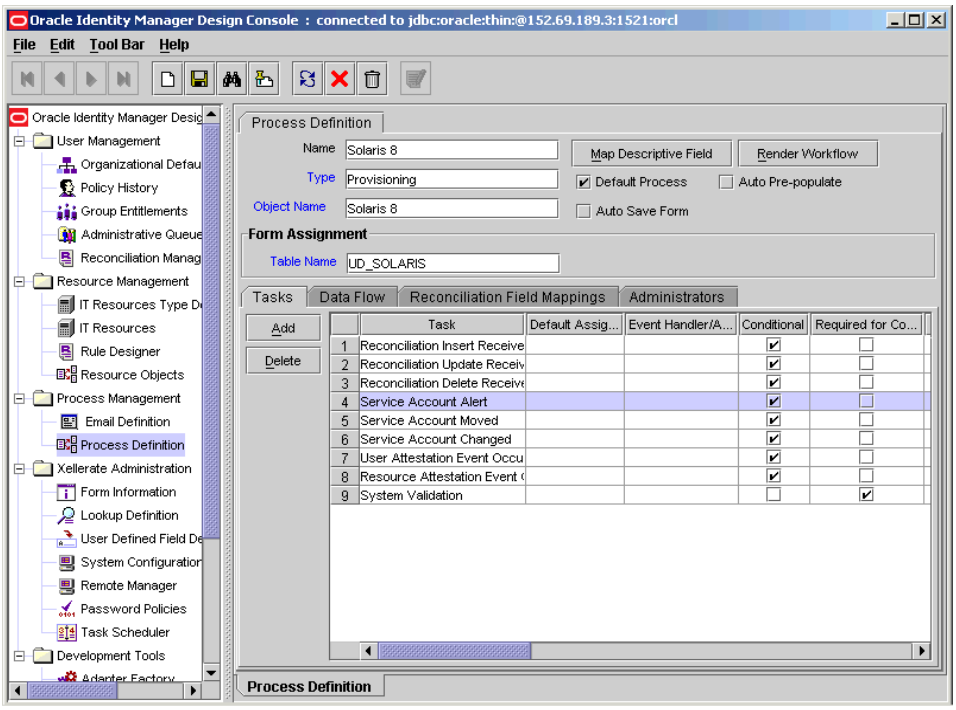
The Process Definition Form

A process is the mechanism by which a logical workflow (whether used for approvals or provisioning) is represented within Oracle Identity Manager. Process definitions are comprised of tasks. These process tasks represent the steps that must be completed in order to fulfill the purpose of the process. For example, within an approval process, the tasks are used to represent the individual approvals that must be obtained before a particular action can take place. Within a provisioning process, the tasks are used to actually enable access for a user or organization on the target resource.

The Process Definition form, as shown in Figure 7–2, is located in the Process Management folder. It is used to create and manage the approval and provisioning processes that you associate with your resource objects.

Note: The *standard approval process*, associated with the *Request* object, can also be managed using this form.

Figure 7–2 The Process Definition Form



For this example, the *Solaris 8* provisioning process has been created and assigned to the Solaris 8 resource object.

Now that we have reviewed about processes, you will learn about the data fields of the Process Definition form. The following table describes the fields of this form.

Field Name	Description
Name	The name of the process.
Type	The classification type of the process definition. Currently, a process definition can be categorized as either an Approval or a Provisioning process.
Object Name	The name of the resource object to which the process will be assigned.
Map Descriptive Field	By clicking this button, you can select a field that will be used as an identifier of the process definition, once an instance is assigned to a resource object.
Render Workflow	Clicking this button will launch a web browser and the Workflow Renderer tool will display the current workflow definition.

Field Name	Description
Default Process	This check box is used to determine whether the current process is to be designated as the default approval or provisioning process for the resource object with which it is associated. By selecting the check box, the process will be set as the default approval or provisioning process for the resource object to which it is assigned.If you clear the check box, the process will not be the default approval or provisioning process for the resource object with which it is associated and will only be invoked if a process selection rule causes it to be chosen.
Auto Save Form	This check box is used to designate whether Oracle Identity Manager should suppress display of the custom form associated with this provisioning process or display it and allow a user to supply it with data each time the process is instantiated. If you select this check box, it designates that Oracle Identity Manager should automatically save the data in the custom process form without first displaying the form. If you select this checkbox, you must supply either system-defined data or ensure that an adapter is configured to populate the form with the required data (since the user will not be able to access the form).If you clear this check box, it designates that Oracle Identity Manager should display the custom process form and allow users to enter data into its fields.
Auto Pre-Populate	This check box designates whether the fields of a custom form that: ■ Are associated with the process ■ Contain fields that have pre-populated adapters attached to them Will be populated by Oracle Identity Manager or a user. If the **Auto Pre-Populate** check box is selected, once the associated custom form appears, the fields that have pre-populate adapters attached to them will be populated by Oracle Identity Manager. When this check box is cleared, these fields must be populated by a user (by clicking the **Pre-Populate** button on the Toolbar or by a user manually entering the data). **Important**: This setting does not control the triggering of the pre-populate adapter. It merely determines whether the contents resulting from the execution of the adapter appear within the associated form field(s) because of Oracle Identity Manager or a user. For more information on pre-populate adapters, refer to *Oracle Identity Manager Tools Reference Guide*. **Note**: Setting this checkbox is only relevant if you have created a process form (that is to be associated with the process) and pre-populate adapters are used with that form.
Table Name	The name of the table, which represents the form that is associated with the process definition.

Now that we have reviewed processes and the data fields of the **Process Definition** form, you are ready to create a process definition.

Create a Process Definition

To create a process definition, perform the following steps:

1. Open the Process Definition form.

2. In the **Name** field, type the name of the process definition.
3. Double-click the **Type** lookup field. From the Lookup dialog box that is displayed, select the classification type (Approval or Provisioning) of the process definition.
4. Double-click the **Object Name** lookup field. From the Lookup dialog box that is displayed, select the resource object that will be associated with the process definition.
5. *Optional*. Select the **Default Process** check box. By doing so, the process will be the default approval or provisioning process for the resource object to which it is assigned.

   If you do not want to designate the current process definition as the default approval or provisioning process for the resource object with which it is associated, proceed to Step 6.
6. *Optional*. Select the **Auto Save Form** check box. This denotes that Oracle Identity Manager should suppress display of provisioning process' custom form and automatically save the data in it. This setting is only applicable to provisioning processes.

   If you want Oracle Identity Manager to display provisioning process' custom form and solicit users for information, clear this check box.

   Important: If you select the **Auto Save Form** check box, make sure that all fields of the associated "custom" process form have adapters associated with them. However, a process form can have default data or object to the process data flow mapping or organization defaults.

   For more information on adapters and their relationship with fields of custom forms, refer to *Oracle Identity Manager Tools Reference Guide*.
7. If a custom form is to be associated with the process definition, this form contains fields that have pre-populate adapters attached to them, and you want these fields to be populated automatically by Oracle Identity Manager, select the **Auto Pre-Populate** check box.

   If the fields of this form are to be populated manually (by an user clicking the **Pre-Populate** button on the Toolbar), clear the **Auto Pre-Populate** check box.

   Note: If the process definition has no custom form associated with it, or this form's fields have no pre-populate adapters attached to them, clear the **Auto Pre-Populate** check box. For more information on pre-populate adapters, refer to *Oracle Identity Manager Tools Reference Guide*.
8. Double-click the **Table Name** lookup field. From the Lookup window that appears, select the table, which represents the form that is associated with the process definition.
9. Click **Save**. The process definition is created. In addition, the **Map Descriptive Field** button is enabled. If you click this button, the Map Descriptive Field dialog box is displayed.

   From this window, you can select the field (for example, the Organization Name field) that will be used as an identifier of the process definition when an instance

of the process is assigned to a resource object. This field and its value will then appear in the Reconciliation Manger form.

Note: If a process has a custom process form attached to it, the fields on that form will also appear within this window and be available for selection.

10. By clicking on the **Render Workflow** button, you can view your workflow definition in a graphical presentation. The Workflow Renderer is a powerful tool in helping you develop your process definition.

Note: For detailed information on how to use the Workflow Definition Renderer, refer to *Oracle Identity Manager Administrative and User Console Guide*.

Tabs on the Process Definition Form

Once you launch the Process Definition form, and create a process definition, the tabs of this form become functional.

The Process Definition form contains the following tabs:

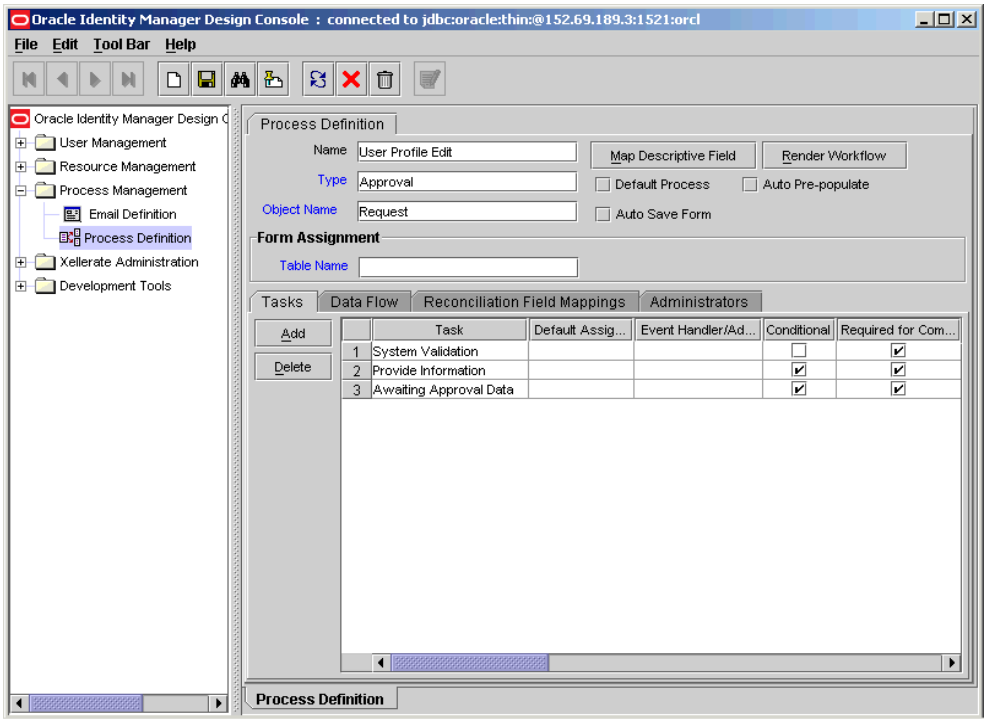
- "Tasks" on page 7-9
- "Data Flow" on page 7-11
- "Reconciliation Field Mappings" on page 7-13
- "Administrators" on page 7-16

Each of these tabs is covered in greater detail in the following sections.

Tasks

Figure 7–3 displays the Tasks tab of the Process Definition form.

Figure 7–3 The Tasks Tab of the Process Definition Form



This tab is used to:

- Create and modify the process tasks that comprise the current process definition
- Remove a process task from the process definition (when it is no longer valid)

In this example, the *Solaris 8* process definition is comprised of 15 process tasks.

> **Note:** To learn more about editing process tasks, refer to "Modify Process Tasks" on page 7-17.

Now that we have reviewed the Tasks tab, you will learn how to add, delete, export, and import process tasks.

Add a Process Task

To add a process task, perform the following steps:

1. Click **Add**. The Creating New Task dialog box is displayed.
2. In the **Task Name** field, enter the name of the process task.
3. From the Toolbar of the Creating New Task window, click **Save**. Then, click **Close**. The process task is added to the process definition.

Edit a Process Task

For instructions on how to edit and set process tasks, refer to "Modify Process Tasks" on page 7-17.

Delete a Process Task

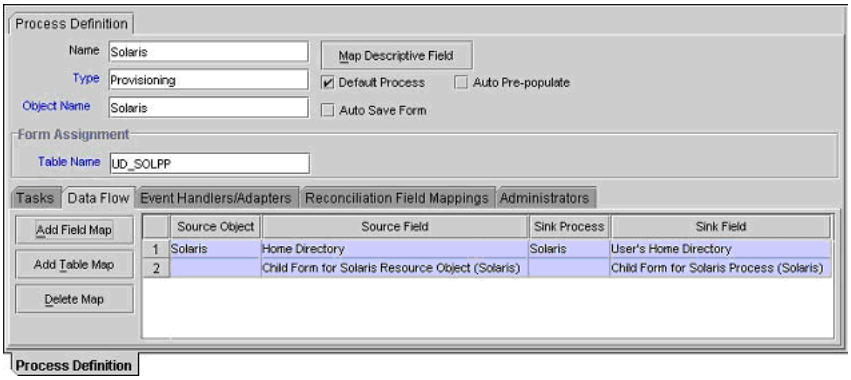
To delete a process task, perform the following steps:

1. Highlight the process task that you want to delete.
2. Click **Delete**. The process task is removed from the process definition.

Data Flow

Figure 7–4 displays the data flow tab of the Process Definition form.

Figure 7–4 Data Flow Tab of the Process Definition Form



This tab is used to define the data flow between:

- The fields of the parent resource form (which is attached to the resource object definition) and the fields of the parent process form (which is attached to the provisioning process definition).
- The fields of the parent resource form and the fields of the child process form (which belongs to the parent process form).
- The fields of the child resource form (which belongs to the parent resource form) and the fields of the child process form.

This tab is relevant only if the parent resource object has a custom resource form attached to it, and the parent process has a custom process form attached to it.

In addition, to map the flow of data between the fields of either a parent resource form and a child process form, or between the fields of a child resource form and a child process form, the custom resource form must have a child resource form assigned to it, and the custom process form must have a child process form assigned to it.

> **Note:** For more information on custom process or resource forms, or to learn more about assigning child forms to parent forms, refer to "The Form Designer Form" on page 9-2.

Once you have defined both a resource object form (for the parent resource object) and a process form (for the parent provisioning process) and have assigned child forms to both the parent resource form and the parent process form, you can establish any required mapping between the fields of these forms.

In the example above, two data flows have been defined. For the first data flow, the value of the *Home Directory* field of the *Solaris* parent resource form is mapped to the *User's Home Directory* field of the *Solaris* parent process form. For the second data flow, the values of the Solaris child resource form are mapped to the appropriate fields of the Solaris child process form.

Note: The values of the fields on the process form cannot be mapped back to the resource form fields. Also, the values of the fields on the child resource form cannot be mapped to those fields that belong to the parent process form.

Now that we have reviewed the **Data Flow** tab, you will learn how to map the following:

- A data field on a parent resource form to a data field on a parent process form
- A data field on a parent resource form to a data field on a child process form
- A data field on a child resource form to a data field on a child process form

Similarly, you will learn how to break the mapping between two data fields.

Map the Data Field of a Parent Resource Form to a Data Field of a Process Form

To map the data field of a Parent Resource form to a data field of a Process form, perform the following steps:

1. Click **Add Field Map**. The Define Data Flow dialog box is displayed.
2. From the **Data Source** combo box, select the desired data field of the parent resource form.
3. From the **Data Sink** combo box, highlight the target data field of the parent or child process form.
4. From the window's Toolbar, click **Save**. Then, click **Close**. The selected data field of the parent resource form is now mapped to the target data field of either the parent or child process form, depending on the selection you made in Step 3 of this procedure.

Map the Data Field of a Child Resource Form to a Data Field of a Child Process Form

To map the data field of a Child Resource form to a data field of a Child Process form, perform the following steps:

1. Click **Add Table Map**. The Add Data Flow Table Mapping dialog box is displayed.
2. From the **Resource Object Child Table** combo box, select the desired table names of the child resource form.
3. From the **Process Child Table** combo box, highlight the target table names of the child process form.
4. From the window's Toolbar, click **Save**. Then, click **Close**. The selected table names of the child resource form is now mapped to the target table names of the child process form.
5. Click **Add Field Map**. The Define Data Flow dialog box is displayed.
6. From the **Table Mapping** combo box, select the desired table name of the child resource form.
7. From the **Data Source** combo box, select the desired data field of the child process form.
8. From the **Data Sink** combo box, select the target data field of the child process form.

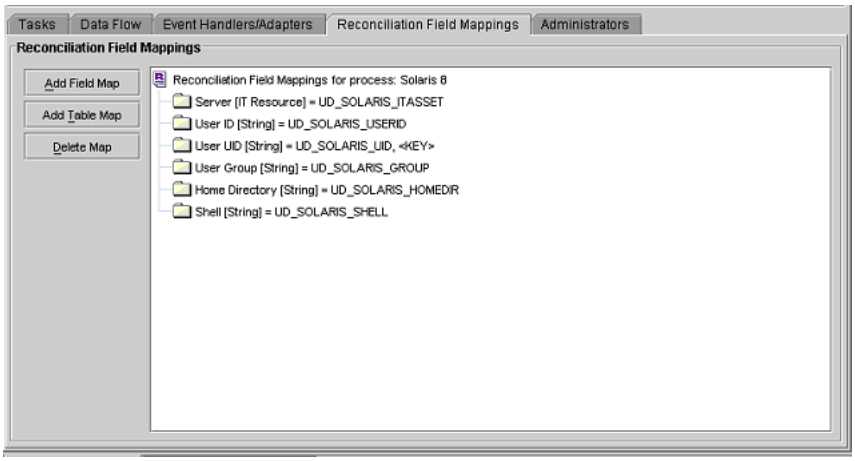
Break the Mapping Between the Data Fields of a Resource Object and a Process

1. Highlight the data fields, which contain a mapping you want to sever.
2. Click **Delete Map**. The selected data field of the resource object form is no longer mapped to the highlighted data field of the process form.

Reconciliation Field Mappings

Reconciliation Field Mappings tab, as shown in Figure 7–5, is used to define the relationship between the data elements in the target system/trusted source and the fields within Oracle Identity Manager with which they are to be linked.

Figure 7–5 The Reconciliation Field Mappings tab of the Process Definition Form



Only those fields that have been defined on the **Reconciliation Fields** tab of the associated resource will be available for mapping assignments. These mappings are used to determine which fields in Oracle Identity Manager are to be populated with the information provided (using reconciliation events) from the target system. In addition, for target resources (not trusted sources), this tab is also used to indicate which fields are key fields. Key fields are the fields for which the values on the process form and the reconciliation event must be the same for a match to be generated on the **Processes Matched Tree** tab of the Reconciliation Manager form. For each mapping, the following information is displayed:

- Name of the field (as defined on the **Reconciliation Fields** tab of the associated resource) on the target system/trusted source that is to be reconciled with data in Oracle Identity Manager.
- Data type associated with the field (as defined on the **Reconciliation Fields** tab of the associated resource). Possible values are Multi-Valued, String, Number, Date, IT resource.
- (**For trusted sources**) The name of the field on the users form (for user discovery) or the Oracle Identity Manager Organizations form (for organization discovery) to which the data in the trusted source field is to be mapped.

> **Note:** If you will be performing both user and organization discovery with a trusted source, organization discovery must be conducted first.

- (**For target resources**) The name of the field on the resource's custom (provisioning) process form to which the data in the target resources field is to be mapped.
- Indicator (**only for target resources**) designating whether the field is a key field within the reconciliation for this target resource. For provisioning processes to be matched to reconciliation event data, the value of the key fields in their process forms must be the same as those in the reconciliation event.

Map a Target Resource Field to Oracle Identity Manager

This procedure is used to map the fields on the target resource/trusted source (as defined on the **Reconciliation Fields** tab of the associated resource definition) to the applicable fields in Oracle Identity Manager. These mapping are used to determine what fields within Oracle Identity Manager are to be updated with the information in a reconciliation event when you click the **Create User** or **Create Organization** button, the **Link** button (on the **Matched Users** or **Matched Organizations** tab) or the **Establish Link** button (on the **Processes Matched Tree** tab) of the Reconciliation Manager form.

Once you have accessed the provisioning process definition for the associated resource and selected the **Reconciliation Field Mappings** tab, use one of the two procedures below.

Note: For user discovery on a trusted source, the resource on which you will define the fields to be mapped is User and the provisioning process on which you will define the field mappings is User. In addition, the Oracle Identity Manager fields (i.e., user attributes) to which you will map your trusted source fields will be derived from the Users form.

For organization discovery on a trusted source, the resource on which you will define the fields to be mapped is *Oracle Identity Manager Organization* and the provisioning process on which you will define the field mappings is *Oracle Identity Manager Organization*. In addition, the Oracle Identity Manager fields (i.e., organization attributes) to which you will map your trusted source fields will be derived from the Organizations form.

Map a Single Value Field

To map a single value field, perform the following steps:

1. Click **Add Field Map**. The Add Reconciliation Field Mappings dialog box is displayed.
2. Select the field on the target system that you wish to map from the menu in the Field Name field. Oracle Identity Manager will automatically supply the field type based on what was entered for this field on the associated **Resource Object** form.
3. For trusted sources:

   Select a value from the **User Attribute** menu and click **OK**. Skip to Step 4.

   For target resources:

   Double-click **Process Data Field**. Select the correct mapping from the **Lookup** dialog box and click **OK**.

4. If you are defining mapping for a trusted source, skip this step. Set the **Key Field for Reconciliation Matching** checkbox (for target resources only). If this checkbox is selected, Oracle Identity Manager will evaluate whether the value of this field on the provisioning process' form matches the value of that field within the reconciliation event (all matched processes appears on the **Processes Matched Tree** tab of the Reconciliation Manager form). If this checkbox is cleared, Oracle Identity Manager will not require the value of this field to match on the process form and reconciliation event for process matching.

   Note: In order for a field to be set as a key field, it must be set as required on the **Object Reconciliation** tab of the applicable resource.

5. Click **Save**. The mapping for the selected field(s) will be applied the next time a reconciliation event is received from the target resource or trusted source.

Map a Multi-Value Field (for target resources only)

To map a multi-value field, perform the following steps:

1. Click **Add Table Map**. The Add Reconciliation Table Mappings dialog box is displayed.
2. Select the multi-value field on the target system that you wish to map from the menu in the Field Name field. Oracle Identity Manager will automatically supply the field type based on what was entered for this field on the associated Resource Object form.
3. Select the child table you defined on the target resource's process form from the Table Name menu (only child tables appears).
4. Double-click **Process Data Field**. Select the correct mapping from the Lookup dialog box and click **OK**.
5. Save and close the Add Reconciliation Table Mappings dialog box.
6. Right-click the multi-value field you just mapped and select Define a property field map from the menu that appears.
7. Select the component (child) field you wish to map. Oracle Identity Manager will automatically supply the field type based on what was entered for this field on the associated Resource Object form.
8. Double-click the **Process Data Field** field. Select the correct mapping from the Lookup dialog box and click **OK**.
9. Set the **Key Field for Reconciliation Matching** checkbox. If this checkbox is selected, Oracle Identity Manager will evaluate whether the value of this field on the provisioning process' child form matches the value of that field within the reconciliation event (all matched processes appears on the **Processes Matched Tree** tab of the Reconciliation Manager form). If this checkbox is cleared, Oracle Identity Manager will not require the value of this field to match on the process form and reconciliation event for process matching. You should ensure that at least one component (child) field of each multi-value field is set as a key field. This will enhance the quality of the matches generated on the **Process Matched Tree** tab.

   Note: In order for a field to be set as a key field, it must be set as required on the **Object Reconciliation** tab of the applicable resource.

10. Repeat Steps 6-9 for each component (child) field defined on the multi-value field.
11. Click **Save**. The mapping for the selected field(s) will be applied the next time a reconciliation event is received from the target resource.

Delete a Mapping

This procedure is used to delete a mapping that has been established between a field on the target system/trusted source (as defined on the **Reconciliation Fields** tab of the associated resource definition) and a field in Oracle Identity Manager. Once you have accessed the provisioning process definition for the associated resource and selected the **Reconciliation Field Mappings** tab:

1. Select the field mapping you wish to delete.
2. Click **Delete Map**. The mapping for the selected field will be deleted.

Administrators

This tab is used to select the user groups that can view, modify, and delete the current process definition.

In addition, the **Write** and **Delete** check boxes are visual indicators of the privileges that a user group has with the process definition. When the **Write** check box is selected, the corresponding user group can read and modify the current process definition. If this check box is cleared, the user group cannot read or edit the process definition.

Similarly, when the **Delete** check box is selected, the associated user group can delete the current process definition. If this check box is cleared, the user group cannot delete the process definition.

For this example, the *SYSTEM ADMINISTRATORS* user group can view, modify, and delete the Solaris 8 process definition.

Now that we have reviewed the **Administrators** tab, you will learn how to assign a user group to a process definition, and remove a user group from a process definition.

Assign a User Group to a Process Definition

1. Click **Assign**. The Groups window is displayed.
2. Select the unassigned group, and assign it to the process definition.
3. Click **OK**. The user group appears in the **Administrators** tab.
4. If you want this user group to be able to view and/or modify the current process definition, double-click the corresponding Write check box. Otherwise, proceed to Step 5.
5. If you want this user group to be able to delete the current process definition, double-click the associated **Delete** check box. Otherwise, proceed to Step 6.
6. Click **Save**. The user group is assigned to the process definition.

Remove a User Group From a Process Definition

1. Highlight the user group that you want to remove.
2. Click **Delete**. The user group is removed from the process definition.

Modify Process Tasks

Once you create a process task for your process definition, you may need to modify it. To do so, double-click its row header. The Editing Task window appears, containing additional information about the process task.

The Editing Task window contains the following tabs:

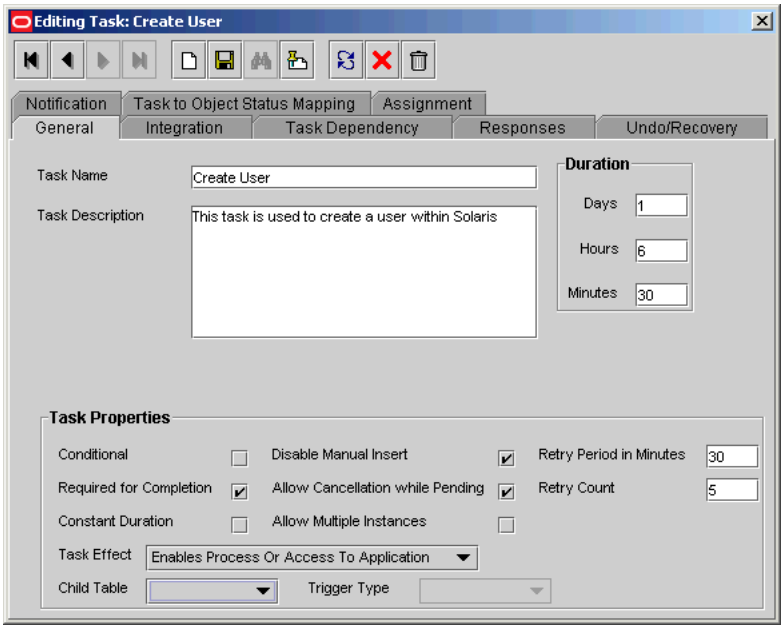
- "General" on page 7-17
- "Integration" on page 7-21
- "Task Dependency" on page 7-23
- "Responses" on page 7-24
- "Undo/Recovery" on page 7-25
- "Notification" on page 7-26
- "Task to Object Status Mapping" on page 7-28
- "Assignment" on page 7-29

Each of these tabs is covered in greater detail in the following sections.

