Oracle® Identity Manager

Design Console Guide

Release 9.0.3

B32453-01

February 2007

ORACLE®

Oracle Identity Manager Design Console Guide, Release 9.0.3

B32453-01

Primary Author: Don Gosselin

Contents

5 User Management

6 Resource Management

7 Process Management

8 Administering Oracle Identity Manager with Design Console

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 Oracle Identity Manager Design Console. This guide describes the basic functionality of Design Console 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 Oracle Identity Manager Design Console. 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 Guide for JBoss*
- *Oracle Identity Manager Installation Guide for WebLogic*
- *Oracle Identity Manager Installation Guide for WebSphere*
- *Oracle Identity Manager Best Practices Guide*
- *Oracle Identity Manager Globalization Guide*
- *Oracle Identity Manager Administrative and User Console Guide*
- *Oracle Identity Manager Administrative and User Console Customization Guide*
- *Oracle Identity Manager Tools Reference Guide*
- *Oracle Identity Manager Audit Report Developer Guide*
- *Oracle Identity Manager API Usage Guide*
- *Oracle Identity Manager Glossary of Terms*

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.

Convention	**Meaning**
`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 with 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. It is based on an open, standards-based technology and features a three-tier architecture (the client application, an Oracle Identity Manager supported J2EE-compliant Application Server, and an ANSI SQL-compliant database). Oracle Identity Manager can provision both LDAP and non-LDAP enabled applications.

Extensive User Management: Oracle Identity Manager enables you to define unlimited user organizational hierarchies and user groups. It supports inheritance, customizable user ID policy management, password policy management, and user access policies that reflect customers' changing business needs. It enables administrators to manage application parameters and entitlements, to view a history of resource allocations, and it provides delegated administration with comprehensive permission settings for user management.

Web-based User Self-Service: Oracle Identity Manager contains a customizable Web-based user self-service portal. This portal enables management of user information, changing and synchronizing passwords, resetting forgotten passwords, requesting available applications, reviewing and editing available entitlements, and initiating or reacting 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, for example,

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 supports complex, branching and 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 for all processes with full state information. The complete OLAP capability of Oracle Identity Manager supports the most complex reports, analysis, and dynamic queries.

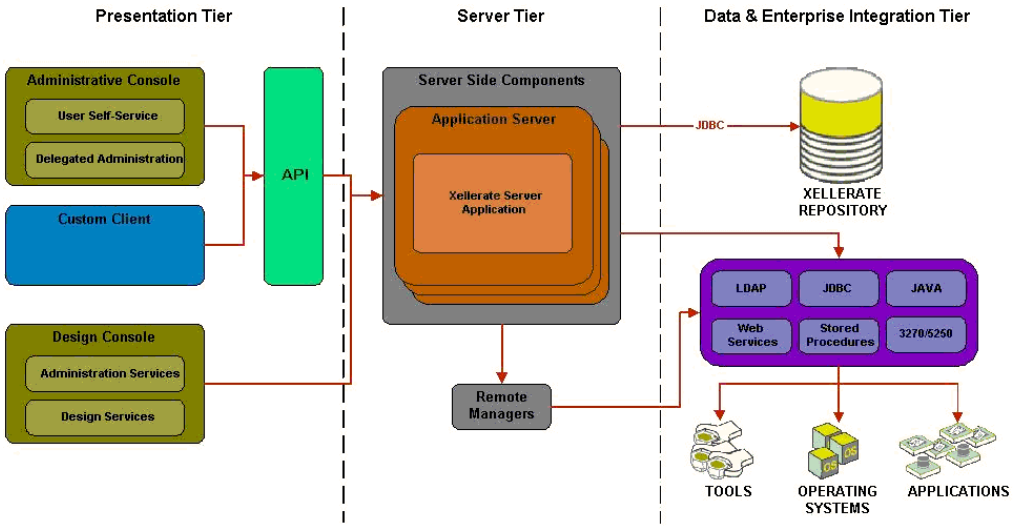
Integration Using the Adapter Factory™: Attempting to support all systems with hand-coded adapters is impractical. Oracle has developed an automated tool for adapter generation. This tool, the Adapter Factory, supports a wide range of interfaces and virtually any application or device. These adapters 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, you can keep existing integrations updated and you can 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 interfaces, Design Console (which is discussed in this guide) and Administrative and User Console. Users log in to Oracle Identity Manager through the Administrative and User Console, which provides the Oracle Identity Manager server with the user's login credentials. With the Administrative and User Console, users search for, edit, and delete information in the Oracle Identity Manager database.