General

Figure 7–6 displays the General tab of the Editing Task dialog box.

Figure 7–6 The General Tab of the Editing Task Dialog Box



This tab is used to set high-level information for the task you want to modify. For this example, the Create User task is used to create a user within the Solaris environment.

Now that we have reviewed top-level information pertaining to process tasks, you will learn about the data fields of the General tab. The following table describes the fields of this tab.

Field Name	Description
Task Name	The name of the process task.
Task Description	Explanatory information about the process task.
Duration	The expected completion time of the current process task (in days, hours, and minutes).
Conditional	This check box is used to determine whether a condition needs to be met for the current process task to be added to the process. If you select this check box, the process task cannot be added to the process unless a condition has been met. By clearing this check box, a condition does not have to be met for the process task to be added to the process.
Required for Completion	This check box is used to determine if the current process task needs to be completed for the process to be completed. If you select this check box, the process cannot be completed if the process task does not have a status of Completed. By clearing this check box, the status of the process task does not affect the completion status of the process.
Constant Duration	N/A
Task Effect	From this combo box, select the process action you want the task to be associated with (for example, disable, enable). A process is able to enable or disable a user's access to a resource. When the disable action is chosen, all tasks associated with the disable action will be inserted. **Note**: If you do not want the process task to be associated with a particular process action, select NONE from the combo box.
Disable Manual Insert	This check box is used to determine whether an user can manually add the current process task to the process. If you select this check box, the process task cannot be added to the process manually. By clearing this check box, an user can add the process task to the process.
Allow Cancellation while Pending	This check box is used to determine whether the process task can be cancelled if its status is Pending. If you select this check box, the process task can be cancelled if it has a Pending status. By clearing this check box, the process task cannot be cancelled if its status is Pending.
Allow Multiple Instances	This check box is used to determine whether the process task can be inserted into the current process more than once. If you select this check box, multiple instances of the process task can be added to the process. By clearing this check box, the process task can be added to the current process only once.
Retry Period in Minutes	If a process task is Rejected, the length of time before Oracle Identity Manager will insert a new instance of that task with a status of Pending. Figure 7–6 on page 7-17, *30* appears in the Retry Period in Minutes text box. If the Create User process task is rejected, in *30* minutes, then Oracle Identity Manager will add a new instance of this task, and assign it a status of Pending.

Field Name	Description
Retry Count	How many times Oracle Identity Manager will retry a rejected task. Figure 7–6 on page 7-17, 5 is displayed in the Retry Count text box. If the Create User process task is rejected, Oracle Identity Manager will add a new instance of this task, and assign it a status of Pending. However, once this process task is rejected for the fifth time, Oracle Identity Manager will no longer insert a new instance of the Create User process task.
Child Table/ Trigger Type	These combo boxes are used to specify the action that Oracle Identity Manager needs to perform within the child table of the custom form that is associated with the current process (as indicated by the **Table Name** field of the **Process Definition** form). From the **Child Table** combo box, select the child table of the custom form, upon which Oracle Identity Manager will perform an action. Then, from the Trigger Type combo box, specify the action that Oracle Identity Manager will perform within this child table. These actions include: ▪ **Insert**. Adding a new value to the designated column of the child table ▪ **Update**. Modifying an existing value from the corresponding column of the child table ▪ **Delete**. Removing a value from the designated column of the child table **Note**: If the custom process form does not have any child tables associated with it, the **Child Table** combo box will be empty. In addition, the Trigger Type combo box will be disabled.

Now that we have reviewed process tasks and the data fields of the General tab, you are ready to modify high-level information pertaining to a process task.

Modify a Process Task's General Information

1. Double-click the row header of the task you want to modify. The Editing Task dialog box is displayed.
2. Click the **General** tab.
3. In the **Description** field, enter explanatory information about the process task.
4. *Optional*. In the **Duration** area, enter the expected completion time of the process task (in days, hours, and minutes).
5. If you want a condition to be met for the process task to be added to the Process Instance, select the **Conditional** check box. Otherwise, proceed to Step 6.

   Important: If you select the **Conditional** check box, make sure you specify the condition that needs to be met for the task to be added to the process.

6. When you want the completion status of the process to be dependent on the completion status of the process task, select the **Required for Completion** check box. By doing so, the process cannot be completed if the process task does not have a status of Completed.

   If you do not want the status of the process task to affect the completion status of the process, proceed to Step 7.

7. When you want to prevent an user from manually adding the process task into a currently running instance of the process, select the **Disable Manual Insert** check box. Otherwise, proceed to Step 8.
8. If you want an user to be able to cancel the process task if its status is Pending, select the **Allow Cancellation while Pending** check box. Otherwise, proceed to Step 9.
9. When you want to allow this task to be inserted multiple times within a single process instance, select the **Allow Multiple Instances** check box. Otherwise, proceed to Step 10.
10. Click the **Task Effect** combo box. From the custom menu that appears, select one of the following menu items:
    - **Enable Process or Access to Application**. If a resource is reactivated using the enable function, all tasks with this effect will be inserted will be inserted into the process. If you select this option, be sure the **Allow Multiple Instances** check box is selected.
    - **Disable Process or Access to Application**. If a resource is de-activated using the disable function, all tasks with this effect will be inserted into the process. If you select this option, be sure the **Allow Multiple Instances** check box is selected.
    - **No Effect**. This is the default process action associated with all tasks. If this option is selected, the task will only be inserted during normal provisioning (unless it is conditional).
11. *Optional*. If the process task is *Rejected*, you may want Oracle Identity Manager to insert a new instance of this process task (with a status of *Pending*). In order for this to occur, a value must be entered in the **Retry Period in Minutes** field. This designates the length of time (in minutes) that Oracle Identity Manager will wait before adding this process task instance.

    In the **Retry Count** text box, enter the number of time Oracle Identity Manager will retry a rejected task. For example, suppose 3 appear in the **Retry Count** text box for the process task. If it is rejected, Oracle Identity Manager will add a new instance of this task, and assign it a status of Pending. However, once this process task is rejected for the fourth time, Oracle Identity Manager will no longer insert a new instance of the process task.

    Note: If either the Retry Period or Retry Count is selected, you must specify parameters for the other option since they are both related.

12. From the **Child Table** combo box, select the child table of the custom form, upon which Oracle Identity Manager will perform an action.

    Then, from the **Trigger Type** combo box, specify the action that Oracle Identity Manager will perform within this child table. These actions include:
    - **Insert**. Adding a new value to the designated column of the child table.
    - **Update**. Modifying an existing value from the corresponding column of the child table.
    - **Delete**. Removing a value from the designated column of the child table.

Note: If the custom process form does not have any child tables associated with it, the **Child Table** combo box will be empty. In addition, the **Trigger Type** combo box will be disabled.

13. Click **Save**. The modifications to the process task's top-level information reflects the changes you made in the **General** tab.

Integration

Through the **Integration** tab, you can:

- Automate a process task by attaching an event handler or task adapter to it.
- Map the variables of the task adapter, so Oracle Identity Manager can pass the appropriate information when the adapter is triggered. This occurs when the process task's status is Pending.
- Break the link between the adapter/event handler and the process task, once the adapter or event handler is no longer applicable with the process task.

In this example, the adpSOLARISCREATEUSER adapter is attached to the Create User process task. This adapter has nine adapter variables, all of which are mapped correctly (as indicated by the Y, which precedes each variable name).

Tip: event handlers are preceded with tc (Thor class), such as *tcCheckAppInstalled*. These are event handlers that Oracle provides. Customer created event handlers cannot have tc preceded in their name. Adapters are preceded with adp (for example, *adpSOLARISCREATEUSER*).

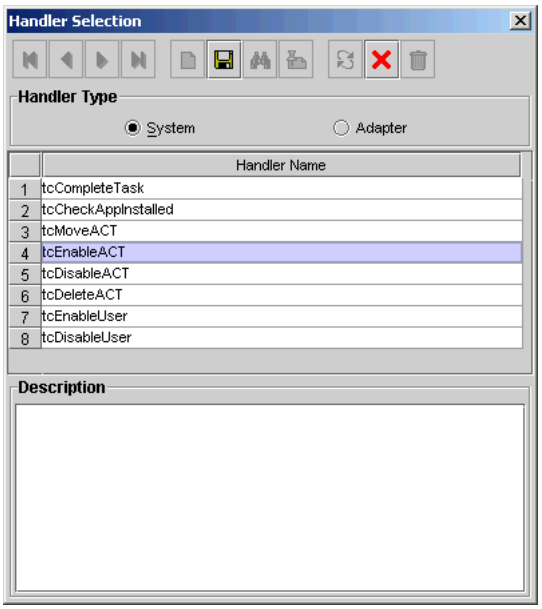
Note: For more information on adapters and event handlers, refer to "The Adapter Factory Form" on page 9-2 and "The Event Handler Manager Form" on page 10-1.

Now that we have reviewed the Integration tab, you will learn how to assign an adapter or an event handler to a process task, map the variables of an adapter, and remove an adapter or event handler from a process task.

Assign an Adapter or Event Handler to a Process Task

1. Double-click the row header of the process task to which you want to assign an event handler or adapter. The Editing Task window appears.
2. Click the **Integration** tab.
3. Click **Add**. The **Handler Selection** dialog box is displayed, as shown in Figure 7–7.
4. To assign an event handler to the process task, select the **System** radio button. To add an adapter to the process task, select the **Adapter** radio button. A list of event handlers or adapters, which you can assign to the process task, appears in the **Handler Name** region.

Figure 7–7 The Handler Selection Dialog Box



5. Select the event handler or adapter that you want to assign to the process task.
6. From the Handler Selection window's Toolbar, click **Save**. A confirmation dialog box appears.
7. Click **OK**. The event handler or adapter is assigned to the process task.

Important: If you have assigned an adapter to the process task, the adapter will not work until you map the adapter variables correctly. To learn how to map adapter variables, refer to "Map Adapter Variables" on page 7-22.

Map Adapter Variables

1. Select the adapter variable that you want to map.
2. Click **Map**. The Data Mapping for Variable window appears.
3. Complete the Map To, Qualifier, IT Asset Type, IT Asset Property, Literal Value, and Old Value fields.

Note: For more information on which items to select, refer to the Oracle Identity Manager Tools Reference Guide.

Caution: In order to trigger a task associated with a change to a parent form field, the name of the task must be <field> Updated, where <field> is the name of the parent form field. If the task is not named according to this convention, then it will not be triggered during field update.

---

4. From the Data Mapping for Variable window's Toolbar, click Save.
5. Then, click **Close**. The mapping status for the adapter variable changes from N to Y. This indicates that the adapter variable has been mapped.

Remove an Adapter or Event Handler From a Process Task

1. Click **Remove**. A confirmation dialog box is displayed.
2. Click **OK**. The event handler or adapter is removed from the process task.

Task Dependency

The **Task Dependency** tab is used to determine the logical flow of process tasks within a process. Through this tab, you can:

- Assign **preceding** tasks to a process task. These tasks must have a status of Completed before Oracle Identity Manager or an user can trigger the current process task.
- Assign **dependent** tasks to a process task. Oracle Identity Manager or an user can trigger these tasks only after the current process task has a status of Completed.
- Break the link between a preceding task and the current task (when the preceding task's completion status no longer has any bearing on the current task being triggered).
- Break the link between the current task and a dependent task (when the current task's completion status no longer has any bearing on triggering the dependent tasks).

For this example, the *Create User* process task does not have any preceding tasks. As a result, Oracle Identity Manager will trigger this task whenever task is added inserted into the process (for example, when the associated resource is requested).

In addition, the *Create User* process task has seven dependent tasks. Once this task achieves a status of Completed, each of these process tasks will be assigned a status of *Pending* (before that, each dependent task will have a status of Waiting). As a result, Oracle Identity Manager will then be able to trigger them.

Now that we have reviewed task dependencies, you will learn how to assign preceding and dependent tasks to a process task. In addition, you will learn how to remove preceding and dependent tasks from a process task.

Assign a Preceding Task to a Process Task

1. Double-click the row header of the process task to which you want to assign a preceding task. The **Editing Task** window appears.
2. Click the **Task Dependency** tab.
3. From the Preceding Tasks region, click **Assign**. The **Assignment** window appears.
4. From this window, select the preceding task, and assign it to the process task.
5. Click **OK**. The preceding task is assigned to the process task.

Remove a Preceding Task from a Process Task

1. 1.Highlight the preceding task that you want to delete.
2. 2.From the Preceding Tasks region, click Delete. The preceding task is removed from the process task.

Assign a Dependent Task to a Process Task

1. Double-click the row header of the process task to which you want to assign a dependent task. The Editing Task window appears.
2. Click the **Task Dependency** tab.

3. From the **Dependent Tasks** region, click **Assign**. The Assignment window appears.
4. From this window, select the dependent task, and assign it to the process task.
5. Click **OK**. The dependent task is assigned to the process task.

Remove a Dependent Task from a Process Task

1. Highlight the dependent task that you want to delete.
2. From the **Dependent Tasks** region, click **Delete**. The dependent task is removed from the process task.

Responses

The Responses tab is used to:

- Define the response codes that can be received in conjunction with the execution of a particular process tasks. The responses codes can be used to represent specific conditions on the target system.
- Define the conditional tasks that will be launched, if a particular response code is received in conjunction with the execution of this process task. These tasks are called generated tasks.
- Remove a response from a process task, when it is no longer valid.
- Remove a generated task from a process task, when it is no longer valid.

For this example, when the *Create User* process task is *Completed*, the *SUCCESS* response is activated. As a result, a dialog box appears, displaying the "The user was created successfully." message. In addition, Oracle Identity Manager will trigger the *Enable User* process task.

Now that we have reviewed responses and generated tasks, you will learn how to assign a response and a generated task to the current process task. In addition, you will learn how to remove a response and a generated task from the current process task.

Note: By default, the *UNKNOWN* response is defined for each process task that is rejected. This way, even when the System Administrator does not add any responses to a process task, if this task is rejected, the user will be notified, using an error message in a dialog box.

Add a Response to a Process Task

1. Double-click the row header of the process task to which you want to add a response. The Editing Task window appears.
2. Click the **Responses** tab.
3. Within the **Responses** region, click **Add**. A blank row appears within the Responses region.
4. Add information into the **Response** field. This field contains the response code value. This field is case-sensitive.
5. Add information into the **Description** field. This field contains explanatory information about the response. If the process task triggers the response, this information appears in the task information dialog box.

6. Double-click the **Status** lookup field. From the Lookup window that appears, select a task status level. If the response code is received, it will cause the task to be set to this status.
7. Click **Save**. The response you added would now reflect the settings you have entered.

Remove a Response From a Process Task

1. Highlight the response that you want to delete.
2. From the **Responses** region, click **Delete**. The response is removed from the process task.

Assign a Generated Task to a Process Task

1. Double-click the row header of the process task to which you want to assign a generated task. The Editing Task window appears.
2. Click the **Responses** tab.
3. Select the response code for which you wish to assign generated tasks (i.e., the tasks to be generated).
4. From the **Tasks to Generate** region, click **Assign**. The Assignment window appears.
5. From this window, select the generated task and assign it to the process task response.
6. Click **OK**. The generated task is assigned to the process task.

Remove a Generated Task From a Process Task

1. Select the desired response code.
2. Highlight the generated task that you want to delete.
3. From the Tasks to Generate region, click Delete. The generated task is removed from the process task.

Undo/Recovery

The Undo/Recovery tab is used to:

- Define process tasks that will be triggered when the current process task is Cancelled. These process tasks are known as undo tasks.
- Remove an undo task from a process task, when it is no longer valid.
- Define process tasks that will be triggered when the current process task is Rejected. These tasks are called recovery tasks.
- Remove a recovery task from a process task, when it is no longer valid.

For this example, if the *Create User* process task is *Cancelled*, the *Delete User* undo task will be triggered. Similarly, if the *Create User* task is *Rejected*, Oracle Identity Manager will trigger the *Enable User* recovery task.

Note: As stated previously, when the current process task is Rejected, Oracle Identity Manager will trigger any recovery tasks that have been assigned to the process task. By selecting the Complete on Recovery check box, Oracle Identity Manager will change the status of the current process task from Rejected to Unsuccessfully Completed upon completion of all recovery tasks that are generated. This way, Oracle Identity Manager can trigger other, dependent process tasks.

Now that we have reviewed about undo and recovery tasks, you will learn how to assign an undo and recovery task to the current process task. In addition, you will learn how to remove an undo and recovery task from the current process task.

Assign an Undo Task to a Process Task

1. Double-click the row header of the process task to which you want to assign an undo task. The Editing Task window appears.
2. Click the **Undo/Recovery** tab.
3. Within the **Undo Tasks** region, click **Assign**. The Assignment window appears.
4. From this window, select the undo task, and assign it to the process task.
5. Click **OK**. The undo task is assigned to the process task.

Remove an Undo Task From a Process Task

1. Highlight the undo task that you want to delete.
2. From the **Undo Tasks** region, click **Delete**. The undo task is removed from the process task.

Assign a Recovery Task to a Process Task

1. Double-click the row header of the process task to which you want to assign a recovery task. The Editing Task window appears.
2. Click the **Undo/Recovery** tab.
3. From the **Recovery Tasks** region, click **Assign**. The Assignment window appears.
4. From this window, select the recovery task, and assign it to the process task.
5. Click **OK**. The recovery task is assigned to the process task.
6. *Optional*. If you want the status of the current process task to change from Rejected to Unsuccessfully Completed upon completion of all recovery tasks that are generated (so Oracle Identity Manager can trigger other, dependent process tasks) select the Complete on Recovery check box. Otherwise, leave this check box empty.

Remove a Recovery Task From a Process Task

1. Highlight the recovery task that you want to delete.
2. From the **Recovery Tasks** region, click **Delete**. The recovery task is removed from the process task.

Notification

This tab is used to designate the e-mail notification to be generated when the current process task achieves a particular status. For each status a task can achieve, a separate

e-mail notification can be generated. If an e-mail notification is no longer valid, you can remove it from the **Notification** tab.

For this example, when the Create User process task achieves a status of Completed, Oracle Identity Manager will send the Process Task Completed e-mail notification to the user who will be provisioned with the resource once the task is completed. In addition, if the Create User process task is rejected, the Process Task Rejected e-mail notification will be sent to this user and the user's manager.

Note: Oracle Identity Manager can only send an e-mail notification to a user if you have first created a template for the e-mail message, using the E-mail Definition form.

For more information on creating e-mail notifications, refer to "The Email Definition Form" on page 7-1.

Now that we have reviewed about e-mail notifications, you will learn how to assign e-mail notifications to a process task, and remove e-mail notifications from a process task.

Assign an E-Mail Notification to a Process Task

1. Double-click the row header of the process task to which you want to assign an e-mail notification. The Editing Task dialog box is displayed.
2. Click the **Notification** tab.
3. Click **Assign**. The Assignment dialog box is displayed.
4. From this window, select the e-mail template definition to use, and assign it to the process task.
5. Click **OK**. The name of the e-mail notification appears in the Notification tab.
6. Double-click the **Status** lookup field. From the Lookup window that appears, select a completion status level. When the process task achieves this status level, Oracle Identity Manager will send the associated e-mail notification.
7. Select the check boxes, which represent the users who will receive the e-mail notification. Currently, an e-mail notification can be sent to the following users:
   - **Assignee**. This user is responsible for completing the associated process task.
   - **Requester**. This user requested the process that contains the corresponding process task.
   - **User**. This user will be provisioned with the resource once the associated process task is Completed.
   - **User's Manager**. This user is the supervisor of the user, who will be provisioned with the resource once the corresponding process task is Completed.
8. Click **Save**. The e-mail notification is assigned to the process task.

Remove an E-Mail Notification From a Process Task

1. Highlight the e-mail notification that you want to delete.
2. Click **Delete**. The e-mail notification is removed from the process task.

Task to Object Status Mapping

A resource object contains data that is used to provision resources to users and applications. This data includes approval and provisioning processes.

In addition, a resource object is provided with pre-defined provisioning statuses, which represent the various statuses of the resource object throughout its lifecycle as it is being provisioned to the target user or organization. By accessing the **Currently Provisioned** tab of the **Resource Objects** form, you can see the provisioning status of that resource object at any time. These values are also displayed in the **Object Process Console** tab on the **Users** and **Organizations** forms.

Note: Provisioning statuses are defined in the **Status Definition** tab of the **Resource Objects** form.

The provisioning status of a resource object is determined by the status of its associated approval and provisioning processes, as well as the tasks that comprise these processes. For this reason, you must provide a link between the status of a process task and the provisioning status of the resource object to which it is assigned.

The **Task to Object Status Mapping** tab is used to create this link. Also, when this connection is no longer relevant, or you wish to associate a process task status with a different provisioning status for the resource object, you must sever the link that currently exists.

For this example, there are five mappings between process task statuses and provisioning statuses of a resource object. When the *Create User* process task achieves a status of *Completed*, the associated resource object will be assigned a provisioning status of *Provisioned*. However, if this task is cancelled, the provisioning status for the resource object will be *Revoked*. *None* indicates that the achievement of this status by the process task has no impact on the provisioning status of the resource object.

Now that we have reviewed the relationship between process task statuses and provisioning statuses, you will learn how to map a process task status to a provisioning status, and unmap a process task status from a provisioning status.

Map a Process Task Status to a Provisioning Status

1. Double-click the row header of the process task, which has a status that you want to map to the provisioning status of a resource object. The Editing Task window appears.
2. Click the **Task to Object Status Mapping** tab.
3. Highlight the desired process task status.
4. Double-click the **Object Status** lookup field. From the Lookup window that appears, select the provisioning status of the resource object to which you want to map the process task status.
5. Click **OK**. The provisioning status you selected appears within the Task to Object Status Mapping tab.
6. Click **Save**. The process task status is mapped to the provisioning status.

Unmap a Process Task Status From a Provisioning Status

1. Highlight the desired process task status.

2. Double-click the **Object Status** lookup field. From the Lookup window that appears, select None. None indicates that the achievement of this status by the process task has no impact on the provisioning status of the resource object.
3. Click **OK**. The provisioning status of None appears within the **Task to Object Status Mapping** tab.
4. Click **Save**. The process task status is no longer mapped to the provisioning status of the resource object.

Assignment

Assignment Tab of the Editing Task Window

This tab is used to specify assignment rules for the current process task. These rules will determine how the process task will be assigned.

> **Note:** For the most part, task assignment rules are associated with tasks of approval processes, since these tasks are usually completed manually. On the other hand, tasks belonging to provisioning processes are usually automated. As a result, they do not need task assignment rules.

For this example, when the *Create User* process task is inserted in the process, the *Solaris Process Tasks* - User rule will be evaluated (since it has a priority value of 1). If that rule's criteria are satisfied, the task will be assigned to the user named *RLAVA* (and the task will be marked to escalate in 600,000 milliseconds, or 10 minutes).

If the criteria of the *Solaris Process Tasks* - User rule are not satisfied, Oracle Identity Manager will evaluate the criteria of the Solaris Process Tasks - Group rule. If that rule's criteria are satisfied, the task will be assigned to the *SYSTEM ADMINISTRATORS* user group (and the task will be marked to escalate in 10 minutes).

> **Note:** Only rules with a classification type of **Task Assignment** can be assigned to a process task. For more information on specifying the classification type of a rule, refer to "The Rule Designer Form" on page 6-6. In addition, Oracle Identity Manager comes pre-defined with a Default rule. This rule always evaluates to true. As a result, it can be used as a safeguard mechanism to ensure that at least one pre-defined task assignment takes place if all the other rules fail.

Now that we have reviewed rules and their relationship to process tasks, you will learn about the data fields of the Assignment tab. The following table describes the fields of this tab.

Field Name	Description
Rule	The name of the Task Assignment rule to evaluate.

Field Name	Description
Target Type	The classification type of the user or user group that is responsible for completing the current process task. Currently, the process task can be assigned to: ■ **User**. An Oracle Identity Manager user. ■ **Group**. A user group. ■ **Group User with Highest Priority**. The member of the specified user group with the highest priority number. ■ **Group User with Least Load**. The member of the specified user group with the fewest process tasks assigned to him/her. ■ **Request Target User's Manager**. The supervisor of the user, who is being provisioned with the resource. ■ **Object Authorizer User with Highest Priority**. The member of the user group (designated as an Object Authorizer user group for the resource) with the highest priority number. ■ **Object Authorizer User with Least Load**. The member of the user group (designated as an Object Authorizer user group for the resource) with the fewest process tasks assigned to him/her. ■ **Object Administrator**. A user group that is defined as an administrator of the associated resource object. ■ **Object Administrator User with Least Load**. The member of the user group (designated as an Object Administrator user group) with the fewest process tasks assigned to him/her. **Note**: Object Authorizer and Object Administrator user groups are defined in the **Object Authorizers** and **Administrators** tabs, respectively, of the Resource Objects form.
Adapter	This is the name of the adapter. Double click this field to get a lookup form for all existing adapters.
Adapter Status	This is the status of the adapter.
Group	The user group to which the current process task is assigned.
User	The user to which the current process task is assigned.
Email Name;Send Email	By selecting an e-mail notification from the **Email Name** Lookup field, and selecting the Send Email check box, Oracle Identity Manager will send the e-mail notification to a user or user group once the current process task is assigned.
Escalation Time	The amount of time (in milliseconds) that the user or user group, which is associated with the rule that Oracle Identity Manager triggers, has to complete the process task. If this process task is not completed within the allotted time, Oracle Identity Manager will then re-assign it to another user or user group. The escalation rule adheres to the order defined by the target type parameter.
Priority	The priority number of the rule that is associated with the current process task. This number indicates the order in which Oracle Identity Manager will evaluate the rule.

Now that we have reviewed task assignment rules and the data fields of the Assignment tab, you are ready to add a task assignment rule to a process task. In addition, when the rule is no longer valid, you will learn how to remove it from the process task.

Add a Rule to a Process Task

1. Double-click the row header of the task to which you want to add a rule. The Editing Task window appears.
2. Click the **Assignment** tab.
3. Click **Add**. A blank row appears within the Assignment tab.
4. Double-click the **Rule** lookup field. From the Lookup window that appears, select the rule that you wish to add to the process task. Then, click **OK**.
5. Double-click the **Target Type** lookup field. From the Lookup window that appears, select the classification type of the user or user group (*User*, *Group*, *Group User with Highest Priority*, *Group User with Least Load*, *Request Target User's Manager*, *Object Authorizer User with Highest Priority*, *Object Authorizer User with Least Load*, *Object Administrator*, *Object Administrator User with Least Load*) that is responsible for completing the process task. Then, click **OK**.
6. Double-click the **Group** lookup field. From the Lookup window that appears, select the user group that is responsible for completing the process task. This setting is only necessary if you selected *Group*, *Group User with Highest Priority* or *Group User with Least Load* in the **Target Type** field. Then, click **OK**.

   OR

   Double-click the **User lookup** field. From the Lookup window that appears, select the user who is responsible for completing the process task. This setting is only necessary if you selected User in the **Target Type** field. Then, click **OK**.
7. Double-click the **Email Name** field. From the Lookup window that appears, select the e-mail notification that will be sent to the corresponding user or user group once the task is assigned. Click OK. Then, select the Send Email check box.

   If you do not want Oracle Identity Manager to send an email notification when the task is assigned, proceed to Step 8.
8. In the **Escalation Time** field, enter the time (in milliseconds) that the selected user or user group has to complete the process task.

   When you do not want to associate a time limit with the rule you are adding to the process task, leave the **Escalation Time** field empty, and proceed to Step 10.
9. In the **Priority** field, enter the priority number of the rule that you are adding to the process task.
10. Click **Save**. The rule is added to the process task.

Remove a Rule From a Process Task

1. Highlight the rule that you want to delete.
2. Click **Delete**. The rule is removed from the process task.

8

Oracle Identity Manager (Xellerate) Administration

This chapter describes the administration of Oracle Identity Manager (Xellerate). It contains the following topics:

Overview

The Oracle Identity Manager (Xellerate) Administration folder provides System Administrators with the tools necessary to manage Oracle Identity Manager administrative features. This folder contains the following forms:

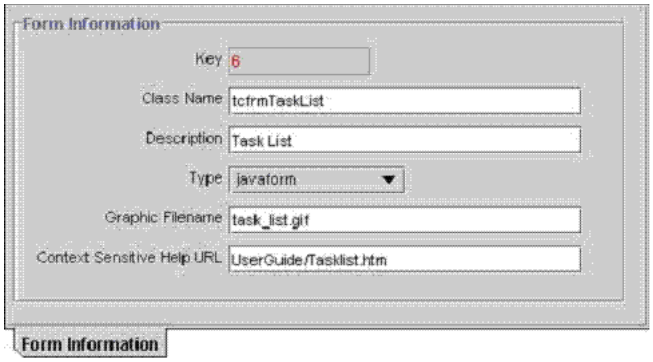
- **Form Information**: This form is used to specify the class name, form label, form type, menu item, graphic icon, and online Help topic to be associated with a given Oracle Identity Manager form. You can also use this form to modify the folders and folder items that appear within the Oracle Identity Manager Explorer.
- **Lookup Definition**: This form is used to create and manage lookup definitions. A lookup definition represents a lookup field and the values that are accessible from that lookup field.
- **User Defined Field Definition**: This form is used to create and manage user-defined fields. A user-defined field allows you to store additional information for Oracle Identity Manager forms.
- **System Configuration**: This form is used to define and set the value of properties that control the behavior of the Client and/or Server. In addition, you may specify the users and/or user groups to which the value of a property setting applies. Alternately, you may specify that the value of a property setting apply to all users.
- **Remote Manager**: This form displays information about the servers that Oracle Identity Manager uses to communicate with third-party programs. These servers are known as remote managers.

- **Task Scheduler**: This form is used to set up the schedules that will determine when scheduled tasks are to be run.

The Form Information Form

The Form Information form, as shown in Figure 8–1, is located in the Oracle Identity Manager Administration folder. It is used to specify the class name, label (that appears in the Oracle Identity Manager Explorer), form type, graphic icon, and help context to be associated with a given Oracle Identity Manager form. You can also use this form to modify the folders and folder items that appear within the Oracle Identity Manager Explorer.

Figure 8–1 The Form Information Form



The following table describes the data fields of this form.

Field Name	Description
Key	The system-generated ID for the form or folder.
Class Name	The name of the class associated with the form or folder. For the forms and folders that are pre-installed with Oracle Identity Manager, this will be a Thor class.
Description	The label that appears for this form or folder within the Oracle Identity Manager Explorer. For forms of *childform* type, this value must include the name of the parent form and adhere to the following naming convention: *<parent_form_name>.<child_form_name>*.
Type	The form type associated with the form or folder. For folders, this must be *folder*. Valid selections are *folder*, *export*, *processform*, *childform*, *javaform*, *import*, and *menuitem*.
Graphic Filename	The name of the graphic file that appears as an icon next to the form or folder in the Oracle Identity Manager Explorer.
Context Sensitive Help URL	The URL of the online Help topic that appears if the user presses **F1** when this form is active.

Add an Oracle Identity Manager Form/Folder

To add an Oracle Identity Manager form or folder, perform the following steps:

1. Access the Form Information form.

2. Enter the name of the class that will be used to render the form in the **Class Name** field.
3. Enter the label you wish to be displayed for the form or folder in the Oracle Identity Manager Explorer in the **Description** field.

> **Note:** For forms of *childform* type, this value must include the name of the parent form and adhere to the following naming convention: <*parent_form_name*>.<*child_form_name*>.

4. Select the desired item from the **Type** combo box.
   - For folders, select *folder*.
   - For forms related to export procedures, select *export*.
   - For forms related to a process, select *processform*.
   - For tabs that appear within other forms, or for forms that are nested within other forms, select *childform*.
   - For general forms, select *javaform*.
   - For forms related to import procedures, select *import*.
   - For menu items associated with the Oracle Identity Manager Administrative and User Console, select *menuitem*.

> **Note:** For more information on the Oracle Identity Manager Web Guide, refer to *Oracle Identity Manager Administrative and User Console Guide*.

5. Enter the name of the icon or graphic image file to be used within the Oracle Identity Manager Explorer for the form or folder in the **Graphic Filename** field.
6. Enter the URL of the online Help topic for the form in the **Context Sensitive Help URL** field. This will be the file displayed if the user presses **F1** when the form is active.
7. Click **Save**. The form is added. In addition, a system-generated ID for the form or folder appears within the **Key** field.

Modify the Oracle Identity Manager Explorer

The Oracle Identity Manager Explorer and layout of its folders and folder items can be modified based on different user group levels.

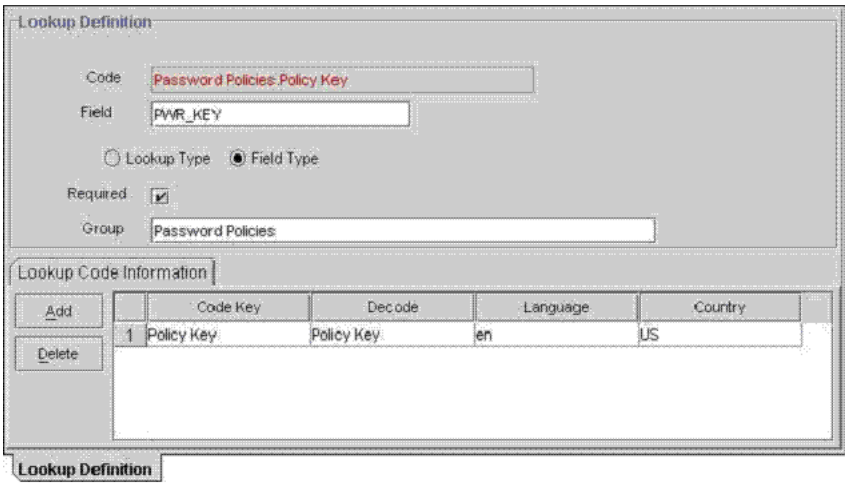
> **Note:** Click the plus sign (+) to expand a folder, and show folder items, or click the minus sign (-) to hide folder items.

The folders and folder items that a user can access are based on the user groups of which the user is a member. For example, suppose the *IT DEPARTMENT* user group can open the System Configuration form, and the *HR DEPARTMENT* user group is able to launch the Lookup Definition form. If a user belongs to both user groups, he or she can access the System Configuration form *and* the Lookup Definition form.

The Lookup Definition Form

The Lookup Definition form, as shown in Figure 8–2, is located within the Oracle Identity Manager Administration folder. It is used to create and manage lookup definitions.

Figure 8–2 The Lookup Definition Form



A lookup definition represents:

- The name and description of a text field;
- A lookup field and the values that are accessible from that lookup field (by double-clicking it); or;
- A combo box, and the commands that can be selected from that combo box.
- These items, which contain information pertaining to the text field, lookup field, or combo box, are known as lookup values.

Users can access lookup definitions from one of two locations:

- A form or tab that comes packaged with Oracle Identity Manager; or
- A user-created form or tab (built using the Form Designer form).

The following table describes the data fields of the Lookup Definition form.

Field Name	Description
Code	The name of the lookup definition.
Field	The name of the table column of the form or tab from which the text field, lookup field, or combo box field will be accessible.

Field Name	Description
Lookup Type/Field Type	These radio buttons are used to designate whether the lookup definition is to represent a text field, a lookup field, or a combo box. By selecting the **Field Type** radio button, the lookup definition will represent a text field. If you select the **Lookup Type** radio button, the lookup definition is to represent either a lookup field or a combo box, along with the values that are to be accessible from that lookup field or combo box. **Note**: For forms or tabs that come packaged with Oracle Identity Manager, the lookup definition has already been set as either a lookup field *or* a combo box. This cannot be changed. However, you can add or modify the values that are accessible from the lookup field or combo box. For forms or tabs that are user-defined, the user determines whether the lookup definition will represent a lookup field or a combo box through the **Additional Columns** tab of the Form Designer form. For more information on specifying the data type of a lookup definition, refer to "Additional Columns" on page 9-5.
Required	By selecting this check box, the lookup definition is designated as required. As a result, Oracle Identity Manager will not allow the contents of the corresponding form or tab to be saved to the database until the field or combo box, represented by the lookup definition, is supplied with data.
Group	The name of the Oracle Identity Manager or user-defined form on which the lookup definition is to appear.

Now that we have reviewed the data fields of this form, you will learn how to create a lookup definition.

Create a Lookup Definition

To create a lookup definition, perform the following steps:

1. Open the Lookup Definition form.
2. In the **Code** field, enter the name of the lookup definition.
3. In the **Field** field, enter the name of the table column of the Oracle Identity Manager or user-created form or tab, from which the text field, lookup field, or combo box field will be accessible.
4. If the lookup definition is to represent a lookup field or combo box, select the **Lookup Type** radio button.

   Note: For more information on specifying whether the lookup definition will represent a lookup field or a combo box, refer to the table that appears earlier in this section.

   If the lookup definition is to represent a text field, select the **Field Type** radio button.
5. *Optional*. If you want to set Oracle Identity Manager to save the contents of the corresponding form or tab to the database only when the field or combo box,

represented by the lookup definition, is supplied with data, select the **Required** check box. Otherwise, proceed to Step 6.

6. In the **Group** field, enter the name of the Oracle Identity Manager or user-defined form on which the lookup definition appears.

   Note: You must adhere to certain naming conventions for the text you enter into the **Code**, **Field**, and **Group** text boxes.

   For more information on these naming conventions, refer to Section , "The Lookup Definition Form" on page 8-4.

7. Click **Save**. The lookup definition is created. The associated text field, lookup field, or combo box will now appear in the Oracle Identity Manager or user-defined form or tab you specified.

The Lookup Code Information Tab

The Lookup Code Information tab is located in the lower half of the Lookup Definition form. It is used to create and manage detailed information related to the selected lookup definition. This information, which includes the names, descriptions, language codes, and country codes of a value pertaining to the lookup definition, is known as a **lookup value**.

The following procedures show how to create, modify, and delete a lookup value.

Caution: For internationalization purposes, a lookup value must be supplied with both a language and country code.

When creating a new lookup definition, ensure to save it before adding lookup values to it.

Create or Modify a Lookup Value

To create or modify a lookup value, perform the following steps:

1. Open the Lookup Definition form.
2. Access a lookup definition.
3. If you are creating a lookup value, click **Add**. A blank row appears within the **Lookup Code Information** tab.

   If you are modifying a lookup value, highlight the lookup value that you want to edit.
4. Add or edit the information in the **Code Key** field. This field contains the name of the lookup value.

   In addition, if the **Lookup Type** radio button is selected, this field also represents what appears within the lookup field or combo box once the user makes a selection.
5. Add or edit the information in the **Decode** field. This field contains a description of the lookup value.

   Also, if the **Lookup Type** radio button is selected, this field also represents:

   - The items that appears within a lookup window (once the user double-clicks the corresponding lookup field); or

- The commands that are to be displayed within the associated combo box.

6. Add or edit the information in the **Language** field. This field contains a two-character language code for the lookup value.
7. Add or edit the information in the **Country** field. This field contains the lookup value's two-character country code.
8. Click **Save**. The lookup value you created or modified will now reflect the settings you have entered.

Delete a Lookup Value

To delete a lookup value, perform the following steps:

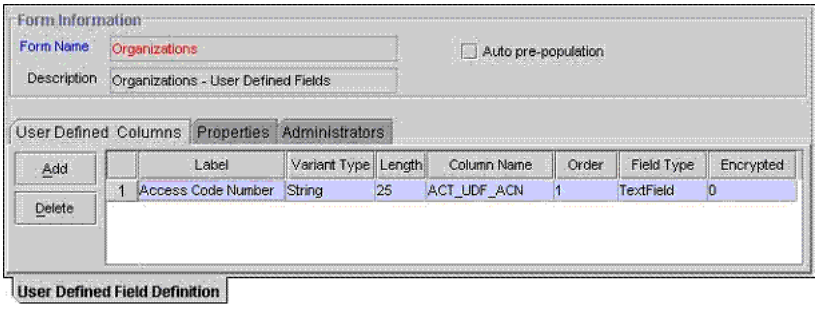
1. Open the Lookup Definition form.
2. Access a lookup definition.
3. Highlight the lookup value that you want to remove.
4. Click **Delete**. The selected lookup value is deleted.

The User Defined Field Definition Form

Sometimes, other than the fields that Oracle Identity Manager provides by default, you may need to store additional information. When this occurs, you can create the fields that will contain this information, and add them to various Oracle Identity Manager forms. These fields, which you create, are known as **user-defined fields**.

The User Defined Field Definition form, as shown in Figure 8–3, is located in the Oracle Identity Manager Administration folder. It is used to create and manage user-defined fields for the **Organizations**, **Users**, **Requests**, **Resource Objects**, **User Groups**, and **Form Designer** forms.

Figure 8–3 The User Defined Field Definition Form



Note: The user-defined field appears on the **User Defined Fields** tab of the form that appears in the **Form Name** data field. For this example, the *Access Code Number* user-defined field will be added to the **User Defined Fields** tab of the Organizations form.

Now that we have reviewed user-defined fields, you will learn about the data fields of the User Defined Field Definition form. The following table describes the fields of this form.

Field Name	Description
Form Name	The name of the form that the user-defined fields, which are displayed within the **User Defined Columns** tab, appears. **Important**: Since the user-defined fields for a user pertain to the user's profile information, they are displayed within the **User Profile** tab of the **Users** form.
Description	Additional information about the user-defined field definition.
Auto Pre-Population	This check box designates whether the user-defined fields for a form, which have pre-populated adapters attached to them, will be populated by Oracle Identity Manager or a user. If the **Auto Pre-Population** check box is selected, the user-defined fields that have pre-populate adapters attached to them will be populated by Oracle Identity Manager. When this check box is cleared, these fields must be populated by a user (by clicking the **Pre-Populate** button on the Toolbar or by a user manually entering the data). **Important**: This setting does not control the triggering of the pre-populate adapter. It merely determines whether the contents resulting from the execution of the adapter appear within the associated user-defined field (s) because of Oracle Identity Manager or a user. For more information on pre-populate adapters, refer to *Oracle Identity Manager Tools Reference Guide*. **Note**: Setting this checkbox is relevant only if you have created a user-defined field, and a pre-populate adapter is associated with that field.

Now that we have reviewed the data fields of this form, you will learn how to select a target form for the user-defined fields you will be creating.

Select the Target Form for a User-Defined Field

To select the target form for a user-defined field, perform the following steps:

1. Open the User Defined Field Definition form.
2. Double-click the **Form Name** lookup field. From the Lookup window that appears, select the Oracle Identity Manager form (**Organizational Defaults**, **Policy History**, **Group Entitlements**, **Resource Objects**, or **Form Designer**) that will display the user-defined field you will be creating.
3. Click **Query**. The form to which you will be adding the user-defined field is selected.

Tabs on the User Defined Field Definition Form

Once you launch the User Defined Field Definition form, and select a target form for the user-defined fields you will be creating, the tabs of this form become functional.

The User Defined Field Definition form contains the following tabs:

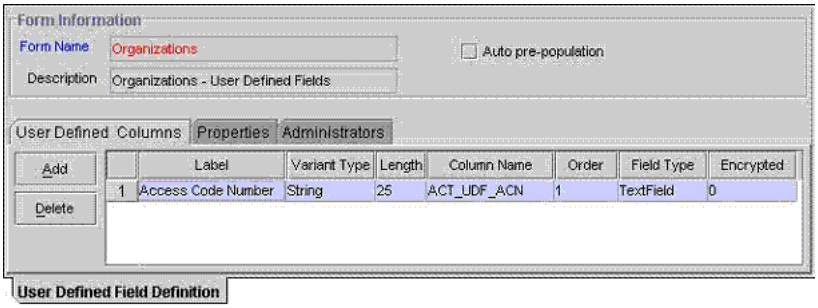
- "User Defined Columns" on page 8-9
- "Properties" on page 8-12
- "Administrators" on page 8-13

Each of these tabs is covered in greater detail in the sections that follow.

User Defined Columns

Figure 8–4 displays the User Defined columns tab of the User Defined Field Definition Form.

Figure 8–4 User Defined Columns Tab of the User Defined Field Definition Form



This tab is used to:

- Create a user-defined field.
- Set the variant type, length, and field type for the user-defined field.
- Specify the order in which the user-defined field appears on the **User Defined Fields** tab of the target form.
- Determine whether the information, which is associated with the user-defined field, is to be encrypted when it is exchanged between the Client and the Server.
- Remove a user-defined field, when it is no longer valid.

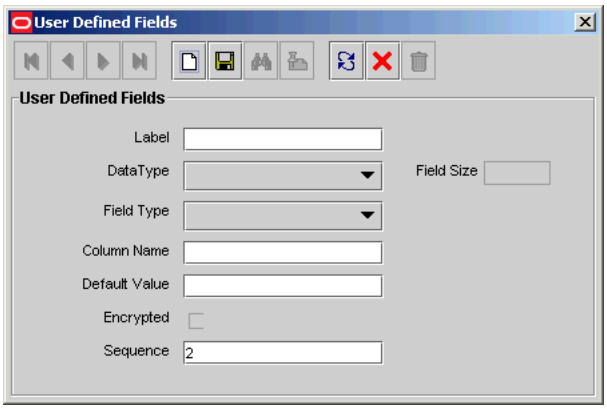
> **Caution:** the field's order number determines the order in which a user-defined field appears on a form. For this example, the *Access Code Number* user-defined field has an order number of *1*. Therefore, this field appears first on the **User Defined Fields** tab of the Organizations form.

Now that we have reviewed the **User Defined Columns** tab, you will learn how to add a user-defined field to an Oracle Identity Manager form, and remove a user-defined field from an Oracle Identity Manager form.

Add a User-Defined Field to an Oracle Identity Manager Form

1. Click **Add**. The User Defined Fields dialog box is displayed, as shown in Figure 8–5.

Figure 8–5 The User Defined Fields Dialog Box



Field Name	Description
Label	The label that is associated with the user-defined field. This label appears next to the user-defined field on the **User Defined Fields** tab of the target form. **Important**: The maximum length for a label is 30 characters.
Data Type	From this combo box, select one of the following data types for the user-defined field: ▪ **String**. A series of alphanumeric characters can be entered into this user-defined field. ▪ **Date**. When this user-defined field appears on a form, and a user double-clicks it, the Date and Time dialog box appears. ▪ **Integer**. A number without a decimal point (3) can be entered into this user-defined field. ▪ **Boolean**. When this user-defined field appears on a form, a user can enter two values into it: *True (1)* or *False (0)*. ▪ **Double**. A double-precision floating-point number (or a "double" number) can be entered into this user-defined field.
Field Size	In this text field, enter the maximum amount of numbers or characters that a user can enter into the user-defined field. **Note**: The **Field Size** text field is enabled only for the **String** data type.

Field Name	Description
Field Type	From this combo box, select one of the following field types for the user-defined field: ■ Text Field. The user-defined field appears on the **User Defined Fields** tab of the target form as a text field. ■ Lookup Field. The user-defined field appears on the **User Defined Fields** tab of the target form as a Lookup field. ■ Combo Box. The user-defined field appears on the **User Defined Fields** tab of the target form as a combo box. ■ Text Area. The user-defined field appears on the **User Defined Fields** tab of the target form as a text area. ■ Password Field. The user-defined field appears on the **User Defined Fields** tab of the target form as a text field. From this text field, a user can either query for an encrypted password (it appears as a series of asterisks [*]), or populate the field with an encrypted password, and save it to the database. ■ Check Box. The user-defined field appears on the **User Defined Fields** tab of the target form as a check box. ■ Date Field with Dialog. This data field appears on the **User Defined Fields** tab of the target form as a Lookup field. Once the user double-clicks this Lookup field, a Date & Time window appears. Oracle Identity Manager will then populate the data field with the date and time that the user selects from this window. **Note**: The field types that appear within this combo box reflect the data type that is displayed within the **Data Type** combo box.
Column Name	The name of the user-defined field that is recognized by the database. **Note**: This name is comprised of the <*TABLE NAME_UDF_*> prefix, followed by the label, which is associated with the user-defined field. So, if the **Table Name** field of the **Organizations** form is *ACT*, and the name for the data field is *ACN*, the name of the user-defined field, which the database recognizes, would be *ACT_UDF_ACN*. **Important**: The name that you enter into the **Column Name** field cannot contain any spaces.
Default Value	This value appears within the user-defined field once it appears on the target form.
Encrypted	This check box is used to determine whether the information, which appears within the associated user-defined field, is to be encrypted when it is exchanged between the Client and the Server. If this check box is selected, the information that is displayed within the user-defined field is encrypted when it is exchanged between the Server and the Client. When this check box is cleared, the information that appears in the user-defined field will not be encrypted as it is exchanged between the Client and the Server.

Field Name	Description
Sequence	This field represents the order in which the user-defined field appears on the designated form. For example, if a *2* appears in the **Sequence** field, it appears below the user-defined field with a sequence number of *1*.

2. Set the parameters for the user-defined field you are adding to a form, as shown in Figure 8–6.

Figure 8–6 The User Defined Fields Dialog Box - Filled

For this example, the *Access Code Number* user-defined field appears first on the **User Defined Fields** tab of the Organizations form. The data type of this field is *String*, and a user can enter up to *25* digits into it.

3. From this window, click **Save**.
4. Click **Close**. The user-defined field appears within the **User Defined Columns** tab. Once the target form is launched, this user-defined field appears within the **User Defined Fields** tab of that form.

Caution: Since the user-defined fields for a user pertain to the user's profile information, they are displayed within the **User Profile** tab of the **Users** form.

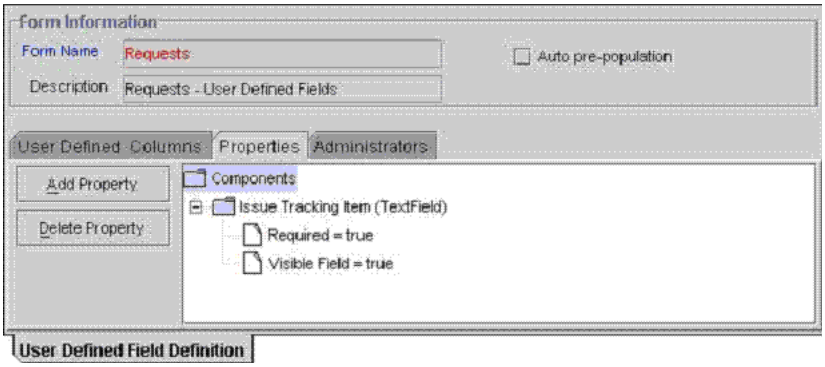
Remove a User-Defined Field from an Oracle Identity Manager Form

1. Highlight the desired user-defined field.
2. Click **Delete**. The user-defined field is removed.

Properties

Figure 8–7 displays the Properties tab of the User Defined Field Definition form.

Figure 8–7 The Properties Tab of the User Defined Field Definition Form



This tab is used to assign properties and property values to the data fields, which appear on the **User Defined Fields** tabs of various Oracle Identity Manager forms.

For this example, the **User Defined Fields** tab of the *Requests form* displays one data field: *Issue Tracking Item*. This data field contains the following properties:

- **Required**, which determines whether the data field needs to be populated for the *Requests* form to be saved. The default property value for the **Required** property is *false*.
- **Visible Field**, which establishes whether the data field appears on the *Requests* form. The default property value for the **Visible Field** property is *true*.

Since the property values for the **Required** and **Visible Field** properties are *true* for this data field, once the *Requests* form is launched, the *Issue Tracking Item* data field appears within the **User Defined Fields** tab. In addition, this field needs to be populated for the form to be saved.

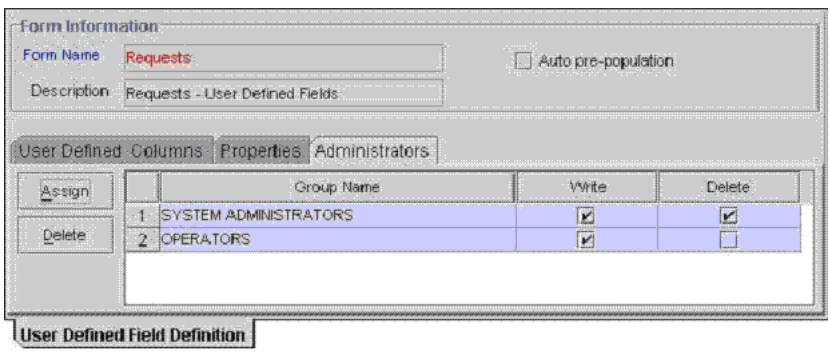
The following section describes how to add and remove a property and property value to a data field.

Note: To learn how to add a property and property value to a data field, or remove a property and property value from a data field, refer to "The Form Designer Form" on page 9-2.

Administrators

Figure 8–8 displays the Administrators tab of the User Defined Field Definition form.

Figure 8–8 Administrators Tab of the User Defined Field Definition Form



This tab is used to specify the user groups that have administrative privileges over the current record of the User Defined Field Definition form. In addition, the **Write** and **Delete** check boxes on this form are used to designate whether these administrative groups can modify and/or delete information pertaining to the current user-defined field (UDF) definition.

Now that we have reviewed the **Administrators** tab, you will learn how to assign administrative privileges to a user group for a UDF definition, and remove administrative privileges from a user group for a UDF definition.

Assign Administrative Privileges to a User Group for a UDF Definition

1. Click **Assign**. The Assignment dialog box is displayed.
2. Select the user group, and assign it to the UDF definition.
3. Click **OK**. The user group appears in the **Administrators** tab.
4. If you want this user group to be able to view and/or modify information pertaining to the current definition, double-click the corresponding **Write** check box. Otherwise, proceed to Step 5.
5. If you want this user group to be able to delete information contained within the current definition, double-click the associated **Delete** check box. Otherwise, proceed to Step 6.
6. Click **Save**. The user group is assigned to the UDF definition. The members of this user group can view, modify, and/or delete information contained within this definition.

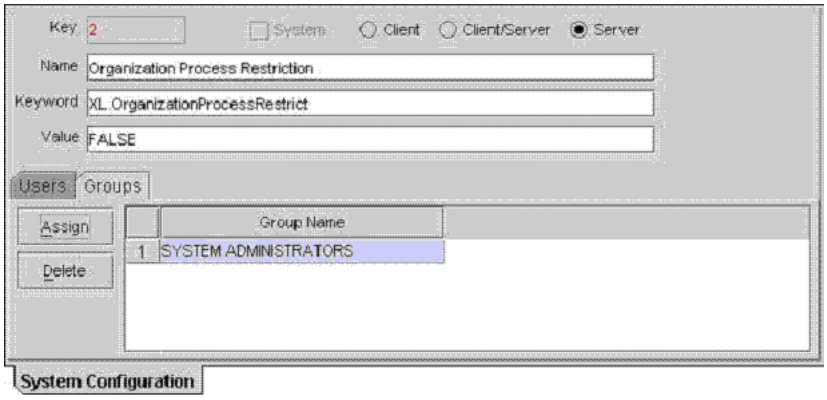
Remove Administrative Privileges From a User Group for a UDF Definition

1. Highlight the user group that you want to remove.
2. Click **Delete**. The user group is removed from the UDF definition. Its members no longer have administrative privileges for the definition.

The System Configuration Form

The System Configuration form, as shown in Figure 8–9, is located in the Oracle Identity Manager Administration folder. It is used to define and set the value of properties that control the behavior of the Oracle Identity Manager Client and/or Server. In addition, you may specify the users and/or user groups to which the value of a property setting applies. Alternately, you may specify that the value of a property setting apply to all users.

Figure 8–9 The System Configuration Form



The following table describes the data fields of this form:

Field Name	Description
Key	The system-generated ID for one instance of the property definition. There may be more than one instance of a definition (for example, one for System Administrators, another for all users).
System	This check box is used to designate whether this instance of the property definition applies to all users in Oracle Identity Manager (i.e., it is a system-wide instance) or only to select users and user groups. To apply this setting to all users, select this check box (the **Users** and **Groups** tabs will be disabled). To specify that an instance of the property apply to certain users and groups, clear this check box. **Note**: The **System** check box will be disabled if the **Server** radio button (described below) is selected.
Client **Client/Server** **Server** [Radio buttons]	These three radio buttons are used to designate whether this instance of the property definition applies to the Client, the Server, or both. If the **Client** radio button is selected, the property value only applies to the Client. If the **Client/Server** radio button is selected, the property value applies to both the Client and Server. If the **Server** radio button is selected, the property value only applies to the Server. Selecting this option will disable the **System** checkbox (since system-wide settings do not apply to the Server).
Name	The name of the property. This should be an intuitive description of what the property controls. It does not need to be unique.

Field Name	Description
Keyword	The property's unique ID. This must be identical for each instance of this property. For example, if you wish to set the *Record Read Limit* property (the maximum number of records a user's query may retrieve) differently for two separate users, you would need to create two instances of this property definition. **Note**: For more information on the various properties you can set for the Client and/or the Server, refer to the "System Properties" on page A-17.
Value	The value to which this instance of the property definition has been set. This will be the value applied to those users/groups assigned to this instance of the property (unless the **System** checkbox is selected, denoting that the instance applies to all users).

Now that we have reviewed the basic characteristics of a system property, you are ready to define instances of property definitions, and assign users or groups to these instances. Also, when an instance of a property definition no longer applies to a user or group, you will learn how to remove the user or group from this instance.

Create or Edit an Instance of a Property Definition

To create a new instance or edit an existing instance of a property definition, perform the following steps:

1. Access the System Configuration form.
2. If you are creating a new instance of a property definition, click **New** on the Toolbar. Ensure that the values in the **Name** and **Keyword** fields are the same for all instances of this property definition (for example, *Record Read Limit*, *XL.READ_LIMIT*).

   Note: It is recommended that you copy these values from the other instances of this property definition to minimize any chance of a typing error.

   If you are editing an existing instance of a property definition, query for the property definition.
3. Select the **Client**, **Client/Server**, or **Server** radio button depending on whether the instance of this property definition will apply to the Client only, both the Client and the Server, or just the Server.
4. Designate whether you wish this instance of the property definition to apply to all users or only to select users and user groups by selecting or clearing the **System** check box.

   Note: If you selected the **Server** radio button in Step 3, the **System** check box will be disabled. When this occurs, proceed to Step 5.

5. Enter the desired value in the **Value** field. This will be the value of the property for this instance of the definition.
6. Click **Save**. The instance of the property definition is created or modified.

Now that you have added or edited an instance of a property definition, you will learn how to assign users and groups to this instance.

Assign a User or Group to an Instance of a Property Definition

To assign a user or group to an instance of a property definition, perform the following steps:

> **Caution:** If this is a system-wide instance (i.e., the **System** check box is selected), it will be applied to *all* users and groups. As a result, you do not need to assign it to a particular user or group.

1. Access the System Configuration form.
2. Query for the instance of the property definition you wish to assign to a user or group.

> **Note:** To learn more about the various property definitions to which you can assign users and groups, refer to "System Properties" on page A-17.

3. Select the **Client**, **Client/Server**, or **Server** radio button, depending on whether the instance of this property definition will apply to the Client only, both the Client and the Server, or just the Server.
4. To assign the property instance to one or more users, click the **Users** tab. Otherwise, to assign the property instance to one or more user groups, click the **Groups** tab.
5. Click **Assign**. The Assignment dialog box is displayed.
6. Select and assign the desired users or groups and then, click **OK**.
7. Click **Save**. The instance of the property definition is assigned to the user(s) and/or group(s) you selected in Step 6.

Remove a User or Group From an Instance of a Property Definition

To remove a user or group from an instance of a property definition, perform the following steps:

1. Access the System Configuration form.
2. Query for the instance of the property definition from which you wish to remove a user or group.
3. Highlight the desired user or group (from the **Users** or **Groups** tabs, respectively).
4. Click **Delete**. The user or group is removed from the instance of the property definition. As a result, the property is no longer associated with the user or group.

The Remote Manager Form

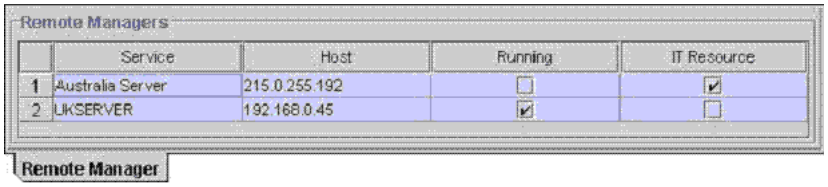
The Remote Manager is a light-weight network component (server) that enables to integrate with target systems whose APIs do not have the ability to communicate over a network, or do have network awareness but are not secure. This is accomplished by having a Remote Manager work as a server on the target system, and an Oracle

Identity Manager Server work as its client, such that the Oracle Identity Manager Server sends a request for the Remote Manager to instantiate the target system APIs on the target system itself, and invokes methods on its behalf.

The Remote Manager form, as shown in Figure 8–10, is located in the Oracle Identity Manager Administration folder. It is used to display the following:

- The names and IP addresses of the remote managers that communicate with Oracle Identity Manager.
- Whether the remote manager is running.
- Whether it represents IT resource(s) that Oracle Identity Manager can use.

Figure 8–10 The Remote Manager Form



For this example, there are two remote managers that can communicate with Oracle Identity Manager: Australia Server and UKSERVER.

The Australia Server remote manager has an IP address of *215.0.255.192*. Though it can handshake with Oracle Identity Manager, because the **Running** check box is cleared, the remote Server is down. Lastly, the **IT Resource** check box is selected, signifying that this remote manager represents IT resource(s) that can be used by Oracle Identity Manager.

The UKSERVER remote manager has an IP address of *192.168.0.45*. Since the **Running** check box is selected, the remote Server is operable. However, because the **IT Resource** check box is cleared, this remote manager does not represent IT resource(s) that Oracle Identity Manager can use.

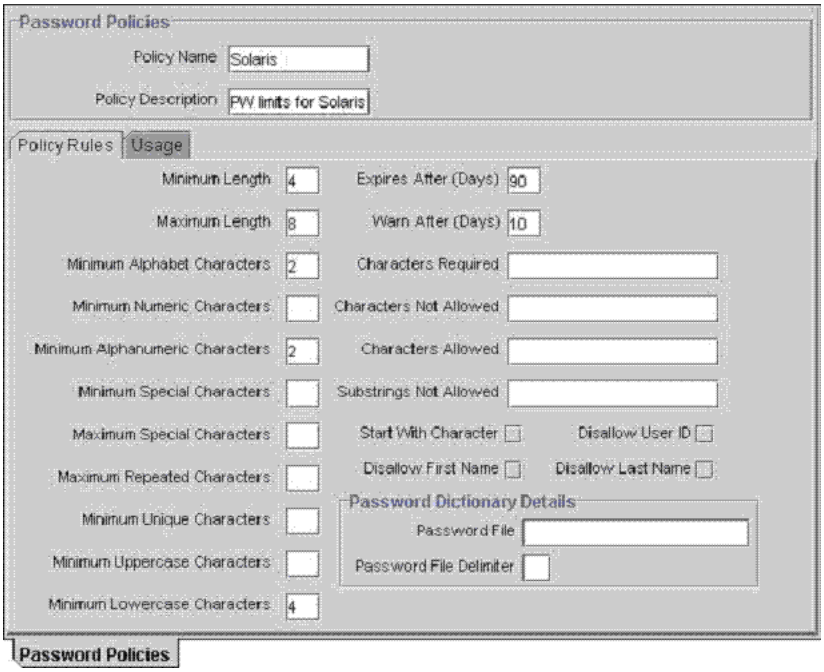
Note: To learn how the Remote Manager form is used with other Oracle Identity Manager forms, refer to *Oracle Identity Manager Tools Reference Guide*.

The Password Policies Form

The Password Policies form, as shown in Figure 8–11, is located in the Oracle Identity Manager Administration/Policies folder. It is used to:

- Set password restrictions (for example, defining a password's minimum and maximum length).
- See the rules and resource objects that are associated with a password policy.

Figure 8–11 The Password Policies Form



You will now learn about the data fields of the Password Policies form. The following table describes the data fields of this form.

Field Name	Description
Policy Name	The password policy's name.
Policy Description	Explanatory information about the password policy.

Now that we have reviewed password policies and the data fields of the Password Policies form, you are ready to create a password policy.

Create a Password Policy

To create a password policy, perform the following steps:

1. Open the Password Policies form.
2. In the **Policy Name** field, enter the name of the password policy 3.
3. In the **Policy Description** field, enter explanatory information about the password policy.
4. Click **Save**. The password policy is created.

Note: Once a password policy is created, it must be supplied with criteria and associated with a resource. To supply your password policy with criteria, use the **Policy Rules** tab of this form. To associate your password policy with a resource, use the **Password Policies Rule** tab of the Resource Object form to create a password policy/rule combination that will be evaluated when accounts are created or updated on the resource. The password policy will then be invoked and applied when that rule's criteria are satisfied. Multiple resources can use each password policy.

Tabs on the Password Policies Form

Once you launch the Password Policies form, and create a password policy, the tabs of this form become functional.

The Password Policies form contains the following tabs:

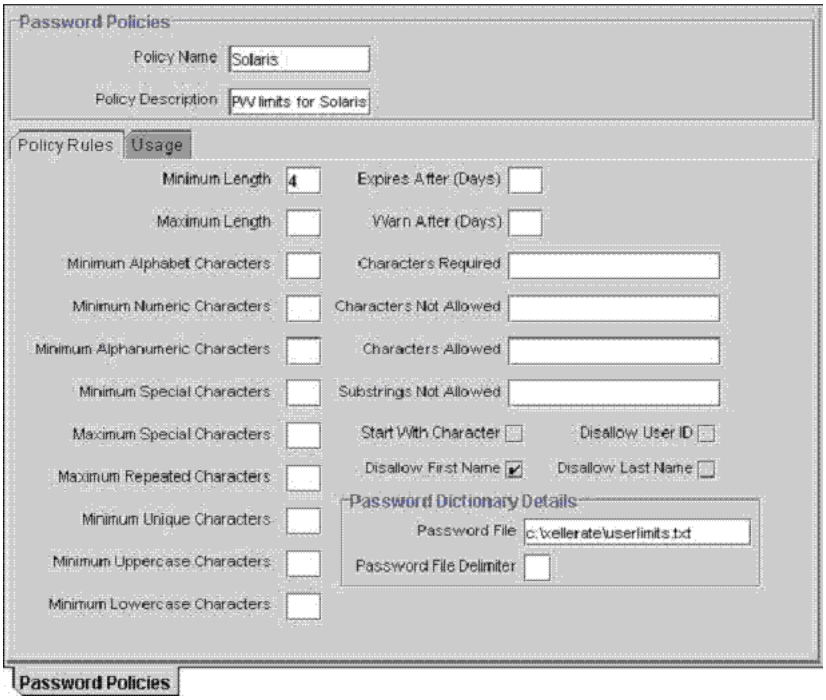
- "Policy Rules" on page 8-20
- "Usage" on page 8-24

Each of these tabs is covered in greater detail in the following sections.

Policy Rules

Figure 8–12 displays the Policy Rules tab of the Password Policies Form.

Figure 8–12 The Policy Rules Tab of the Password Policies Form



This tab is used to specify the criteria of your password policy (for example, defining a password's minimum and maximum length).

You may use either or both of the following methods to set password restrictions:

- Enter information into the appropriate text boxes or select the desired check boxes. As an example, to indicate that a password must have a minimum length of four characters, type *4* into the **Minimum Length** text box. For another example, to prohibit Oracle Identity Manager from accepting a user's first name as a valid password, select the **Disallow First Name** check box.
- Enter a path and filename into the **Password File** text box (for example, *c:\xellerate\userlimits.txt*). This file contains pre-defined terms that are not allowed as passwords. The delimiter specified in the Password File Delimiter field separates these terms.

Now that we have reviewed password restrictions, you will learn about the data fields of the **Policy Rules** tab. These are the fields into which you will specify the password limitations.

> **Note:** If a data field is empty, the password does not have to meet the criteria of that field for it to be valid. For example, when the **Minimum Numeric Characters** and **Maximum Numeric Characters** data fields are blank, Oracle Identity Manager will accept the password, regardless of how many digits it has.

The following table describes the data fields of the Policy Rules tab.

Field Name	Description
Minimum Length	The fewest number of characters that a password can have for it to be valid. For example, if *4* appear in the **Minimum Length** text box, the password must have at least four characters for it to be accepted.
Maximum Length	The highest number of characters that a password can have for it to be valid. As an example, if *8* appear in the **Maximum Length** text box, the password will not be accepted if it has more than eight characters.
Minimum Alphabet Characters	The fewest number of letters that a password can have for it to be valid. For example, if *2* appear in the **Minimum Alphabet Characters** text box, the password will not be accepted if it has fewer than two letters.
Minimum Numeric Characters	The fewest number of digits that a password can have for it to be valid. As an example, if *1* appears in the **Minimum Numeric Characters** text box, the password must have at least one number for it to be accepted.
Minimum Alphanumeric Characters	The fewest number of letters *or* digits that a password can have for it to be valid. For example, if *6* appear in the **Minimum Alphanumeric Characters** text box, the password must be comprised of at least six letters or numbers for it to be accepted.

Field Name	Description
Minimum Special Characters	The fewest number of non-alphanumeric characters (for example, #, %, or &) that a password can have for it to be valid. As an example, if *1* appears in the **Minimum Special Characters** text box, the password must have at least one non-alphanumeric character for it to be accepted.
Maximum Special Characters	The highest number of non-alphanumeric characters that a password can have for it to be valid. For example, if *3* appear in the **Maximum Special Characters** text box, the password will not be accepted if it has more than three non-alphanumeric characters.
Maximum Repeated Characters	The highest number of duplicate characters that a password can have for it to be valid. As an example, if *2* appear in the **Maximum Repeated Characters** text box, the password will not be accepted if more than two characters are repeated. So, for this example, *RL112233* would not be a valid password (three characters of the password are repeated).
Minimum Unique Characters	The fewest number of non-repeating characters that a password can have for it to be valid. As an example, if *1* appears in the **Minimum Unique Characters** text box, the password will not be accepted if every character of the password is repeated at least once. Therefore, for this example, *1a23a321* would not be a valid password (each character of the password is repeated).
Minimum Uppercase Characters	The fewest number of uppercase letters that a password can have for it to be valid. For example, if *8* appear in the **Minimum Uppercase Characters** text box, the password will not be accepted if it has fewer than eight uppercase letters.
Minimum Lowercase Characters	The fewest number of lowercase letters that a password can have for it to be valid. As an example, if *8* appear in the **Minimum Lowercase Characters** text box, the password will not be accepted if it has fewer than eight lowercase letters.
Expires After (Days)	The maximum number of days for which a password is valid. For example, if *30* appear in the **Expires After (Days)** text box, and the password is created on November 1, it will not be valid on December 1 (31 days will have elapsed).
Warn After (Days)	The number of days that will pass before a user is notified that a password will expire on a designated date. As an example, suppose *30* appear in the **Expires After (Days)** text box, *10* is displayed in the **Warn After (Days)** text box, and the password is created on November 1. On November 11, the user will be informed that the password will expire on December 1.
Characters Required	The characters that a password *must* have for it to be valid. For example, if x appears in the **Characters Required** text box, the password will be accepted only if it contains an "*x*".
Characters Not Allowed	The characters that a password *must not* have for it to be valid. As an example, if *!* appears in the **Characters Not Allowed** text box, the password will not be accepted if it contains an "*!*".

Field Name	Description
Characters Allowed	The characters that a password *can* have for it to be valid. For example, if % appears in the **Characters Allowed** text box, the password will be accepted if it contains a "%".
Substrings Not Allowed	A series of consecutive alphanumeric characters that a password *must not* have for it to be valid. As an example, if *IBM* appears in the **Substrings Not Allowed** text box, the password will not be accepted if it contains the letters "*I*", "*B*", and "*M*", in successive order.
Start With Character	This check box is used to specify whether a password is to begin with a character. By selecting this check box, the password must start with a character for it to be valid. If you clear this check box, the password will be accepted, even if it does not begin with a character.
Disallow First Name	This check box is used to specify whether the user's first name is to be accepted as all or a portion of the password. By selecting this check box, the password will not be valid if the user's first name is entered into the **Password** field. If you clear this check box, the password will be accepted, even if it contains the user's first name.
Disallow User ID	This check box is used to specify whether the User ID is to be accepted as all or a portion of the password. By selecting this check box, the password will not be valid if the User ID is entered into the **Password** field. If you clear this check box, the password will be accepted, even if it contains the User ID.
Disallow Last Name	This check box is used to specify whether the user's last name is to be accepted as all or a portion of the password. By selecting this check box, the password will not be valid if the user's last name is entered into the **Password** field. If you clear this check box, the password will be accepted, even if it contains the user's last name.
Password File	The path and name of a file that contains pre-defined terms, which are not allowed as passwords. Note: If any settings in the **Policy Rules** tab differ from the specifications in the password file, Oracle Identity Manager will defer to the tab's settings.
Password File Delimiter	The character used to separate terms in the password file from one another. For example, if a "," appears in the **Password File Delimiter** text box, the terms of the password file will be separated by commas.

Now that we have reviewed the data fields of the **Policy Rules** tab, you are ready to specify the criteria (or rules) for the password policy.

Set the Criteria for a Password Policy

1. Access the desired password policy definition.
2. Click the **Policy Rules** tab.

3. Enter information into the appropriate text boxes.

   AND/OR

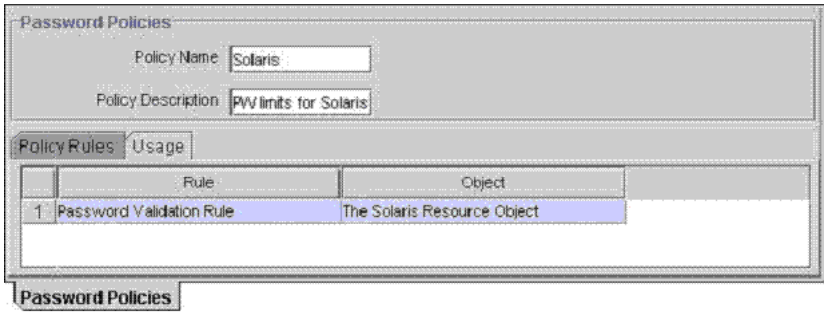
   Select the desired check boxes.

4. Click **Save**. The rules for the password policy are set.

Usage

Figure 8–13 displays the Usage tab of the Password Policies form.

Figure 8–13 The Usage Tab of the Password Policies Form



Within this tab, you can see the rules and resource objects that are associated with the current password policy.

For this example, the *Solaris* password policy and the *Password Validation Rule* have been assigned to *The Solaris Resource Object*.

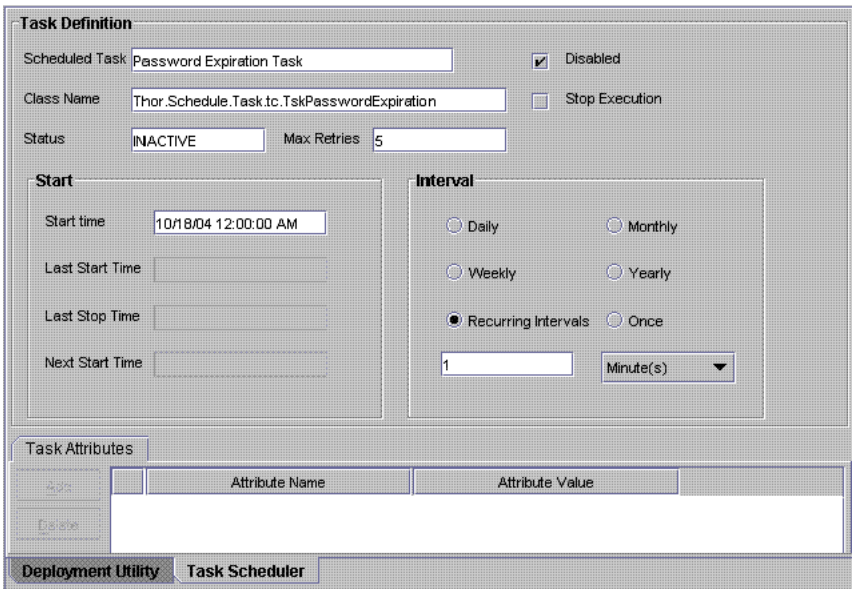
> **Note:** For more information on the relationship between password policies and resource objects, refer to "Password Policies Rule" on page 6-24.

The Task Scheduler Form

The Task Scheduler form, as shown in Figure 8–14, is located in the Oracle Identity Manager Administration/Job Scheduling Tools folder. It is used to define:

- When your tasks are scheduled to be run
- The attributes of these scheduled tasks

Figure 8–14 The Task Scheduler Form



Caution: As stated above, the Task Scheduler form is used to determine when a task is scheduled to be run. However, the Oracle Identity Manager program that triggers the execution of this task is referred to as the **scheduler daemon**.

Since the scheduler daemon cannot perform its designated function if it is not running, you must verify that is it active.

For more information on modifying the value of a system property, refer to "The System Configuration Form" on page 8-14.

The following table lists and describes the data fields of the Task Scheduler form.

Field Name	Description
Scheduled Task	The name of the task that is scheduled to be run.
Class Name	The name of the Java class that executes the scheduled task. **Important**: The scheduler daemon triggers the execution of a scheduled task. The Java class actually executes the task.
Status	The task's status. Currently, a scheduled task has four status levels: ▪ **INACTIVE**. The scheduled task is not running. Also, a task's status is *INACTIVE* if it has been executed successfully, and it is set to run again (at the date and time specified in the **Next Start Time** field). ▪ **RUNNING**. The scheduled task is being executed. ▪ **COMPLETED**. The scheduled task has been executed successfullyThe task will not run again (the **Once** radio button is selected). ▪ **ERROR**. A problem occurred while the task was being executed.

Field Name	Description
Max Retries	If the task is not completed, the number of times that Oracle Identity Manager attempts to complete the task before assigning a status of *ERROR* to it.
Disabled	This check box is used to designate whether the scheduler daemon triggers a scheduled task. If this check box is selected, the scheduler daemon does not trigger the task, even when the date and time that appears in the **Start Time** or **Next Start Time** fields matches the current date and time. When this check box is cleared, and the date and time that is displayed in the **Start Time** or **Next Start Time** fields matches the current date and time, the scheduler daemon triggers the task.
Stop Execution	This check box is used to designate whether the scheduler daemon can stop a scheduled task with a status of *RUNNING*. If this check box is selected, and the task's status is *RUNNING*, the scheduler daemon stops the task from being executed. In addition, the task's status changes to *INACTIVE*. When this check box is cleared, the scheduler daemon does not stop a task with a status of *RUNNING* from being executed.
Start Time	The date and time of when the task is scheduled to run for the first time. **Note**: If the task is set to be run more than once, the scheduler daemon refers to the date and time that appears in the **Next Start Time** field.
Last Start Time	The latest date and time of when the task started to run.
Last Stop Time	The most recent date and time of when the task stopped running.
Next Start Time	The subsequent date and time of when the task is scheduled to run. **Note**: If the task is set to be run only once, the scheduler daemon refers to the date and time that is displayed in the **Start Time** field.
Daily, Weekly, Monthly, Yearly	These radio buttons are used to designate whether the task is to be run daily, weekly, monthly, or annually, respectively. If one of these radio buttons are selected, the scheduler daemon triggers the associated task once a day, week, month, or year, at the date and time specified in the **Start Time** field. When all of these radio buttons are cleared, the scheduler daemon does not trigger the associated task on a daily, weekly, monthly, or annual basis.
Recurring Intervals	This radio button is used to designate that the task is to be run on a fixed, recurring basis. If this radio button is selected, the scheduler daemon triggers the associated task on a recurring basis. When this radio button is cleared, the scheduler daemon does not trigger the associated task on a recurring basis. **Note**: If the **Recurring Intervals** radio button is selected, you must set the interval by entering a value into the text field below the radio button, and selecting a unit of measure from the adjacent combo box.

Field Name	Description
Once	This radio button is used to designate that the task is to be run only once. If this radio button is selected, the scheduler daemon triggers the associated task once, at the date and time specified in the **Start Time** field. When this radio button is cleared, the scheduler daemon triggers the associated task more than once.

Create a Task Schedule

To create a task schedule, perform the following steps:

1. Access the Task Scheduler form.
2. Enter the name of the scheduled task in the **Scheduled Task** field.
3. Enter the name of the Java class that executes the scheduled task in the **Class Name** field.
4. Enter a number into the **Max Retries** field. This number represents how many times Oracle Identity Manager attempts to complete the task before assigning a status of *ERROR* to it.
5. Ensure that the **Disabled** and **Stop Execution** check boxes are cleared.
6. Double-click the **Start Time** field. From the Date & Time window that appears, set the date and time that the task is scheduled to run. If you have specified that the task is to be executed on a recurring basis (by selecting the **Recurring Intervals** radio button), the date and time that is displayed in this field is referenced to determine when next to run the associated task.
7. Set the scheduling parameters (in the **Interval** region):
   - To set the task to run on a recurring basis, select the **Daily**, **Weekly**, **Monthly**, or **Yearly** radio buttons.
   - To set the task to run only once, select the **Once** radio button.
   - To set the task to run on a fixed, recurring basis, select the **Recurring Intervals** radio button. Then, set the interval by entering a value into the text field below the radio button. Then select a unit of measure from the adjacent combo box.
8. Click **Save**. The task schedule is created. In addition, *INACTIVE* is displayed within the **Status** field (since the task is not currently running). However, once the date and time that you set in Step 6 matches the current date and time, the scheduler daemon triggers the scheduled task.

Now that you have defined a schedule for a task, if the task needs attributes, you must set them. Otherwise, the task schedule is not functional.

Also, when an existing task attribute is no longer relevant, you must remove it from the task schedule.

The following procedures show you how to add an attribute to a task schedule, and remove a task attribute from the task schedule.

Add a Task Attribute

To add a task attribute, perform the following steps:

1. Click **Add**.
2. Within the **Attribute Name** field, enter the name of the task attribute.
3. Within the **Attribute Value** field, type the attribute's value.
4. From the Toolbar, click **Save**. The task attribute is added to the task schedule.

Remove a Task Attribute

To remove a task attribute, perform the following steps:

1. Highlight the task attribute that you want to remove.
2. Click **Delete**. The attribute is removed from the task schedule.

9

Development Tools

This chapter describes the full suite of development tools in Oracle Identity Manager. It contains the following topics:

Overview

Oracle Identity Manager provides a full suite of development tools that enable advanced System Administrators or developers to customize Oracle Identity Manager. This folder contains the following forms:

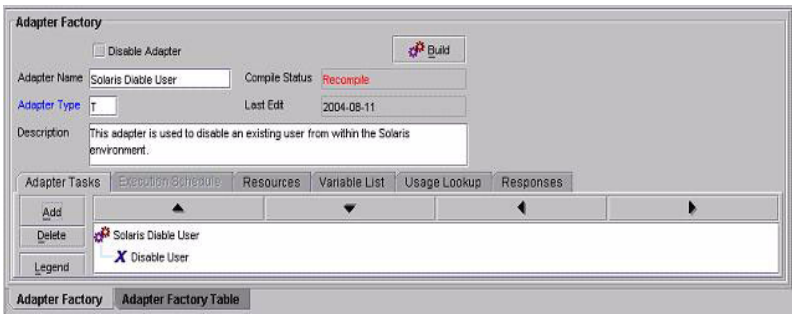
- Adapter Factory: This form is used to create and manage the code, which enables Oracle Identity Manager to communicate with any IT Resource simply by connecting to that resource's API. This code is known as an adapter.
- Adapter Manager: This form is used to compile multiple adapters simultaneously.
- Form Designer: This form is used to create process and resource object forms that do not come packaged with Oracle Identity Manager.
- Error Message Definition: This form is used to create the error messages that appears in dialog boxes when certain problems occur while using Oracle Identity Manager. In addition, this form enables a System Administrator or developer to define the error messages that users can access when they create error handler tasks using the Adapter Factory form.
- The Development Tools/Business Rule Definition folder provides System Administrators and developers with the tools necessary to manage event handlers and data objects in Oracle Identity Manager. This folder contains the following forms:
  - Event Handler Manager: This form allows you to create and manage the event handlers that are used with Oracle Identity Manager.
  - Data Object Manager: Through this form, you can define a data object, assign event handlers and adapters to it, and map any adapter variables associated with it.
- Reconciliation Rules: This form is used to create and manage reconciliation rules in Oracle Identity Manager.

The Adapter Factory Form

The Adapter Factory is a code-generation tool, provided by Oracle Identity Manager that enables a user to create Java classes, known as adapters. Figure 9–1 displays the Adapter Factory Form.

Adapters extend the internal logic and functionality of Oracle Identity Manager. In addition, they interface with any IT Resource, simply by connecting to that resource's API.

Figure 9–1 The Adapter Factory Form

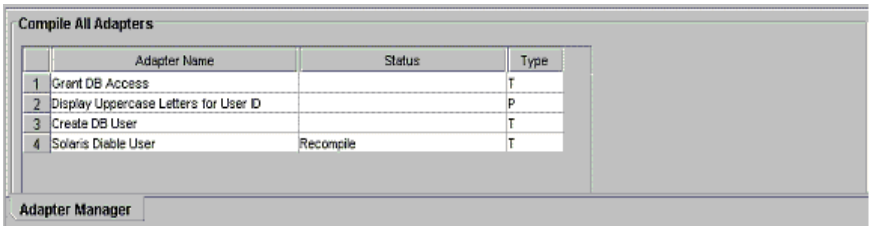


Note: For more information on adapters or the Adapter Factory, refer to *Oracle Identity Manager Tools Reference Guide*.

The Adapter Manager Form

The Adapter Manager form is located in the Development Tools folder. It is used to compile multiple adapters simultaneously, as shown in Figure 9–2.

Figure 9–2 The Adapter Manager Form



The Form Designer Form

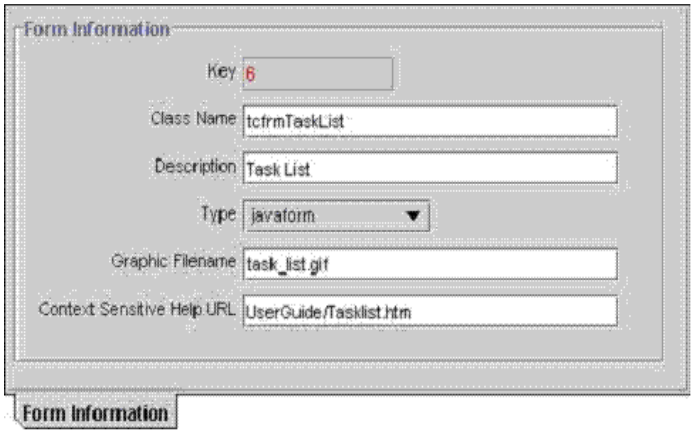
Sometimes, the information required to provision resources to a target user or organization cannot be retrieved from any existing Oracle Identity Manager form. When this occurs, you need to use the Form Designer form (located in the Development Tools folder) to create a form with fields that contain the relevant information. Then, you have to assign this form to the process or resource object that is associated with provisioning resources to the user or organization. Figure 9–3 displays the Form Designer Form.

There are four reasons why Oracle Identity Manager displays a resource object or process form that a user creates using the Form Designer form. These reasons, in order of importance, are:

1. If the resource object form is attached to a resource object that is requested, and the Launch Object Form menu command is selected (by right-clicking the resource object from the Process Console tab of the Requests form).
2. When the resource object form is attached to a resource object that is direct provisioned.
3. If the process form is attached to the standard approval process, and the Launch Form menu command is selected (by right-clicking the process from the Process Console tab of the Requests form).
4. When the process form is attached to the appropriate provisioning process, and the Launch Form menu command is selected (by right-clicking the process from the Object Process Console tab of the Organizations or Users forms).

As an example, when Oracle Identity Manager or one of its users attempts to complete the resource object or process, the assigned form is triggered. When this occurs, either Oracle Identity Manager or a user populates the fields of this form. After the data is saved, the corresponding process or resource object can achieve a status of Completed, and Oracle Identity Manager can provision the appropriate resources to the target organizations or users.

Figure 9–3 The Form Designer Form



For this example, the Solaris form (represented by the UD_SOLARIS name in the Table Name field) has been created and assigned to both the Solaris resource object and provisioning process.

> **Note:** The table name contains the `UD_ prefix`, followed by the form name. So, for this example, since the name of the form is SOLARIS, its table name is `UD_SOLARIS`.

The following table describes the data fields of the Form Designer form

Field Name	Description
Table Name	The name of the database table that is associated with the form. **Note**: The table name contains the `UD_ prefix`, followed by the form name. So, if the name of the form were SOLARIS, its table name would be `UD_SOLARIS`.

Field Name	Description
Description	Explanatory information about the form. **Important**: The text that appears in the Description field is the name of the form.
Preview Form	When you click this button, the form appears. This way, you can see how it looks and functions before you make it active.
Form Type	These radio buttons are used to designate whether the form is to be assigned to a process or a resource object. If you select the Process radio button, then the form is associated with an approval or provisioning process. By selecting the Object radio button, the form is to be assigned to a resource object.
Object Name	This is the name of the resource that can be provisioned (for example, a database, server, software application, file, or directory access). Also, referred to as a *resource object name*. Double-click in this field to see the available resource object names.
Latest Version	The most recent version of the form.
Active Version	The version of the form that is used with the designated process or resource object. **Note**: Once a version of the form appears in the Active Version field, it cannot be modified.
Current Version	This version of the form is the one being viewed and has information, which appears throughout the various tabs of the Form Designer form.
Create New Version	If you click this button, you can assign an additional name to the existing version of a form. As a result, you can modify this version, without impacting the original version of the form. **Note**: If you create a new version of the form and click **Refresh**, the name that you provided for this version appears in the Current Version combo box.
Make Version Active	By clicking this button, you can specify that the current version of the form is be the one that is to be assigned to the process or resource object. In other words, this version is now active. **Note**: Once a version of the form is active, it cannot be modified. Instead, you must construct an additional version of the form (by clicking the Create New Version button).

Now that we have reviewed forms and the data fields of the Form Designer form, you are ready to create a form.

Create a Form

To create a form, perform the following steps:

1. Open the Form Designer form.
2. In the Table Name field, type the name of the database table that is associated with the form.

> **Note:** The table name contains the `UD_ prefix`, followed by the form name. So, if the name of the form were SOLARIS, its table name would be `UD_SOLARIS`.

3. In the Description field, enter explanatory information about the form.
4. If the form is assigned to an approval or provisioning process, select the Process radio button. If the form is to be assigned to a resource object, select the Object radio button.
5. Click **Save**. The form is created. In addition, the words Initial Version appear in the Latest Version field. This signifies that you can populate the tabs of the Form Designer form with information, so the form is functional with its assigned process or resource.

Tabs of the Form Designer Form

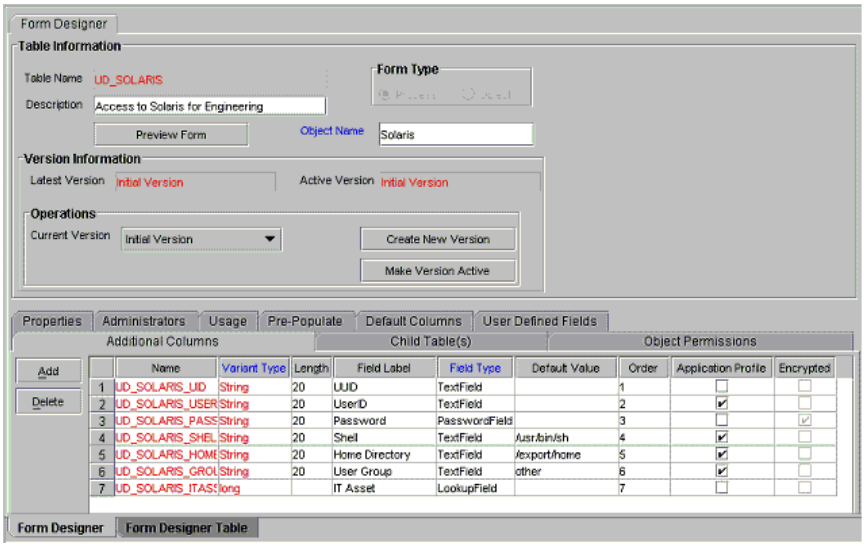
Once you launch the Form Designer form, and create a form, the tabs of this form become functional. The Form Designer form contains the following tabs:

Each of these tabs is covered in greater detail in the following sections.

Additional Columns

Figure 9–4 displays the Additional Columns tab of the Form Designer Form. This tab is used to create and manage data fields. These data fields appears on the associated form that is created through the Form Designer form.

Figure 9–4 The Additional Columns Tab of the Form Designer Form



The following table contains various characteristics of the data fields.

Name	Description
Name	The name of the data field, which appears in the database, and is recognized by Oracle Identity Manager. **Note**: This name is comprised of the **<TABLENAME_>** prefix, followed by the name of the data field. So, if the name that appears in the Table Name field of the Form Designer form is *UD_PASSWORD*, and the name for the data field is USERNAME, the data field name, which appears in the database, and Oracle Identity Manager recognizes, would be *UD_PASSWORD_USERNAME*.
Variant Type	From this Lookup field, select the variant type for the data field. The variant type denotes the type of data that the field accepts. This data field must be one of nine variant types: *Byte*, *Double*, *Date*, *Byte Array*, *Boolean*, *Long*, *String*, *Short*, and *Integer*.
Length	The length (in characters) of the data field.
Field Label	The label that is associated with the data field. This label appears next to the data field on the form that is generated by Oracle Identity Manager.

Name	Description
Field Type	From this Lookup field, select the data type of the data field. The data type represents how the data appears within the field. This data field must be one of the following nine data types: ■ Text Field: This data field appears on the generated form as a text field. If the text field is display-only (the text within the field appears in red), a user can only use the field to perform a query. Otherwise, the user can also populate the field with information, and save it to the database. ■ Lookup Field: This data field appears on the generated form as a Lookup field. If this Lookup field is display-only, a user can only use the field to perform a query. Otherwise, the user can also populate the field with a value from the associated Lookup window, and save this value to the database. ■ Text Area: This data field appears on the generated form as a text area. If this text area is display-only, a user can only read the information that is displayed within the text area. Otherwise, the user can also populate the text area with data, and save this information to the database. ■ IT Resource Lookup Field: This data field appears on the generated form as a Lookup field. From this Lookup field, a user can select a lookup value, which represents an IT Resource, and save this value to the database. **Important**: If you select this data field, you must specify the type of server for the IT Resource from the combo box that appears within the Property Value text box. For more information on adding a property value to a data field, refer to "Add a Property and Property Value to a Data Field" on page 9-13. ■ Date Field: This data field appears on the generated form as a text field. If this text field is display-only, a user can only use the field to perform a query. Otherwise, the user can also populate the field with a date and time (by double-clicking the field and selecting a date and time from the Date & Time window that appears). Then, this date and time can be saved to the database. ■ Check Box: This data field appears on the generated form as a check box. If this check box is display-only, a user can only see whether the check box is selected or cleared. Otherwise, the user can also select or clear the check box, and save this setting to the database. ■ Password Field: This data field appears on the generated form as a text field. From this text field, a user can either query for an encrypted password (it appears as a series of asterisks [*], or populate the field with an encrypted password, and save it to the database. ■ Radio Button: This data field appears on the generated form as a radio button. A user can select or clear the radio button, and save this setting to the database. ■ Combo Box: This data field appears on the generated form as a combo box. A user can select an item from the combo box, and save this selection to the database.
Default Value	This value appears within the associated data field once the form is generated, and if no other default value has been specified from the scenarios listed below: ■ A pre-populate adapter, which is attached to the form field, is executed. ■ A data flow exists between a field of a custom form assigned to a resource object and a field of a custom form associated with a process. ■ A data flow exists between a field of a custom form assigned to one process and a field of a custom form associated with another process. ■ A resource object, which has been requested for an organization, has a custom form attached to it. In addition, one of the fields of this custom form has a default value associated with it.

Name	Description
Order	The sequence number, which represents where the data field is positioned on the generated form. For example, a data field with an order number of 2 appears below a data field with an order number of 1.
Application Profile	This check box is used to designate whether the most-recent value of this field should appear on the Object Profile tab of the Users form once the resource associated with this form has been provisioned to the user, and achieved a status of Enabled. If this check box is selected, the label and value of this field appears on the Object Profile tab of the Users form for users provisioned with the resource. If this check box is cleared, the value of this field does not appear on the Object Profile tab of the Users form for users provisioned with the resource.
Encrypted	This check box is used to determine whether the information, which appears within the associated data field, is to be encrypted when it is transmitted between the Server and the Client. If this check box is selected, the information that is displayed within the data field will be encrypted when it is transmitted between the Client and the Server. When this check box is cleared, the information that appears in the data field will not be encrypted as it is transmitted between the Server and the Client.

Important: When creating a data field of text (field type) with the Encrypted option selected, the values appears as clear text in the Administrative and User Console and the data will be encrypted in the database.

When creating a data field of password (type field) with the Encrypted option selected, the value appears as asterisks (*) in the Administrative and User Console and the data will be encrypted in the database.

Now that we have reviewed the relationship between data fields and a form, you will learn how to add a data field to a form. In addition, once a data field is no longer valid, you will learn how to remove it from the form.

Add a Data Field to a Form

To add a data field to a form, perform the following steps:

1. Click **Add**. A blank row appears within the Additional Columns tab.
2. In the **Name** field, enter the name of the data field, which appears in the database, and is recognized by Oracle Identity Manager.

   Note: This name is comprised of the <**TABLENAME**_> prefix, followed by the name of the data field.

   So, if the name that appears in the Table Name field is `UD_PASSWORD`, and the name for the data field is USERNAME, the data field name, which appears in the database, and Oracle Identity Manager recognizes, would be `UD_PASSWORD_USERNAME`.

3. Double-click the Variant Type lookup field. From the Lookup window that appears, select the variant type for the data field. Currently, a data field can have

one of nine variant types: *Byte*, *Double*, *Date*, *Byte Array*, *Boolean*, *Long*, *String*, *Short*, and *Integer*.

4. In the **Length** field, enter the length (in characters) of the data field.
5. In the **Field Label** field, enter the label that will be associated with the data field. This label appears next to the data field on the form that is generated by Oracle Identity Manager.
6. Double-click the **Field Type** lookup field. From the Lookup dialog box that is displayed, select the data type for the data field. Presently, a data field can have one of nine data types: Text Field, Lookup Field, Text Area, IT Resource Lookup Field, Date Field, Check Box, Password Field, Radio Button, and Combo Box.

   Note: For more information on data types, refer to the table, which appears earlier in this section.

7. In the Default Value field, enter the value that appears within the associated data field once the form is generated, and if no other default value has been specified.

   Note: For more information on the scenarios where a default value could be set, refer to the table that appears earlier in this section.

8. In the Order field, enter the sequence number, which will represent where the data field will be positioned on the generated form. For example, a data field with an order number of 2 appears below a data field with an order number of 1.
9. If you want a specific organization or user's values to supersede the value that appears in the Default Value field, select the Application Profile check box. Otherwise, proceed to Step 10.
10. If you want the information that appears within the data field to be encrypted when it is transmitted between the Client and the Server, select the Encrypted check box. Otherwise, proceed to Step 11.
11. Click **Save**. The data field is added to the form.

Remove a Data Field From a Form

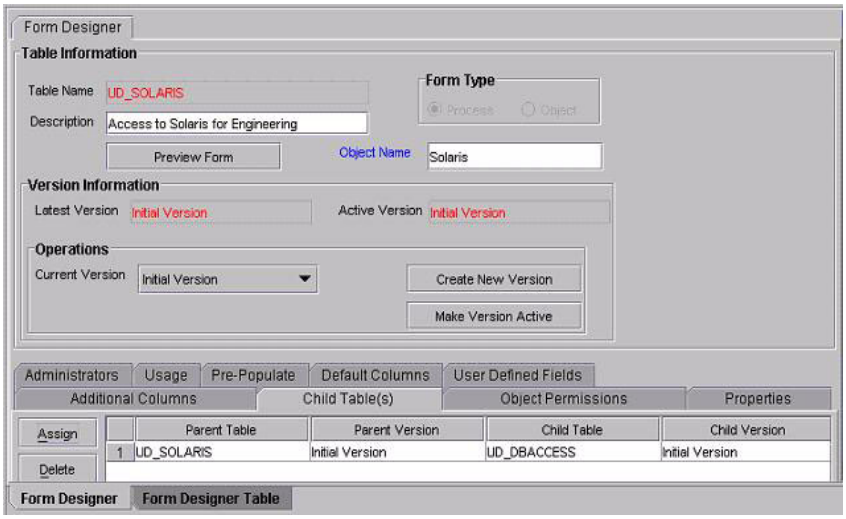
To remove a data field from a form, perform the following steps:

1. Highlight the data field that you want to remove.
2. Click **Delete**. The data field is removed from the form.

Child Table(s)

Figure 9–5 displays the Child Table(s) tab on the Form Designer Form.

Figure 9–5 The Child Table(s) Tab of the Form Designer Form



Sometimes you may have to add the same data fields to multiple forms that are created using the Form Designer form. There are two ways to do this:

- You can add the data fields to each form manually, through the form's Additional Columns tab.
- You can group the data fields together and save them under one form name. Then, you can assign this form to each form that requires these data fields.

This form, which contains the data fields that are required by another form, is known as a child table.

Assigning child tables to a form increases your efficiency as a user. Without child tables, for every form that needs data fields, you would have to set the parameters for each field. So, if five forms require the identical data field, you would have to set the parameters for this field five, separate times (one for each form).

If you use a child table for one form, and then decide that you want to apply it to another form, Oracle Identity Manager enables you to do so. Simply remove the child table from the first form, and assign it to the target form. This way, the child table that you assign to one form can be reused for all forms created with the Form Designer form.

In addition, you can configure Oracle Identity Manager to perform one of the following actions within a column of a child table:

- Insert. Add a new value to the designated column of the child table.
- Update. Modify an existing value from the corresponding column of the child table.
- Delete. Remove a value from the designated column of the child table.

> **Note:** For more information on setting up Oracle Identity Manager to insert, edit, or delete a value from within a column of a child table, refer to "The Process Definition Form" on page 7-5.

For this example, the UD_SOUTH child table is assigned to the Results of 1Q 2004 Sales form (represented by the UD_SALES2 table name). Once this form is launched, the data fields contained within the UD_SOUTH child table appears within the form.

Now that we have reviewed child tables, you will learn how to assign a child table to a form. In addition, when you no longer want the data fields of a child table to appear on a form, you will learn how to remove a child table from a form.

> **Important:** If the form, which is represented by the child table, has not been made active, you cannot assign it to the parent form.

Assign a Child Table to a Form

To assign a child table to a form, perform the following steps:

1. Click **Assign**. The Assignment window is displayed.
2. From this window, select the child table, and assign it to the form.
3. Click **OK**. The selected child table is assigned to the form.

> **Important:** If the form, which is represented by the child table, has not been made active, it will not appear within the Assignment window. As a result, you cannot assign it to the parent form.

Remove a Child Table From a Form

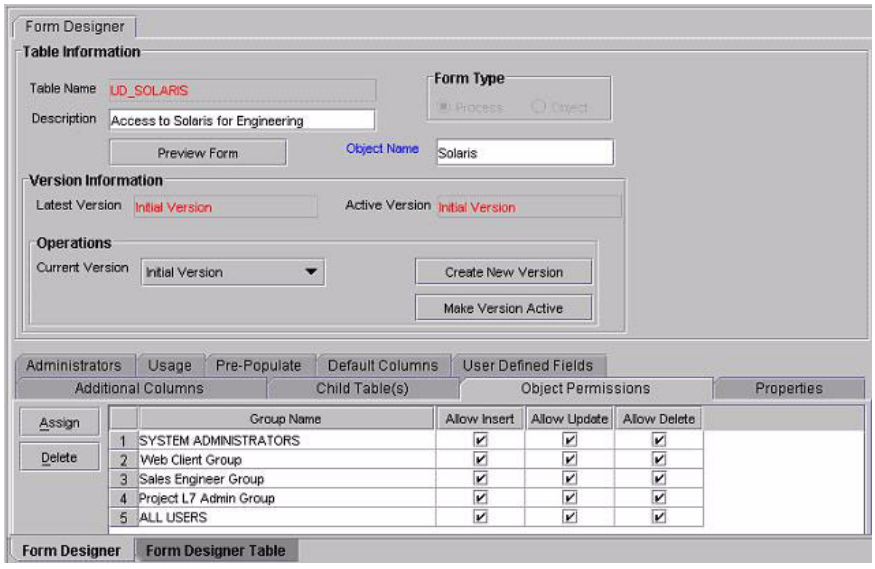
To remove a child table from a form, perform the following steps:

1. Highlight the child table that you want to remove.
2. Click **Delete**. The child table is removed from the form.

Object Permissions

Figure 9–6 displays the Object Permissions tab of the Form Designer Form. This tab is used to select the user groups that can add, modify, and/or remove information from within the custom form when it is instantiated.

Figure 9–6 The Object Permissions Tab of the Form Designer Form



In addition, the Allow Insert, Allow Update, and Allow Delete check boxes are visual indicators of the privileges that a user group has with the form. When the Allow Insert check box is selected, the corresponding user group can add information into the fields

of the user-created form. If this check box is cleared, the user group cannot populate the fields of this form.

Similarly, when the Allow Update check box is selected, the associated user group can modify existing information in the fields of the user-created form. If this check box is cleared, the user group cannot edit the fields of this form.

Lastly, when the Allow Delete check box is selected, the corresponding user group can delete data from instantiations of the user-created form. If this check box is cleared, the user group cannot delete data from fields of this form (when it is instantiated).

For this example, the SYSTEM ADMINISTRATORS user group can create, modify, and delete information that appears in the Results of 1Q 2004 Sales form (represented by the UD_SALES2 name in the Table Name field). The IT DEPARTMENT user group can only delete records of this form (Its Allow Insert and Allow Update check boxes are cleared.). The HR DEPARTMENT user group can create and modify information from within the Results of 1Q 2004 Sales form. However, because the Allow Delete check box is cleared, this user group is not able to delete this information.

Now that we have reviewed the Object Permissions tab, you will learn how to assign a user group to a user-created form, and remove a user group from a user-created form.

Assign a User Group to a User-Created Form

To assign a user group to a user-created form, perform the following steps:

1. Click **Assign**. The Assignment dialog box is displayed.
2. Select the user group, and assign it to the form that was created by a user.
3. Click **OK**. The user group appears in the Object Permissions tab.
4. If you *do not* want this user group to be able to add information into a record of the user-created form, double-click the corresponding Allow Insert check box. Otherwise, proceed to Step 5.
5. If you *do not* want this user group to be able to modify information from within a record of the user-created form, double-click the associated Allow Update check box. Otherwise, proceed to Step 6.
6. If you *do not* want this user group to be able to delete a record of the user-created form, double-click the corresponding Allow Delete check box. Otherwise, proceed to Step 7.
7. Click **Save**. The user group is assigned to the user-created form.

Remove a User Group From a User-Created Form

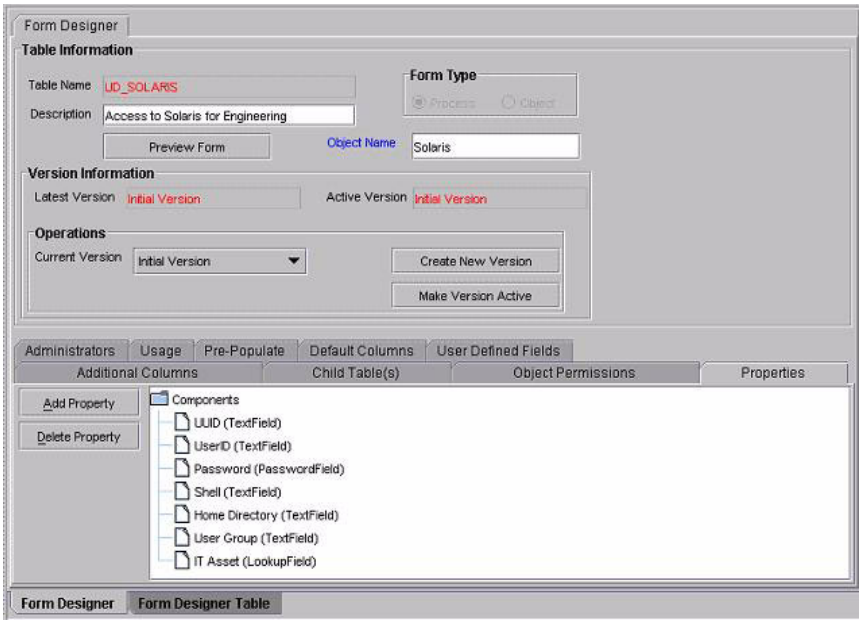
To remove a user group from a user-created form, perform the following steps:

1. Highlight the user group that you want to remove.
2. Click **Delete**. The user group is removed from the user-created form.

Properties

Figure 9–7 displays the Properties Tab of the Form Designer Form. This tab is used to assign properties and property values to the data fields, which appear on the form that is created through the Form Designer form.

Figure 9–7 The Properties Tab of the Form Designer Form



For this example, the Results of 1Q 2004 Sales form are comprised of two data fields: **User Name** and **Password**. Each data field contains the following properties:

- **Required**, which determines whether the data field needs to be populated for the generated form to be saved. The default property value for the Required property is false.
- **Visible Field**, which establishes whether the data field appears on the form, once Oracle Identity Manager generates the form. The default property value for the Visible Field property is true.

Since the property values for the Required and Visible Field properties are true for both data fields, once the Results of 1Q 2004 Sales form is generated, both of these data fields appears. In addition, each field needs to be populated for the form to be saved.

Now that we have reviewed how properties and property values relate to data fields, you will learn how to add a property and property value to a data field. Also, when a property and property value are no longer valid for a data field, you must remove them from the data field.

Note:

The Properties tab will be disabled until you create a data field for the form, using the Additional Columns tab.

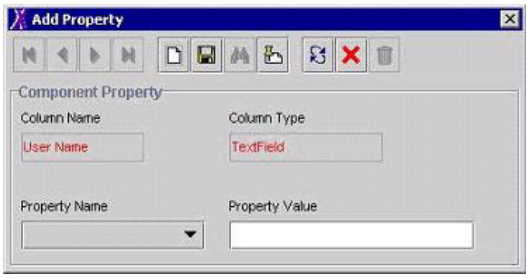
For more information on the properties and property values you can select, refer to "Data Types" on page A-11.

Add a Property and Property Value to a Data Field

To add a property and property value to a Data Field, perform the following steps:

1. Highlight the data field to which you want to add a property and property value.
2. Click **Add Property.** The Add Property dialog box is displayed, as shown in Figure 9–8.

Figure 9–8 The Add Property Dialog Box



Note: The text that appears in the Column Name and Column Type text boxes reflects the name and type of the data field you selected.

In this example, the User Name data field has been selected (as indicated by User Name appearing within the Column Name field). In addition, the data type of this field is a text field.

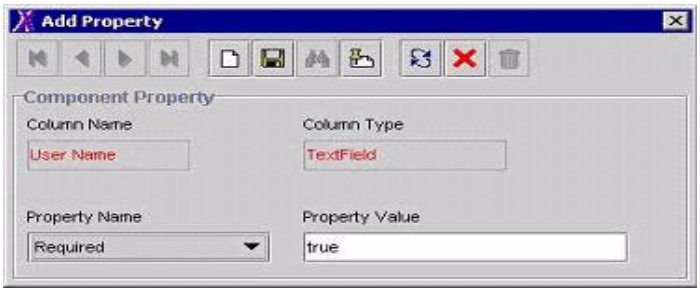
The following table will help you understand the various regions of the Add Property dialog box.

Name	Description
Column Name	The name of the data field.
Column Type	The data type of the data field.
Property Name	From this combo box, select the property for the data field.
Property Value	In this text box, enter the property value, which is associated with the property that appears within the Property Name combo box.

Note: The menu items displayed within the Property Name combo box reflect the data type of the selected data field.

3. Set the parameters for the property and property value that you are adding to the data field. Figure 9–9 displays values filled in the Add Property dialog box.

Figure 9–9 The Add Property Dialog Box - Filled



For this example, since the value of the Required property for the User Name data field has been set to true, once the associated form is generated, this field must be populated. Otherwise, the form cannot be saved.

Note: For more information on which parameters and property values to select, refer to "Data Types" on page A-11.

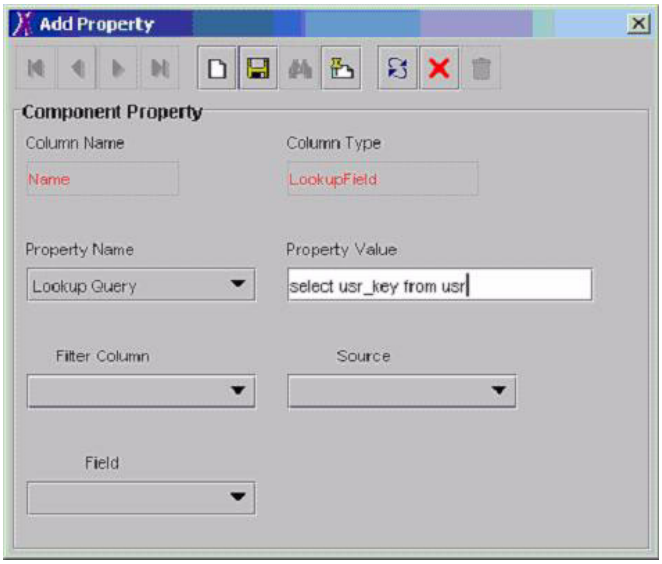
4. From the Add Property window's Toolbar, click Save.
5. Click **Close**. The property and property value are added to the data field.

Add a Property and Property Value for Customized Look Up Query

To add a property and property value for customized lookup query, perform the following steps:

1. Highlight the data field to which you want to add a property and property value.
2. Click **Add Property**. The Add Property dialog box is displayed, as shown in Figure 9–10.

Figure 9–10 The Add Property Dialog Box



Note: The text that appears in the Column Name and Column Type text boxes reflects the name and type of the data field you selected (from the Properties tab of the Form Designer).

In this example, the Name data field has been selected (as indicated by Name appearing within the Column Name field). In addition, the data type of this field is a lookup field.

The combo boxes of the Add Property dialog box are used to help build the "where" clause in the custom lookup query. As you select the values for each box (from the drop-down menu), the where clause (the "WHERE" word is not added automatically) is appended to the custom lookup query.

The following table will help you understand the various regions of the Add Property dialog box. The initial state of all the fields are disabled. Once you have defined the "lookup query" and click **Save**, the fields become active.

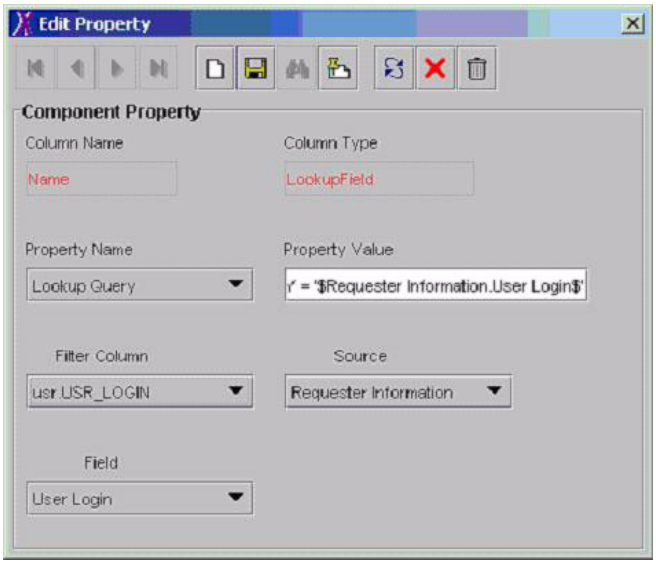
Name	Description
Column Name	The name of the data field.
Column Type	The data type of the data field.
Property Name	From this combo box, select the property for the data field.
Property Value	In this text box, enter the property value, which is associated with the property that appears within the Property Name combo box. In the case of a lookup query, you need to specify both the Oracle Identity Manager form and field, which will be referenced for the query and will be recognized by the database. For example, if Oracle Identity Manager is referring to the user's login, you would enter in the Property Value field, "select usr_key fromusr". After clicking the **Save** button, the Filter Column is active with all the columns of tables.
Filter Column	This is the Oracle Identity Manager form field that is referenced for the lookup query, and which is recognized by the database. This field is populated with all columns of table specified in the Property Value field. If multiple tables are used in the query, then all tables are shown. For example, "usr.USR_LOGIN" signifies that Oracle Identity Manager will refer to User Login field from the Users form for the lookup query.
Source	After the Filter Column variable is selected, the Source field is populated with all possible sources of value. The list of values in this field is dependent upon the type of form, for which the lookup field is being defined. For instance, the list displayed is different if the lookup query is for a Object Form or a Process Form. The Source field is a "user-friendly" name for the value that appears within the Filter Column combo box. For example, Requester Information refers to the usr.USR portion of the Filter Column value.
Field	This field is populated based on what value is selected in the Source field. Use this field in creating the "select" statement, which is needed for the column name. For example, the User Login corresponds to the _LOGIN part in the Filter Column value.

Note: The menu items displayed within the Property Name combo box reflect the data type of the selected data field.

Also, the Source and Field combo boxes of the Add Property dialog box are applicable only when Lookup Query appears within the Property Name.

3. Set the parameters for the property and property value that you are adding to the data field.

Figure 9–11 The Edit Property Dialog Box



Remove a Property and Property Value From a Data Field

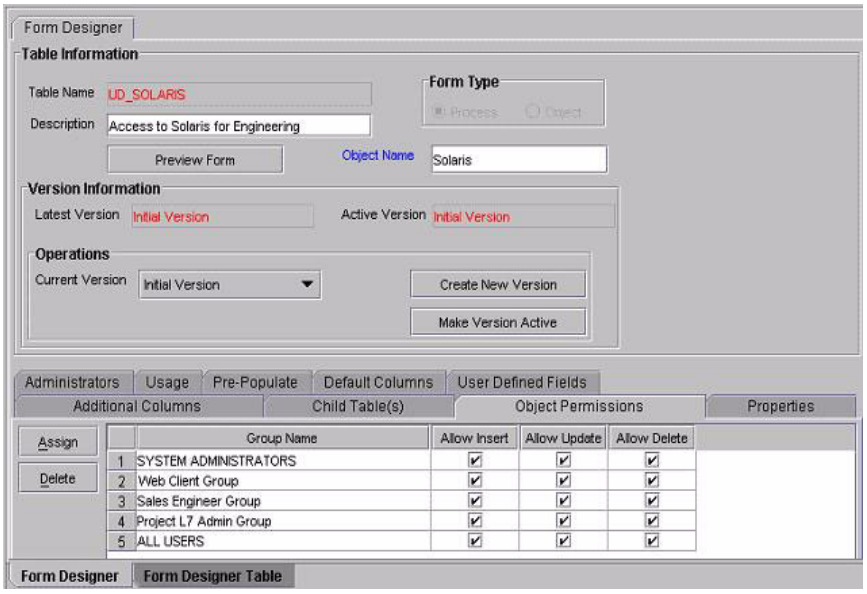
To remove a property and property value from a data field, perform the following steps:

1. Highlight the property and property value that you want to remove.
2. Click **Delete Property**. The property and its associated value are removed from the data field.

Administrators

Figure 9–12 displays the Administrators tab of the Form Designer Form. This tab is used to select the user groups that can view, modify, and delete the current record of the form that was created by a user using the Form Designer form.

Figure 9–12 The Administrators Tab of the Form Designer Form



In addition, the Write and Delete check boxes are visual indicators of the privileges that a user group has with the record. When the Write check box is selected, the corresponding user group can view and modify information for the current record of the form. If this check box is cleared, the user group cannot view or edit information for this record.

Similarly, when the Delete check box is selected, the associated user group can remove information from the current record of the form. If this check box is cleared, the user group cannot delete information from this record.

Now that we have reviewed the Administrators tab, you will learn how to assign administrative privileges to a user group for a record of a user-created form, and remove administrative privileges from a user group for a record of a user-created form.

Assign Administrative Privileges to a User Group for a Record of a User-Created Form

To assign administrative privileges to a user group for a record of a user-created form:

1. Click **Assign**.The Assignment dialog box is displayed.
2. Select the user group, and assign it to the record of the user-created form.
3. Click **OK**. The user group appears in the Administrators tab.
4. If you want this user group to be able to create and/or modify information for the current record of the user-created form, double-click the corresponding Write check box. Otherwise, proceed to Step 5.
5. If you want this user group to be able to remove information from the current record of the user-created form, double-click the associated Delete check box. Otherwise, proceed to Step 6.
6. Click **Save**. The user group now has administrative privileges for this record of the user-created form.

Remove Administrative Privileges from a User Group for a Record of a User-Created Form

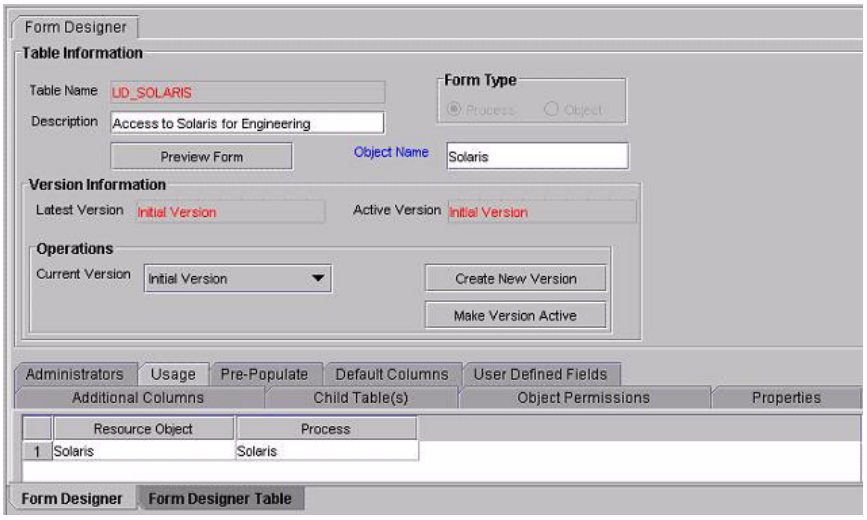
To remove administrative privileges from a user group for a record of a user-created form, perform the following steps:

1. Highlight the user group that you want to remove.
2. Click **Delete**. The user group no longer has administrative privileges for this record of the user-created form.

Usage

Figure 9–13 displays the Usage tab of the Form Designer Form. In this tab, you can see the resource objects and/or processes to which the current form has been assigned.

Figure 9–13 The Usage Tab of the Form Designer Form



For this example, the Solaris form (represented by the UD_SOLARIS name in the Table Name field) has been created and assigned to both the Solaris resource object and provisioning process.

> **Note:** The table name contains the UD_ prefix, followed by the form name. So, for this example, since the name of the form is Solaris, its table name is UD_SOLARIS.
>
> This tab will be populated with information only after you click the **Make Version Active** button, and attach the form to a resource object or provisioning process.

Pre-Populate

This tab is used to:

- Attach a pre-populate adapter to a data field of the user-created form.
- Select the rule that will determine if this adapter will be executed to populate the designated data field with information.
- Set the priority number for the selected rule.
- Map the adapter variables of the pre-populate adapter to their proper locations.

> **Note:** For more information on pre-populate adapters, attaching pre-populate adapters to fields of user-created forms, or mapping the variables of a pre-populate adapter, refer to *Oracle Identity Manager Tools Reference Guide*.

Default Columns

A form, which is created by using the Form Designer form, is comprised of two types of data fields:

- Data fields that are created by a user (using the Additional Columns tab)
- Data fields that are created by Oracle Identity Manager, and added to the form, once the form is created

Through the Default Columns tab, you can see the names, variant types, and lengths of the data fields, which are added, by default, to a user-created form. As a result, by viewing these data fields, you can see all data fields for this type of form, without launching SQL*Plus, or a similar database application.

User Defined Fields

This tab is used to view and access any user-defined fields that have been created for the Form Designer form. Once a user-defined field has been created, it appears on this tab and be able to accept and supply data.

Note: For instructions on how to create fields for user-created forms, refer to "The User Defined Field Definition Form" on page 8-7.

Create an Additional Version of a Form

Sometimes, when you create a form, and populate the tabs of the Form Designer form with information, so the form will work with the process or resource object to which it will be assigned, you may wish to create a different version of the form. This way, you can modify this version, without impacting the original version of the form.

The following procedure will show you how to create an additional version of a form.

1. Open the Form Designer form.
2. Query for the specific form of which you want to create a different version.
3. Click the **Current Version** combo box. From the drop-down menu that appears, select the version of the form of which you are creating an additional version.
4. Click the **Create New Version** button. The Create a New Version window is displayed.
5. In the **Label** field, enter the name of the additional version of the form.
6. From the Create a New Version window's Toolbar, click **Save**.
7. Then, from this Toolbar, click **Close**. The additional version of the form is created. When you click the Current Version combo box, the version's name, which you entered into the Label field in Step 5, appears. By selecting this version, you can populate the tabs of the Form Designer form with information, without impacting the original version of the form.

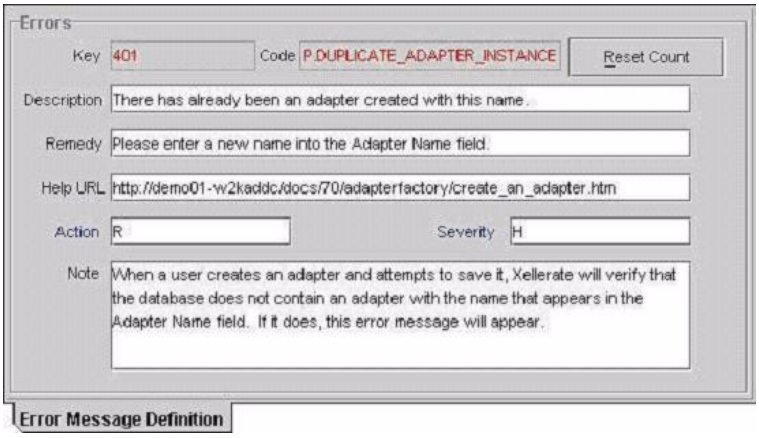
The Error Message Definition Form

The Error Message Definition form, as shown in Figure 9–14, is located in the Development Tools folder. It is used to:

- Create the error messages that appears in dialog boxes when certain problems.
- Define the error messages that users can access when they create error handler tasks using the Adapter Factory form.

Note: For more information on creating error handler tasks, refer to *Oracle Identity Manager Tools Reference Guide*.

Figure 9–14 The Error Message Definition Form



The following table describes the data fields of the Error Message Definition form.

Field Name	Description
Key	The error message definition's unique, system-generated identification number.
Code	The code that represents the error message definition.
Reset Count	When you click this button, Oracle Identity Manager resets the counter to 0 for the number of times this error message appears.
Description	A description of the error message.
Remedy	A description of how to fix the condition that causes the error message to appear.
Help URL	The link to the URL that contains an online Help topic for this error message.
Action	A one-letter code, representing the seriousness of the condition that causes the error message to appear. An error message has three levels of seriousness: Error (E), Rejection (R), and Fatal Rejection (F).
Severity	For classification purposes, you can categorize the seriousness of the condition, which results in the error message being displayed, even further. An error message has six sub-levels of severity: None (N), Low (L), Medium (M), High (H), and Crash (C).
Note	Explanatory information about the error message.

Now that we have reviewed error message definitions and the data fields of the Error Message Definition form, you are ready to create an error message.

Create an Error Message

To create an error message, perform the following steps:

1. Open the Error Messaging Definition form.
2. In the **Code** field, enter a code that represents the error message definition.
3. In the **Description** field, enter a description of the error message.

4. In the **Remedy** field, you can enter a description of how to fix the condition that causes the error message to appear.
5. In the **Help URL** field, you can enter the link to the URL that contains an online Help topic for this error message.
6. *Optional*. Double-click the **Action Lookup** field. From the Lookup dialog box that appears, you can select a code that represents the seriousness of the condition that causes the error message to appear. These codes, listed by degree of seriousness (from lowest to highest), are:
   - Error (E). Oracle Identity Manager stores the error message, and stops any related operations from being triggered. Instead, it rolls back to the previous operation.
   - Reject (R). Oracle Identity Manager stores the rejection message, but does not prevent subsequent operations from being executed.
   - Fatal Reject (F). Oracle Identity Manager stores the rejection message, and stops any subsequent operations from being triggered. However, it keeps all operations that were executed up to the fatal rejection.
7. *Optional*. Double-click the **Severity Lookup** field. From the Lookup dialog box that appears, you can select a code (None (N), Low (L), Medium (M), High (H), or Crash (C)). This code represents a more-detailed classification of the code that appears in the Action lookup field.
8. In the Note field, you can enter explanatory information about the error message.
9. Click **Save**. The error message is created. Oracle Identity Manager will populate the Key field with a unique identification number. Once a condition arises that causes this error message to appear, the text in the Description field appears in a dialog box.

   Tip: If you have created an error message definition, and you want to reset how many times the error message appears; you can do so by clicking the Reset Count button. Once you click this button, the counter will be reset to 0.

10

Business Rule Definition

This chapter describes the Business Rule Definition of Oracle Identity Manager. It contains the following topics:

Overview

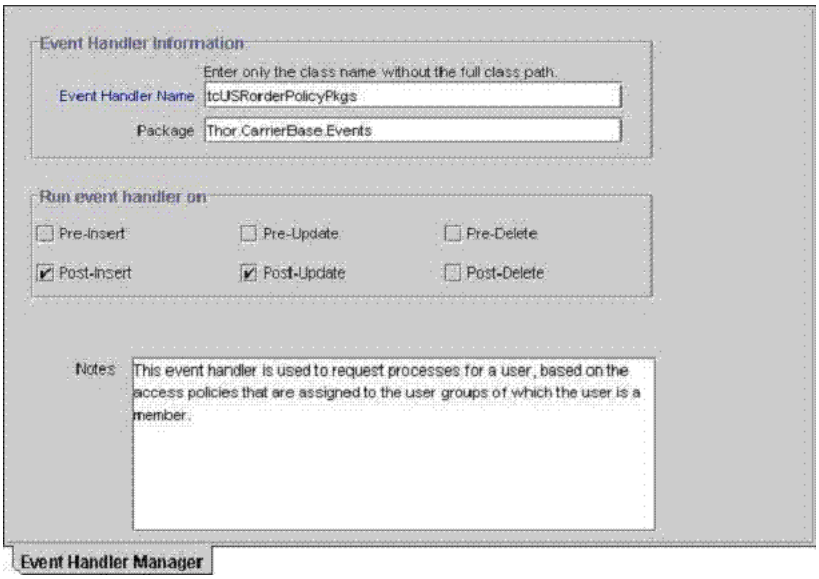
The Development Tools/Business Rule Definition folder provides System Administrators and developers with the tools necessary to manage the event handlers and data objects of Oracle Identity Manager. This folder contains the following forms:

- Event Handler Manager: This form allows you to create and manage the event handlers that are used with Oracle Identity Manager.
- Data Object Manager: This form allows you to define a data object, assign event handlers and adapters to it, and map any adapter variables associated with it.

The Event Handler Manager Form

Figure 10–1 displays the Event Handler Manager form, which is located in the Development Tools/Business Rule Definition folder. It is used to manage the Java classes that process user-defined or system-generated actions (or events). These classes are known as event handlers. When you add a new event handler to Oracle Identity Manager, you must first register it here, so Oracle Identity Manager can recognize it.

Figure 10–1 Event Handler Manager Form



There are two types of event handlers:

- Event handlers that are created through the Adapter Factory form. These event handlers, which begin with the letters "adp," are known as adapters.
- Event handlers that are created internally within Oracle Identity Manager. These event handlers, which begin with the letters "tc," are referred to as system event handlers.

In addition, through the Event Handler Manager form, you can specify when you want Oracle Identity Manager to trigger an event handler. An event handler can be scheduled to run on:

- Pre-Insert: Before information is added to the database
- Pre-Update: Before information is modified within the database
- Pre-Delete: Before information is removed from the database
- Post-Insert: After information is added to the database
- Post-Update: After information is modified within the database
- Post-Delete: After information is removed from the database

> **Important:** To actually use an event handler, you must attach it to a data object (using the Data Object Manager form). For more information on assigning event handlers to data objects, refer to "The Data Object Manager Form" on page 10-4.

You will now learn about the data fields of the Event Handler Manager form. Table 10–1 describes the data fields of this form.

Table 10–1 Data Field

Field Name	Descriptions
Event Handler Name	The name of the event handler.
Package	The Java package to which the event handler belongs.

Table 10–1 (Cont.) Data Field

Field Name	Descriptions
Pre-Insert	By selecting this check box, Oracle Identity Manager can trigger the event handler before information is added to the database.
Pre-Update	If you select this check box, Oracle Identity Manager can trigger the event handler before information is modified within the database.
Pre-Delete	By selecting this check box, Oracle Identity Manager can trigger the event handler before information is removed from the database.
Post-Insert	If you select this check box, Oracle Identity Manager can trigger the event handler once information is added to the database.
Post-Update	By selecting this check box, Oracle Identity Manager can trigger the event handler after information is modified within the database.
Post-Delete	If you select this check box, Oracle Identity Manager can trigger the event handler once information is removed from the database.
Notes	Additional information about the event handler.

Now that we have reviewed event handlers and the data fields of the Event Handler Manager form, you are ready to create and modify event handlers.

Add or Modify an Event Handler

To add or modify an event handler, perform the following steps:

1. Open the Event Handler Manager form.
2. If you are adding an event handler to Oracle Identity Manager, enter the name of the event handler into the **Event Handler Name lookup** field.

   If you are modifying an event handler, double-click the **Event Handler Name lookup** field. From the Lookup dialog box that appears, select the event handler that you wish to edit.

   Caution: Any event handlers that begin with the letters "adp" is associated with adapters, and should not be modified. However, you can modify system event handlers (event handlers that begin with the letters "tc").

3. In the **Package** field, add or edit the name of the Java package of which the event handler is a member.
4. Select or clear the checkboxes that correspond to when you want Oracle Identity Manager to either trigger the event handler or not activate the event handler, respectively. An event handler can be scheduled to run on pre-insert, pre-update, pre-delete, post-insert, post-update, and post-delete.

   Important: Selecting a check box does not mean that the event handler will be triggered at that time (for example, on pre-insert). It signifies that the event handler can run at that time.

In the **Notes** area, you can add or edit explanatory information about the event handler. Click **Save**. The event handler you added or modified will now reflect the settings you have entered.

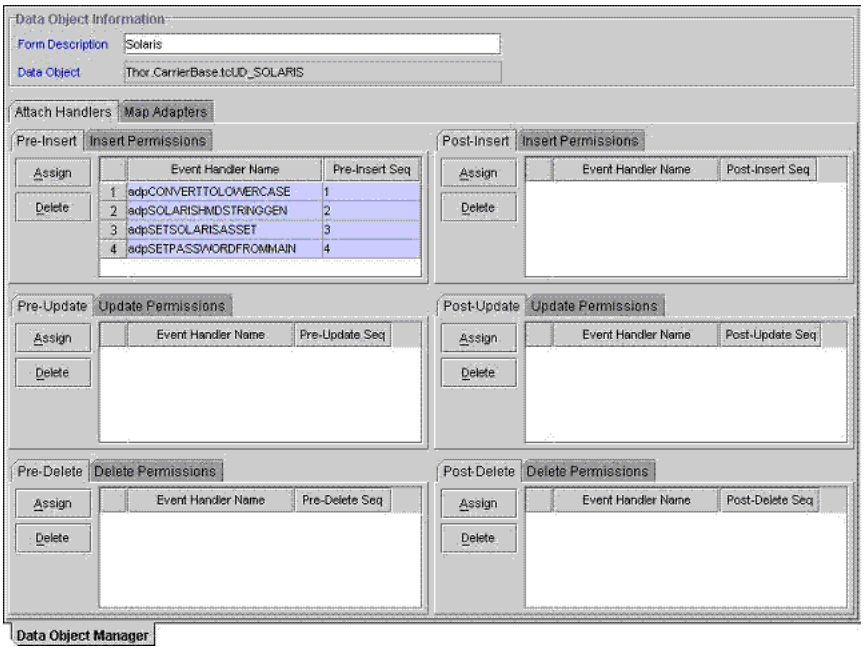
The Data Object Manager Form

Figure 10–2 displays the Data Object Manager form, which is located in the Development Tools/Business Rule Definition folder. It is used to:

- Assign a rule generator adapter, entity adapter, or an event handler to an object, which can add, modify, or delete data to or from the database. This type of object is known as a data object.
- Schedule the adapter or event handler to be executed during a particular execution schedule (pre-insert, pre-update, pre-delete, post-insert, post-update, or post-delete).
- Organize the order in which Oracle Identity Manager will trigger adapters or event handlers that belong to the same execution schedule.
- See the user groups that can add, modify, and delete the current data object.
- Map the variables of an adapter to their proper source and target locations.

Note: For more information on adapter variables, rule generator adapters, and entity adapters, refer to the *Oracle Identity Manager Tools Reference Guide*.

Figure 10–2 Data Object Manager Form



You will now learn about the data fields of the Data Object Manager form. Table 10–2 describes the data fields of this form.

Table 10–2 Data Field

Field	Description
Form Description	The name of the form, which is associated with the data object.
Data Object	The name of the data object, to which you are assigning event handlers rule generator adapters, or entity adapters.

Now that we have reviewed data objects and the data fields of the Data Object Manager form, you are ready to select the target data object to which a rule generator adapter, entity adapter, or event handler will be assigned.

Select a Target Data Object

To select a target data object, perform the following steps:

1. Open the Data Object Manager form.
2. Double-click the **Form Description** field. From the Lookup dialog box that appears, select the name of the form that is associated with the data object to which you want to assign an event handler, rule generator adapter, or entity adapter.

   Once you select a form, the name of the corresponding data object appears in the **Data Object** field.
3. Click **Save**. The target data object is selected. You can now assign rule generator adapters, entity adapters, and event handlers to it.

Tabs of the Data Object Manager Form

Once you launch the Data Object Manager form, and select a target data object, the tabs of this form become functional.

The Data Object Manager form contains the following tabs:

- Attach Handlers
- Map Adapters

Each of these tabs is covered in greater detail in the following sections.

> **Note:** The Map Adapters tab will become operational only after you assign a rule generator adapter or entity adapter to the data object.

Attach Handlers

This tab is used to select the rule generator adapters, entity adapters, or event handlers that will be assigned to or removed from a data object. This includes:

- Specifying when Oracle Identity Manager will trigger the assigned event handlers or adapters (on pre-insert, pre-update, pre-delete, post-insert, post-update, or post-delete).
- Setting the order that Oracle Identity Manager will trigger the adapters or event handlers that belong to the same execution schedule.

When an event handler, rule generator adapter, or entity adapter no longer needs to be triggered by Oracle Identity Manager, you must remove it from the data object.

For this example, Oracle Identity Manager will trigger the `adpCONVERTTOLOWERCASE`, `adpSOLARISHMDSTRINGGEN`, `adpSETSOLARISASSET`,

and adpSETPASSWORDFROMMAIN adapters on pre-insert. Based on the sequence numbers of these adapters, Oracle Identity Manager will trigger the adpCONVERTTOLOWERCASE adapter first, followed by the adpSOLARISHMDSTRINGGEN, adpSETSOLARISASSET, and adpSETPASSWORDFROMMAIN adapters, respectively.

> **Note:** To see the user groups that can add, modify, and delete the current data object, click the **Insert Permissions**, **Update Permissions**, or **Delete Permissions** tabs, respectively.

The following procedures will demonstrate how to:

- Assign an event handler, rule generator adapter, or entity adapter to a data object.
- Organize the execution schedule of event handlers or adapters.
- Remove an event handler, rule generator adapter, or entity adapter from a data object.

Assign an Event Handler or Adapter to a Data Object

1. Select the tab of the Data Object Manager form that represents when you want the adapter or event handler to be triggered. For example, if you want Oracle Identity Manager to activate an adapter on pre-insert, select the **Pre-Inser**t tab.
2. From the selected tab, click **Assign**. The Assignment dialog box is displayed.
3. Select the event handler or adapter, and assign it to the data object.
4. Click **OK**. The event handler or adapter is assigned to the data object.

Organize the Execution Schedule of Event Handlers or Adapters

1. Highlight the event handler or adapter whose execution schedule you wish to change.
2. Click **Assign**. The Assignment dialog box is displayed.
3. Highlight the event handler or adapter..
4. Click **Up**. The selected event handler or adapter will switch places (and sequence numbers) with the event handler or adapter that precedes it.
5. Or, Click **Down**. The highlighted event handler or adapter will trade places (and sequence numbers) with the event handler or adapter that that follows it.
6. Repeat Steps 3-5 until all event handlers and/or adapters have the appropriate sequence numbers.
7. Click **OK**. The event handlers or adapters will now be triggered in the proper order for the execution schedule(s) you organized.

Remove an Event Handler or Adapter From a Data Object

1. Highlight the desired event handler or adapter.
2. Click **Delete**. The event handler or adapter is removed.

Map Adapters

This tab is used to map the variables of a rule generator or entity adapter to their proper source and target locations. For this example, the

adpSOLARISUSERIDGENERATOR adapter has three variables: firstname, Adapter return value, and lastname. Since a "Y" appears in the Mapped column for each adapter variable, this signifies that all three variables have been mapped to the correct locations, and the adapter's status will change to Ready.

Note: An adapter can have one of three statuses:

- Ready. This adapter has been successfully compiled and all of its variables have been mapped correctly.
- Mapping Incomplete. This adapter has been successfully compiled, but at least one of its variables has been not mapped correctly.
- Mapping Incomplete. This adapter has been successfully compiled, but at least one of its variables has been not mapped correctly.

For more information on compiling adapters and/or mapping its variables, refer to the *Oracle Identity Manager Tools Reference Guide*.

Note: If no adapters are assigned to a data object, the Map Adapters tab will be disabled.

The Reconciliation Rules Form

This form is located in the Development Tools folder. It is used to define the rules that are invoked:

- When Oracle Identity Manager is attempting to determine which user (or organization) record is associated with a change on a trusted source. These rules will be evaluated as soon as all required fields within the reconciliation event have been processed on the Reconciliation Data tab (of the Reconciliation Manager form).
- When Oracle Identity Manager is attempting to determine which user (or organization) record is the owner of an account discovered on a target resource (for example, as a result of a change detected on that system). These rules will be evaluated only when all required fields within the reconciliation event have been processed on the Reconciliation Data tab (of the Reconciliation Manager form) and no processes have been matched to the event on the Processes Matched Tree tab (of the same form).

As mentioned, rules defined using this form is used to match either users or organizations associated with a change on a trusted source or target resource. Rules of these types are referred to as user matching or organization matching rules, respectively. These rules are very similar to the ones you can define using the Rule Designer form except that the rules created using the Reconciliation Rules form are resource object-specific (since they relate to a single target resource) and only affect reconciliation-related functions.

Define a Reconciliation Rule

To define reconciliation rules for user or organization matching, perform the following steps:

1. Access the Reconciliation Rules form.
2. Enter a name for the rule in the **Name** field.
3. Select the target resource with which this rule is to be associated in the **Object** field
4. Enter a description for the rule in the **Description** field.

   Select the **And** or **Or** Operator for the rule. If **And** is selected, then all elements (and rules if they have been nested) of the rule must be satisfied for the rule to be evaluated to true. If **Or** is selected, then the rule will be evaluated to true if any element (or rule if one has been nested) of the rule is satisfied.
5. Click **Save**. The rule definition will be saved. Rule elements must now be created for the rule.

Note: You must ensure that the **Active** checkbox is selected. If this checkbox is not selected, the rule will not be evaluated by Oracle Identity Manager's reconciliation engine when processing reconciliation events related to the resource. However, this checkbox can only be set once Oracle Identity Manager has selected the **Valid** system checkbox. The **Valid** checkbox will only be selected once you have created at least one rule element and Oracle Identity Manager has determined that the logic of this rule element is valid.

Add a Rule Element

To define individual elements within a reconciliation rule, perform the following steps:

1. Access the Rule definition to which you wish to add elements.
2. Click **Add Rule Element** on the Rule Elements tab. The Add Rule Element dialog box is displayed.
3. Click the **Rule Element** tab.
4. Select a user-related data item from the **User Data** menu. This will be the user data element that Oracle Identity Manager will examine when evaluating the rule element. The menu will display all fields on the Oracle Users form (including any user-defined fields you may have created).

Note: If the rule being defined is for organization matching, then both the data available and the name of the menus will be related to organizations rather than users.

---

5. Select an Operator from the **Operator** menu. This will be the criteria that Oracle Identity Manager applies to the attribute for data item you selected when evaluating the rule element. Valid operators are:

- Equals. If you select this option, then the (user or organization record's) data element must exactly match the attribute you select.
- Contains. If you select this option, then the (user or organization record's) data element must only contain (not be an exact match with) the attribute you select.
- Start with. If you select this option, then the (user or organization record's) data element must begin with the attribute you select.
- End with. If you select this option, then the (user or organization record's) data element must end with the attribute you select.

Select a value from the **Attribute** menu. The values displayed in this menu are the fields that have been defined on the Reconciliation Fields tab for the resource associated with the rule. If the reconciliation fields have not yet been designated for the resource, then no values will be available.

Note: When defining a rule element for a target resource (as opposed to a trusted source), only those fields associated with parent tables of the resource's custom process form will be available for selection in the **Attribute** field.

6. If you want Oracle Identity Manager to perform a particular transformation on the data in the Attribute field (before applying the operator), select the desired transformation from the Transform menu.

Note: If you select a value (other than None) from this menu, once you click **Save**, you must also select the tab and set the appropriate properties so that Oracle Identity Manager is able to properly perform the transformation.

The possible transformations are described in Table 10–3.

Table 10–3 Transformation Properties

Transformation	Properties to be set on the Rule Element Properties tab
Substring	Start Point, End Point
Endstring	Start Point
Tokenize	Delimiters, Token Number, Space Delimiter

7. Set the Case-Sensitive check box. If this check box is selected, the value selected in the Attribute field must exactly match the capitalization used in the value being evaluated in the reconciliation event record in order for the rule element to be satisfied. If this check box is cleared, then the value selected in the Attribute field is not required to match the capitalization used in the value being evaluated in the reconciliation event record.
8. Click **Save**.
9. If you select a value (other than None) in the **Transform** menu and have not yet set the properties for the transformation, the Properties Set check box will be clear. You must then select the **Rule Element Properties** tab, set the appropriate properties and click **Save** again.

   The rule element will be added to the rule.
10. Repeat this entire procedure for each rule element you wish to add to the rule.

Note: Ensure that the Active checkbox is selected.

Nest a Rule Within a Rule

You can nest an existing rule within a rule. Oracle Identity Manager will evaluate the criteria of the nested rule in the same manner as any other element of the rule. To nest a rule within a rule, perform the following steps:

1. Access the rule to which you wish to add another rule.
2. Click **Add Rule** on the Rule Elements tab.
3. The Rule Choice lookup dialog box is displayed. Locate and select the desired rule.

   Note: Only reconciliation-related rules that are associated with the same resource object will be available for selection within the dialog box.

4. Click **OK**. The selected reconciliation rule will be added to rule.
5. Repeat steps 2-4 for each rule you wish to nest within the rule.

Delete a Rule Element or Rule

To delete a rule element or a rule, perform the following steps:

1. Access the rule from which you wish to delete an element.
2. Select the rule element or rule to be deleted on the Rule Elements tab.
3. Click **Delete**.

11

Oracle Identity Manager Logging Functions

This chapter describes the Oracle Identity Manager logging functions. It contains the following topics:

Overview

Oracle Identity Manager comes pre-installed with the ability to create log files related to the various activities being performed within the application. The level of information that will be placed in these log files, the location where these log files will be created, the frequency with which these information in these files will be archived can all be customized using the relevant configuration files. In addition, Oracle Identity Manager also provides logs files that contain standard error and standard out messages.

The logs files created by Oracle Identity Manager can be used to track activities being performed in the various modules (for example, adapter factory, task scheduler) of the application and/or monitor error messages and queries performed against the database. Both of these activities can be very helpful when troubleshooting potential problems or testing anticipated application behavior. As mentioned, Oracle Identity Manager allows you to control:

- The level of information (i.e., greater or lesser amount of detail) that will be written to the logs.
- Whether the logs are to be periodically archived and, if so, whether they should be archived based on a user-specified time range or maximum file size.
- The location in which the log file will be placed.

By default there are six log files that will be created by Oracle Identity Manager when the application is running. Three of these log files are controlled using a dedicated `.cfg` file.

The location of log file and its properties will be controlled by the properties file, which is located at `xlclient_home\config\log.properties`.

Setting the Logging Level, Location and Archiving Frequency

The table below explains how to set certain general behavior for the log files controlled using the `.cfg` files.

To Control	Action
The level of information (i.e., greater or lesser amount of detail) that will be written to the logs	Set the level of all the Logger.Module.<module_name> entries to the desired logging level. For example, set the Logger.Module.ServerManager entry to ERROR.
Whether the logs are to be periodically archived and, if so, whether they should be archived based on a user-specified time range or maximum file size	To specify that the log file is never to be archived, set the Logger.LogFile.RollingType entry to NONE. To specify that the log file is to be archived based on time and/or date range, set the Logger.LogFile.RollingType entry to FREQUENCY. Then be sure to set the Logger.LogFile.DatePattern to one of the following: ▪ yyyy-MM: Rollover archiving at the beginning of each month ▪ yyyy-ww: Rollover archiving at the first day of each week. ww is week in year ▪ yyyy-MM-dd: Rollover archiving at midnight each day ▪ yyyy-MM-dd-a: Rollover archiving at midnight and midday each day ▪ yyyy-MM-dd-HH: Rollover archiving at the top of every hour ▪ yyyy-MM-dd-HH-mm: Rollover archiving at the beginning of every minute The default setting of the Logger.LogFile.DatePattern parameter is yyyy-MM-dd (i.e., archive at midnight each day). Each archival log file will have a date (and if applicable time) value appended to its name. For example, using the default setting, the archives logs from January 2, 2004 and January 3, 2004 would be named <logfilename>.log.2004-01-01, <logfilename>.log.2004-01-02, etc. at 12 AM of each day respectively. **Note**: Do not employ the: (colon) symbol anywhere in the data pattern. To specify that the log file is to be archived based on size of the log file, set the Logger.LogFile.RollingType entry to SIZE. Then be sure to set: The Logger.LogFile.MaxFileSize entry to the file size that you wish to cause log file archiving. Once the log file reaches that size, its contents will be rolled over to an archival file and any new logs will be written to the original file. Oracle Identity Manager will continue to create additional archival files until it reaches the number of log files set in Logger.LogFile.MaxBackupIndex entry described below. The log4j.appender.logFile.MaxBackupIndex entry to the maximum number of archival log files you wish to allow Oracle Identity Manager to create. For example, if you set this entry to 5, Oracle Identity Manager will create a maximum of 5 incremental archival log files (not including the actual, non-archival log file). After the fifth archival log is created, additional log archiving will cause the contents of the oldest archival log file to be deleted and replaced with the contents of the next oldest.
The location in which the log file will be placed	To specify the location in which the log file is created, set the Logger.LogFile.FilePath entry to the desired location. For example, to specify that the ServerManager.log file to be created in C:\oracle\xellerate\logs set this entry to ./logs/ServerManager.log (since ./ specifies the location of \oracle\xellerate). Be sure to specify the log file name as well.

A

Reference

This appendix describes the various tables in Oracle Identity Manager.

Tables

The following tables list and describe:

- The parameters you can select when adding or modifying a rule element for a rule
- The parameters and variables to set when you are creating or editing an e-mail definition
- The data types that can be used to create Oracle Identity Manager forms
- The system properties you can set for Oracle Identity Manager
- The lookup types that are used with Oracle Identity Manager

Rule Elements

The following table lists the rule elements that can be used to create Oracle Identity Manager rules, using the **Rule Designer** form.

Type	Sub-Type	Attribute Source	
General	**N/A**	User Profile Data	Email
			End Date
			First Name
			Identity
			Last Name
			Manager Full Name
			Manager Login
			Middle Name
			Organization Name
			Role
			Start Date

Type	Sub-Type	Attribute Source	
General	N/A	User Profile Data	Status
			User Group Name
			User Login
			Oracle Identity Manager Type
			Email
			Any fields that appear in the **User Defined Fields** region of the **User Profile** tab of the **Users** form.
Process Determination	**Organization Provisioning**	Requester Information	Email
			End Date
			First Name
			Identity
			Last Name
			Location Name
			Manager Full Name
			Manager Login
			Middle Name
			Organization Name
			Role
			Start Date
			State
			Status
			User Group Name
			User Login
			Oracle Identity Manager Type
			Any fields that appear in the **User Defined Fields** region of the **User Profile** tab of the **Users** form.

Type	Sub-Type	Attribute Source	
Process Determination	**Organization Provisioning**	Object Information	Object Name
			Object Type
		Request Target Information	Organization Customer Type
			Organization Name
			Organization Status
			Parent Organization
			Any fields that appear in the **User Defined Fields** tab of the **Organizations** form.
		Object Data Information	Any fields that appear in the Additional Columns tab of the Form Designer form for the custom form associated with the resource object.
		Process Data Information	Any fields that appear in the **Additional Columns** tab of the **Form Designer** form for the custom form associated with the process.
	User Provisioning	Requester Information;	Additional Address Info
			Email
		Request Target Information	End Date
			First Name
			Identity
			Last Name
			Manager Full Name
			Manager Login
			Middle Name
			Organization Name
			Role
			Start Date
			Status
			User Group Name
			User Login
			Oracle Identity Manager Type

Type	Sub-Type	Attribute Source	
Process Determination	**User Provisioning**	Requester Information; Request Target Information	Any fields that appear in the **User Defined Fields** region of the **User Profile** tab of the **Users** form.
		Object Information	Object Name
			Object Type
		Object Data Information	Any fields that appear in the **Additional Columns** tab of the **Form Designer** form for the custom form associated with the resource object.
		Process Data Information	Any fields that appear in the **Additional Columns** tab of the **Form Designer** form for the custom form associated with the process.
	Approval; Standard Approval	Requester Information	Email
			End Date
			First Name
			Identity
			Last Name
			Manager Full Name
			Manager Login
			Middle Name
			Organization Name
			Role
			Start Date
			Status
			User Group Name
			User Login
			Oracle Identity Manager Type
			Any fields that appear in the **User Defined** Fields region of the **User Profile** tab of the **Users** form.
		RequestInformation	Request Creation Date
			Request ID
			Request Object Action
			Request Priority
			Requestor

Type	Sub-Type	Attribute Source	
Process Determination	**Approval**	Object Information	Object Name
			Object Type
		Object Data Information	Any fields that appear in the **Additional Columns** tab of the **Form Designer** form for the custom form associated with the resource object.
		Process Data Information	Any fields that appear in the **Additional Columns** tab of the **Form Designer** form for the custom form associated with the process.
Task Assignment	**Organization Provisioning; User Provisioning**	Task Information	Allow Cancellation while Pending
			Allow Multiple Instances
			Assign Task to Manager
			Disable Manual Insert
			Task Conditional
			Task Data Label
			Task Default Assignee
			Task Name
			Task Required for Completion
			Task Sequence
		Process Information	Object Name
			Process Name
			Process Type
		Object Information	Object Name
			Object Type
		Requester Information	Email
			End Date
			First Name
			Identity

Type	Sub-Type	Attribute Source	
Task Assignment	**Organization Provisioning; User Provisioning**	Requester Information	Last Name
			Manager Full Name
			Manager Login
			Middle Name
			Organization Name
			Role
			Start Date
			State
			Status
			User Group Name
			User Login
			Oracle Identity Manager Type
			Any fields that appear in the **User Defined Fields** region of the **User Profile** tab of the **Users** form.
		Object Data Information	Any fields that appear in the **Additional Columns** tab of the **Form Designer** form for the custom form associated with the resource object.
		Process Data Information	Any fields that appear in the **Additional Columns** tab of the **Form Designer** form for the custom form associated with the process.
Pre-Populate	**OrganizationProvisioning; User Provisioning**	Requester Information	Email
			End Date
			First Name
			Identity
			Last Name
			Manager Full Name
			Manager Login
			Middle Name
			Organization Name

Type	Sub-Type	Attribute Source	
Pre-Populate	**Organization Provisioning;User Provisioning**	Requester Information	Role
			Start Date
			Status
			User Group Name
			User Login
			Email
			Any fields that appear in the **User Defined** Fields region of the **User Profile** tab of the **Users** form.
		Request Information	Request Creation Date
			Request ID
			Request Object Action
			Request Priority
			Requestor
		Object Information	Object Name
			Object Type
		Object Data Information	Any fields that appear in the Additional Columns tab of the Form Designer form for the custom form associated with the resource object.
		Process Data Information	Any fields that appear in the Additional Columns tab of the Form Designer form for the custom form associated with the process.
	Organization Provisioning	Request Target Information	Organization Customer Type
			Organization Name
			Organization Status
			Parent Organization
			Any fields that appear in the **User Defined Fields** tab of the **Organizations** form.
	User Provisioning	Request Target Information	Email
			End Date
			First Name
			Identity
			Last Name
			Manager Full Name
			Manager Login

Type	Sub-Type	Attribute Source	
Pre-Populate	**User Provisioning**	Request Target Information	Middle Name
			Organization Name
			Province
			Region
			Role
			Start Date
			Status
			User Group Name
			User Login
			Oracle Identity Manager Type
			Email
			Any fields that appear in the **User Defined Fields** region of the **User Profile** tab of the **Users** form.

E-Mail Variables

The following table lists the variables that can be used to create e-mail templates, using the Email Definition form.

Type	Target	Location Type	Contact Type	Variable
Provisioning Related	User Profile Information; Assignee Profile Information	N/A	N/A	First Name
				Identity
				Last Name
				Manager Login
				Middle Name
				Role
				Status
				User End Date
				User Group Name
				User Login
				User Manager
				User Start Date
				Oracle Identity Manager Type
Provisioning Related	User Profile Information; Assignee Profile Information	N/A	N/A	Any fields that appear in the **User Defined Fields** region of the **User Profile** tab of the **Users** form.

Type	Target	Location Type	Contact Type	Variable
	Object Information	N/A	N/A	Object Name
				Object Target Type
				Object Type
	Process Information	N/A	N/A	Object Name
				Process Name
				Process Type
	Object Data Information	N/A	N/A	Any fields that appear in the **Additional Columns** tab of the **Form Designer** form for the custom form associated with the resource object.
	Process Data Information	N/A	N/A	Any fields that appear in the **Additional Columns** tab of the **Form Designer** form for the custom form associated with the process.
Request Related	Requester Information	N/A	N/A	First Name
				Identity
				Email Address
				Manager Login
				Middle Name
				Role
				Status
				User End Date
				User Group Name
				User Login
				User Manager
				User Start Date
				Oracle Identity Manager Type
				Any fields that appear in the **User Defined Fields** region of the **User Profile** tab of the **Users** form.
Request Related	Request Information	N/A	N/A	First Name
				Identity

Type	Target	Location Type	Contact Type	Variable
				Last Name
				Email Address
				Manager Login
				Role
				Status
				User End Date
				User Group Name
				User Login
				User Manager
				User Start Date
				Oracle Identity Manager Type
				Any fields that appear in the **User Defined Fields** region of the **User Profile** tab of the **Users** form.
Request Related	Request Information	N/A	N/A	List of objects being requested
				List of targets being provisioned
				Request Creation Date
				Request ID
				Request Name
				Request Object Action
				Request Priority
				Requestor
				Number
General	User Profile Information	N/A	N/A	First Name
				Identity
				Last Name
				Email Address
				Manager Login
				Middle Name
				Role
				Status
				User End Date
				User Group Name

Type	Target	Location Type	Contact Type	Variable
				User Login
				User Manager
				User Start Date
				Oracle Identity Manager Type
				Any fields that appear in the **User Defined Fields** region of the **User Profile** tab of the **Users** form.

Data Types

The following table lists and describes the data types that can be used to create Oracle Identity Manager forms, using the Form Designer form.

> **Note:** If any data field has a variant type of Long, Short, Double, or Integer, two additional selections appears when the Property Name combo box is selected: Minimum Numeric Value and Maximum Numeric Value. These items allow you to set the numeric range for the data field.

For example, if a data field has a variant type of **Integer**, the **Minimum Numeric Value** is set to 10, and the Maximum Numeric Value is set to *15*, the only valid entries that can appear in the data field are *10*, *11*, *12*, *13*, *14*, and *15*.

Data Type	Data Property	Description
Text Field	Required	If this text field must be populated for the form to be saved, enter "*true*" into the corresponding **Property Value** text box. Otherwise, type "false" into this text box. **Note**: The default value for this data property is *false*.
	Is Visible	If you want this text field to appear when Oracle Identity Manager generates the form, enter "*true*" into the corresponding **Property Value** text box. Otherwise, type "*false*" into this text box. **Note**: The default value for this data property is *true*.

Data Type	Data Property	Description
Lookup Field	Auto Complete	By entering "*true*" in the corresponding **Property Value** text box, Oracle Identity Manager filters the Lookup field. An user can then add characters to the Lookup field before double-clicking it. By doing so, only those Lookup values which match these characters appears within the Lookup window. As an example, for a **State** lookup field, a user can enter "*new*" into the field. Then, once the user double-clicks the Lookup field, only those states that begins with the letters "*new*" (for example, New Hampshire, New Jersey, New Mexico, and New York) appears within the Lookup window.If you do not want Oracle Identity Manager to filter the Lookup field, enter "false" into the associated **Property Value** text box. .The default property value for the **Auto Complete** property is false.
	Column Captions	In the corresponding **Property Value** text box, enter the name of the column heading that appears in the Lookup window when an user double-clicks the Lookup field. If the Lookup window has multiple columns, enter each column heading into the **Property Value** text box, separating them with commas (for example, *Organization Name*, *Organization Status*).

Data Type	Data Property	Description
Lookup Field	Column Names	In the corresponding **Property Value** text box, enter the name of the database column that represents the column caption that you want to appear within the Lookup window. If the Lookup window has multiple columns, enter each database column into the **Property Value** text box, separating them with commas.
	Column Widths	In the corresponding **Property Value** text box, enter the width of the column that appears in the Lookup window. If the Lookup window has multiple columns, enter each column width into the **Property Value** text box, separating them with commas (for example, *20*,*20*).
	Lookup Column Name	In the corresponding **Property Value** text box, enter the name of the Lookup column (as it appears in the database), which contains the entries that need to appear under a column heading of the Lookup window. If the Lookup window has multiple columns, enter each database column into the Property Value text box, separating them with commas (for example, *org_name*,*org_status*.
	Lookup Query	In the corresponding **Property Value** text box, enter the name of the SQL query that executes when an user double-clicks the Lookup field. As a result, the appropriate Lookup column(s) appears within the Lookup window.
	Lookup Code	In the corresponding **Property Value** text box, enter the lookup definition code. This code contains all information pertaining to the lookup field, including lookup values and the text that appears with the lookup field once a lookup value is selected. **Important**: The Lookup Code data property can be used in lieu of the **Column Captions**, **Column Names**, **Column Widths**, **Lookup Column Name**, and **Lookup Query** properties. In addition, the information contained within the Lookup Code property supersedes any values set within these five data properties. **Tip**: An easy way to enter a lookup code is by launching the Lookup Definition form, querying for the desired code, copying this code to the Clipboard, and pasting it into the Lookup Code field. **Note**: The classification type of the lookup definition code must be of Lookup Type (the Lookup Type radio button on the Lookup Definition form needs to be selected).
	Required	If this **Lookup** field must be populated for the form to be saved, enter "*true*" into the corresponding **Property Value** text box. Otherwise, type "false" into this text box. **Note**: The default value for this data property is *false*.

Data Type	Data Property	Description
Lookup Field	Visible Field	If you want this Lookup field to appear when Oracle Identity Manager generates the form, enter "*true*" into the corresponding Property Value text box. Otherwise, type "*false*" into this text box. **Note**: The default value for this data property is *true*.
Text Area	Number of Rows	Within the corresponding **Property Value** text box, enter the row length of the text area. So, if you want the text area to be five rows in length, type "5" into the **Property Value** text box.
	Required	If this text area must be populated for the form to be saved, enter "*true*" into the corresponding **Property Value** text box. Otherwise, type "*false*" into this text box. **Note**: The default value for this data property is *false*.
	Visible Field	If you want this text area to appear when Oracle Identity Manager generates the form, enter "*true*" into the corresponding Property Value text box. Otherwise, type "*false*" into this text box. **Note**: The default value for this data property is *true*.
IT Resource Lookup Field	Type	If you select this data property, a combo box appears in the **Property Value** text box. From this combo box, select the type of Server for the IT Resource. **Important**: This property is required.
	Required	If this Lookup field must be populated for the form to be saved, enter "true" into the corresponding **Property Value** text box. Otherwise, type "false" into this text box. **Note**: The default value for this data property is *false*.
	Visible Field	If you want this Lookup field to appear when Oracle Identity Manager generates the form, enter "*true*" into the corresponding **Property Value** text box. Otherwise, type "*false*" into this text box. **Note**: The default value for this data property is *true*.
Date Field (Display Only)	Visible Field	If you want this text field to appear when Oracle Identity Manager generates the form, enter "*true*" into the corresponding Property Value text box. Otherwise, type "*false*" into this text box. **Note**: The default value for this data property is *true*.
Check Box(Display Only)	Visible Field	If you want this check box to appear when Oracle Identity Manager generates the form, enter "*true*" into the corresponding **Property Value** text box. Otherwise, type "*false*" into this text box. **Note**: The default value for this data property is *true*.

Data Type	Data Property	Description
Text Area(Display Only)	Number of Rows	Within the corresponding **Property Value** text box, enter the row length of the text area. So, if you want the text area to be five rows in length, type "*5*" into the **Property Value** text box.
	Visible Field	If you want this text area to appear when Oracle Identity Manager generates the form, enter "*true*" into the corresponding **Property Value** text box. Otherwise, type "*false*" into this text box. **Note**: The default value for this data property is *true*.
Date and Time Window	Required	If this text field must be populated for the form to be saved, enter "*true*" into the corresponding **Property Value** text box. Otherwise, type "*false*" into this text box. **Note**: To populate this text field, double-click it, and select a date and time from the Date & Time window that appears. **Note**: The default value for this data property is *false*.
	Visible Field	If you want this text field to appear when Oracle Identity Manager generates the form, enter "*true*" into the corresponding **Property Value** text box. Otherwise, type "*false*" into this text box. **Note**: The default value for this data property is *true*.
Password Field	Required	If this text field must be populated for the form to be saved, enter "*true*" into the corresponding **Property Value** text box. Otherwise, type "*false*" into this text box. **Note**: The default value for this data property is *false*.
	Visible Field	If you want this text field to appear when Oracle Identity Manager generates the form, enter "*true*" into the corresponding **Property Value** text box. Otherwise, type "*false*" into this text box. **Note**: The default value for this data property is *true*.
Radio Button	Button Labels	In the corresponding **Property Value** text box, enter the label for the radio button. For multiple radio buttons, this label represents the heading for the group box, containing the radio buttons. When you are applying a label to multiple radio buttons, enter each label into the **Property Value** text box, separating them with commas (for example, *Sun*, *Microsoft*). Once Oracle Identity Manager generates the form, a group box encompasses these radio buttons, signifying that the buttons are associated with one another.
	Button Values	In the corresponding **Property Value** text box, enter the value for the radio button. This value goes to the database when a user selects the radio button. For multiple radio buttons, enter each value into the Property Value text box, separating them with commas (for example, *on*, *off*).

Data Type	Data Property	Description
Radio Button	Required	If a radio button must be selected for the form to be saved, enter "*true*" into the corresponding **Property Value** text box. Otherwise, type "*false*" into this text box. **Note**: The default value for this data property is *false*.
	Visible Field	If you want this radio button (or group of radio buttons) to appear when Oracle Identity Manager generates the form, enter "*true*" into the corresponding **Property Value** text box. Otherwise, type "*false*" into this text box. **Note**: The default value for this data property is *true*.
Check Box	Required	If this check box must be selected for the form to be saved, enter "*true*" into the corresponding **Property Value** text box. Otherwise, type "*false*" into this text box. **Note**: The default value for this data property is *false*.
	Visible Field	If you want this check box to appear when Oracle Identity Manager generates the form, enter "*true*" into the corresponding **Property Value** text box. Otherwise, type "*false*" into this text box. **Note**: The default value for this data property is *true*.
Combo Box	Lookup Code	In the corresponding **Property Value** text box, enter the Lookup definition code. This code contains all information pertaining to the combo box, including combo box items and the text that appears with the combo box once a lookup value is selected. **Important**: The **Lookup Code** data property can be used in lieu of the **Column Captions**, **Column Names**, **Column Widths**, **Lookup Column Name**, and **Lookup Query** properties. In addition, the information contained within the **Lookup Code** property supersedes any values set within these five data properties. **Tip**: An easy way to enter a lookup code is by launching the **Lookup Definition** form, querying for the desired code, copying this code to the Clipboard, and pasting it into the **Lookup Code** field. **Note**: The classification type of the lookup definition code must be of **Lookup Type** (the **Lookup Type** radio button on the **Lookup Definition** form needs to be selected).
	Required	If this item from this combo box field must be selected for the form to be saved, enter "*true*" into the corresponding **Property Value** text box. Otherwise, type "*false*" into this text box. **Note**: The default value for this data property is *false*.

Data Type	Data Property	Description
	Visible Field	If you want this combo box to appear when Oracle Identity Manager generates the form, enter "*true*" into the corresponding **Property Value** text box. Otherwise, type "false" into this text box. **Note**: The default value for this data property is *true*.
Text Field(Display Only)	Visible Field	If you want this text field to appear when Oracle Identity Manager generates the form, enter "*true*" into the corresponding **Property Value** text box. Otherwise, type "*false*" into this text box. **Note**: The default value for this data property is *true*.
Lookup Field(Display Only)	Auto Complete	By entering "*true*" in the corresponding **Property Value** text box, Oracle Identity Manager filters the Lookup field. An user can then add characters into the Lookup field before double-clicking it. By doing so, only those Lookup values which match these characters appears within the Lookup window. As an example, for a **State** lookup field, a user can enter "*new*" into the field. Then, once the user double-clicks the Lookup field, only those states that begins with the letters "*new*" (for example, New Hampshire, New Jersey, New Mexico, and New York) appears within the Lookup window. If you do not want Oracle Identity Manager to filter the Lookup field, enter "*false*" into the associated **Property Value** text box. The default property value for the **Auto Complete** property is *false*.
	Visible Field	If you want this **Lookup** field to appear when Oracle Identity Manager generates the form, enter "*true*" into the corresponding **Property Value** text box. Otherwise, type "*false*" into this text box. **Note**: The default value for this data property is *true*.

System Properties

The following table lists and describes the system properties of Oracle Identity Manager:

Name	Description	Keyword	Value	S*	Run On
Organization Process Inheritance	Determines if processes allowed for an organization are inherited by sub-organizations.	XL.OrganizationProcessInherit	TRUE	v	S
Organization Process Restriction	Determines whether the processes available for an organization are restricted to available processes of the parent organization (that are not a subset of the parent organization).	XL.OrganizationProcessRestrict	FALSE	v	S

Name	Description	Keyword	Value	S*	Run On
Base Help URL	The location of the online Help files.	XL.BaseHelpUrl	//docs/thorteach.com/72/	v	C
Pending Cancelled Tasks	If this property is set to **TRUE**, and one task in a process is cancelled, then all other tasks of that process also get cancelled.	XL.PendingCancelled	True	v	S
Automator Polling Interval	Sets the frequency of the Job Scheduler (in minutes) and checks for scheduled job tasks.	AUTOMATOR.INTERVAL	2	v	C
Maximum Connection Count	Sets the maximum number of database connections that can be created in the connection pool.	XL.MAX_CONN_CNT	50	v	S
Connection ratio	Sets the number of users that can share a database connection in the connection pool.	XL.DB_RATIO	2	v	S
Initial Connection Count	Sets the initial number of database connections that users can share.	XL.INITIAL_CONN_CNT	1	v	S
Connection Test Interval	Sets the frequency to check the connection pool for connection failures.	XL.TEST_INTERVAL	900,000	v	S
Pool Shrink Interval	Based on the connection ratio and the current user count, connections may be closed and the pool shrunk.	XL.SHRINK_INTERVAL	900,000	v	S
Record Read Limit	Sets the maximum number of records that can be displayed in a query result set.	XL.READ_LIMIT	500	v	C
Number of Questions	Sets the number of questions that need to be completed by a user using the Web Application to reset the user's password.	PCQ.NO_OF_QUES	3	v	C
Use of Default Questions	Determines whether a user is required to answer questions defined in the Web Application, or if the user is required to provide his or her own questions.	PCQ.USE_DEF_QUES	TRUE	v	C

Name	Description	Keyword	Value	S*	Run On
Force to set questions at startup	When the user logs into the Web Application for the first time, he/she needs to set the default questions for resetting his/her password.	PCQ.FORCE_SET_QUES	TRUE	v	C
Orbix IDL Compiler Location	Needs to be set for generating a form, and indicates the location of the Orbix IDL compiler.	SDK.IDL_COMPILER	C:\IONA\BIN		C
IDL Files Location	Needs to be set for generating a form and indicates the location of the IDL files.	SDK.IDL_SOURCE_PATH	C:\DEVEL\JAVA		C
JavaDoc Executable Location	Needs to be set for generating a form and indicates the location of the JavaDoc executable file.	SDK.JAVADOC_CMD	C:\JDK1.3\BIN\JAVADOC		C
Compiled JAR File Location	Needs to be set for generating a form and indicates the location where the JAR files are placed by Oracle Identity Manager.	SDK.JAR_LOCATION	C:\DEVEL\JAVA		C
User Id reuse property	Setting this value to TRUE enables another user to reuse the same User ID after a user is deleted.	XL.UserIDReuse	FALSE		C
Organization Self-Serviceable	Determines if the default value for a process is self-serviceable and if it is set or not.	ORG.SELF_SERVICEABLE_DEFAULT	FALSE		C
Allow application-password change for web application	Determines whether users are allowed to change individual application passwords or only Oracle Identity Manager passwords.	PWR.ENABLE_PASSWORD_CHANGE	FALSE		C
Property dictates whether database name appears		XL.TOOLBAR_DBNAME_DISPLAY	FALSE	v	C
Direct Provisioning vs Request for Access Policy Conflicts		XL.DirectProvision	FALSE		S

Name	Description	Keyword	Value	S*	Run On
Organization Delete/Disable Action		ORG.DisableDeleteActionEnabled	FALSE		S
Show TAME in the Adapter Factory selection task list		AF.TAME_DISPLAY	TRUE	v	C
Email Server		XL.MailServer	localhost		S
User Language		user.language	en	v	C
User Region		user.region	US	v	C
User Variant		user.variant		v	C
Database Maximum Connection Count	This is the maximum number of connection to open. When this limit is reached, the threads requesting a connection are queued until a connection becomes available.	XL.DB_MAX_CONN_CNT	25		S
Database Idle Connection Timeout	This is the maximum number of seconds a connection can go unused before it is closed.	XL.DB_IDLE_TIMEOUT	900		S
Database Forced Connection Timeout	This is the maximum number of a thread can checkout a connection before it is closed and is then returned to the pool. The timeout is a protection against the thread dying, thereby leaving the connection checked out indefinitely.	XL.DB_FORCED_TIMEOUT	10800		S
Database maximum Connection Usage	If this value is greater than zero (0), the number of times a connection can be checked out before it is closed. This is used as a safeguard against cursor leak that occurs if you don't call ResultSet.close() and Statement.close().	XL.DB_MAX_CONN_USAGE	9000		S

Name	Description	Keyword	Value	S*	Run On
Database Trace Enabled	Use this parameter to turn the tracing on or off. If turned on, verbose messages about the pool is printed to STDERR.	XL.DB_ TRACE_ ENABLED	FALSE		S
Request Email		Request.Appr oval Email			S
Scheduler Polling Interval		Scheduler.Polli ngInterval	300000		S
Number of Correct Answers	This value represents how many questions the user needs to answer correctly to reset his/her password.	PCQ.NO_OF_ CORRECT_ ANSWERS	3	v	C
Maximum Number of Login Attempts	This value represents how many consecutive times the user can attempt to login to Oracle Identity Manager unsuccessfully before Oracle Identity Manager locks his/her account. **Note**: If the user's account is locked, the user can unlock it by resetting the "challenge" questions associated with resetting his/her password.	XL.MaxLogin Attempts	3	v	C
Maximum Number of Password Reset Attempts	This value represents how many consecutive times the user can attempt to reset his/her password unsuccessfully before Oracle Identity Manager locks his/her account. **Important**: Once the user's account is locked, the user cannot unlock it. If this occurs, contact the System Administrator.	XL.MaxPassw ordResetAtte mpts	3	v	
Self Registratio n Email From Address		XL.SelfRegistr ationEmailFro mAddress	selfreg@xlselfr eg.com	v	
Profile Edit Email From Address		XL.ProfileEdit EmailFromAd dress	selfreg@xlselfr eg.com	v	S

Name	Description	Keyword	Value	S*	Run On
Is Self-Registration Allowed		XL.SelfRegistrationAllowed	TRUE	v	C
Does user have to provide challenge information during registration		PCQ.PROVIDE_DURING_SELFREG	TRUE	v	C

B

Service Account Management

This appendix describes how to change and manage the service account in Oracle Identity Manager. It contains the following topics:

Overview

Service accounts are general administrator accounts (for example, admin1, admin2, admin3, etc.) that are used for maintenance purposes. Usually these accounts are used to allow one system (rather than a user) to interact with another system. The model for managing and provisioning service accounts is slightly different from normal provisioning.

Service accounts are requested, provisioned, and managed in the same manner as regular accounts. Service accounts use the same resource objects, provisioning processes, and process/object forms as regular accounts. What differs is how the service account lifecycle is managed, and what can be done to it.

A service account is distinguished from a regular account by an internal flag. When a user is provisioned with a service account, Oracle Identity Manager manages a mapping from the user's identity to the service account. This user is considered the owner of the Service Account.

This section contains the following topics:

Service Account Change

A user (administrator) can change an existing "regular" account to be a service account or change an existing service account to be a regular account. If any of these changes occur, then the Service Account Change task is inserted within the provisioning process (becoming active in the Tasks tab of the Process Definition). Any adapter associated with this provisioning process executes. If there is no adapter, then a pre-defined response code is attached.

The relevant APIs for this functionality are:

- tcUserOperations.changeFromServiceAccount

- tcUserOperations.changeToServiceAccount

Service Account Alert

When any lifecycle event occurs for the user to whom the service account is linked, the Service Account Alert task is inserted into the provisioning process of that service account instance. A user (administrator) can use this task to initiate the appropriate actions in response to the event that occurred for the user.

Qualifying lifecycle events for a user are the user being disabled or the user being deleted. In these cases, the only action that happens to the service account instance is the service account alert task being inserted.

This behavior is not followed for events directly on the service account (like explicitly disabling a service account).

Service Account Moved

A user (administrator) can transfer ownership of a service account from one user to another. This translates into the provisioning instance showing up in the resource profile of the new owner, and no longer in the resource profile of the old user. The Service Account Moved task is inserted into the provisioning process of the resource instance after the account is moved. Any adapter associated with this provisioning process executes. If there is no adapter, then a pre-defined response code is attached.

The API method for moving a Service Account is tcUserOperationsIntf.moveServiceAccount.

APIs

The following methods set the flag(s):

- tcRequestOperations.addRequestObject
- tcRequestOperations.setRequestObjectAsServiceAccountFlag
- tcUserOperations.changeFromServiceAccount
- tcUserOperations.changeToServiceAccount
- tcUserOperations.provisionObject
- tcUserOperations.moveServiceAccount
- tcObjectOperations.getServiceAccountList

Service Account Management Behavior

Here are some data points about Service Account Management:

- Service Accounts are requested, provisioned, and managed the same as Regular Accounts. A Service Account is no different from a regular account, in that it uses the same resource object, provisioning processes and process/object forms. It is distinguishable from a Regular Account only by a flag. This flag gets set by the user making the request for the resource, or by the administrator direct provisioning the resource (hence, it is exposed/handled in the APIs).
- During its lifecycle, a Service Account can be changed to a Regular Account, and a Regular Account can be changed to a Service Account. When any of these changes occurs then Service Account Changed task functionality is triggered.

- When the user gets "deleted", the resource is not revoked (the provisioning process for the Service Account should not get cancelled), causing the undo tasks to fire. Instead, the Service Account Alert task functionality is triggered.
- When the user gets "disabled", the resource should not be disabled (tasks of effect "Disable" should not be inserted into the provisioning process for the Service Account instance). Instead, the Service Account Alert task functionality is triggered.
- Explicitly disabling/enabling/revoking a Service Account instance (directly or via request) is managed and behave the same way as Regular Accounts.
- Oracle Identity Manager API can be used to transfer (move) a provisioned service account resource (provisioning process, process form entry, etc) from one user to another. When this happens, the Service Account Move task functionality is triggered.

C

The Form Version Control Utility

This appendix describes the scope, content, and description of the Form Version Control Utility. It contains the following topics:

FVC Utility Scope

The following table provides a scope of the functionalities that are implemented with this utility:

Functionality	Implemented (Yes/No)	Comments
Upgrade process form version	Yes	Ensure that the target form version exists and is the active form version.
Upgrade child form version	Yes	The child form version is automatically upgraded to the child form attached with the active parent form.
Update values on parent form	Yes	Ensure that the target form version exists and has the fields whose values you are trying to update.
Update values on child form	Yes	Ensure that the target child form exists and the user is provisioned with the child form.
Insert values on child form	Yes	Ensure that fields that you are inserting exist on the child form version that is attached with the active parent form.

FVC Utility Content

The following table lists and describes the names and paths of the files that comprise the utility.

File Name with Path	Description
<XLCLIENT_HOME>\ lib\xlFvcUtil.jar	This jar file contains the Form Version Control utility classes required to run it.
<XLCLIENT_HOME>\xlFvcUtil.ear	This ear file contains the Form Version Control utility classes required to run it. This ear file is packaged to run with WebSphere launchClient utility.

File Name with Path	Description
<XLCLIENT_HOME>\fvc.properties	This file contains all the configuration properties regarding the source and target form versions, the fields on them, their values as well as child form information.
<XLCLIENT_HOME>\fvcutil.cmd <XLCLIENT_HOME>\fvcutil_websphere.cmd	These are cmd and shell scripts to run the Form Version Control Utility on windows and UNIX.

FVC Utility Description

Form Version Control utility is designed to update custom process forms version number field as well as data in the additional process form fields. The utility is launched from command console, and operates using command line parameters for login and a properties file. The properties in the parameters as well as validity of user's login and password are verified and appropriate error messages are produced to signify an error when one occurs.

Release Notes

- Per system requirements, utility will update only process forms for objects whose status is not "Revoked".
- The utility has special provisioning for the case where form field values need to be updated but form version should remain the same. In this case the <version to> and <version from> parameters must be the same. The utility will not create and error, but will update field values instead for the version specified, while not changing the version value itself.
- The utility does not have any feature that will allow it to "insert" a child record. A child table record is considered to be a single child table field. Thus, if the following entries exist in the `fvc.properties` file:

  ```
  Child;UD_CF3_FIELD7;tiger;Insert

  Child;UD_CF3_FIELD8;mad;Insert

  Child;UD_CF3_FIELD9;me2;Insert
  ```

This will create three different rows in the child table, instead of creating and inserting a single child record having the above values for the three fields.

Index

K

L

M

N

O

P

Q

R

S

T

U

W