> **Note:** This guide only describes the Oracle Identity Manager Design Console. For information on the Oracle Identity Manager Administrative and User Console, see the *Oracle Identity Manager Administrative and User Console Guide*.

Tier 2: Application Server

The second tier implements the business logic that resides in Java Data Objects. These objects are managed by the supported J2EE application server (JBoss application server, BEA WebLogic, IBM WebSphere, and Oracle Containers for J2EE). 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. To access the business functionality of Oracle Identity Manager, you can use the API layer in 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. It is responsible for the following functions:

- **Logging in to Oracle Identity Manager**: The application server connects the Oracle Identity Manager client to the database.
- **Handling Client Requests**: The application server processes requests from the Oracle Identity Manager client and sends appropriate information from the requests to the database. The Server also delivers responses from the database to the client.
- **Scalability (Connection Pooling/Sharing)**: The 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 prevents unauthorized access by users who might accidentally delete or modify system-level information (system metadata). If an unauthorized user attempts to add, modify, or delete system-level information, the following message appears:

  "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 Design Console

This chapter describes the procedure to start Design Console. It contains the following topics:

Startup

The following procedure describes how to start Design Console.

> **Note:** You can also access the basic features of Oracle Identity Manager by using the Oracle Identity Manager Administrative and User Console. For information on the features of the Oracle Identity Manager Administrative and User Console, see the *Oracle Identity Manager Administrative and User Console Guide.*

To start Design Console:

1. Double-click the **Oracle Identity Manager** client icon on the desktop.

   The Login window appears.

2. Enter your user ID and password.

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

   Your user ID and password cannot have special characters, for example, percent (%), plus (+), equals (=), comma (,), back slash (\), double quotes (“), less than (<), greater than (>), and forward slash (/).

3. Click **Login**.

   The Design Console main screen appears.

   After you log in to Design Console, you can configure the system settings. These settings control the system-wide behavior of Oracle Identity Manager and affect its users. For information on these settings, see Chapter 8, "The System Configuration Form".

3

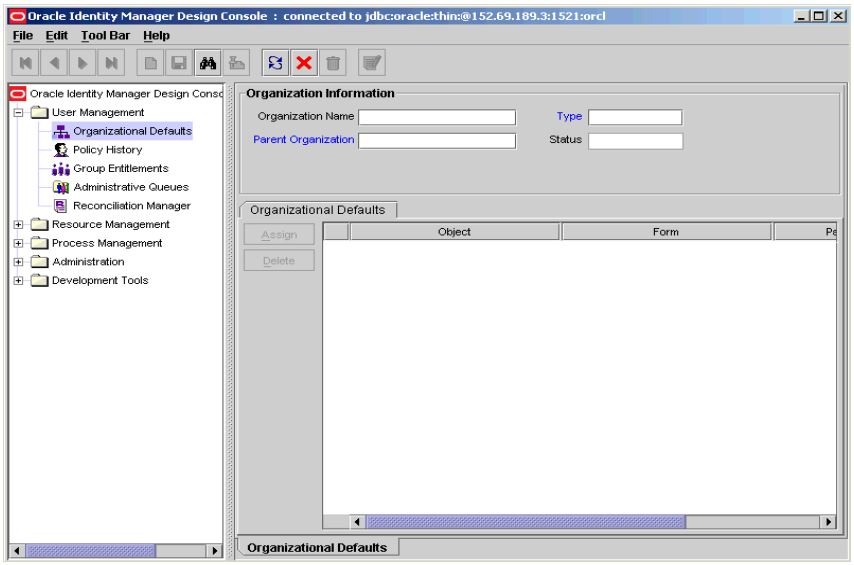
The Design Console Main Screen

This chapter describes the main screen in Design Console. It contains the following topics:

Overview

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

Figure 3–1 Design Console Main Screen



The Design Console main screen consists of four regions:

- The Design Console Menu Bar
- The Design Console Toolbar

- The Design Console Explorer
- The Design Console Workspace

These regions are described in the following sections.

The Design Console Menu Bar

The menu bar appears at the top of the main screen. It contains menus that enable you to perform all operations in the Design Console user interface.

To issue a menu command:

1. Click the menu that contains the command.

   A list of menu items appears.

2. Click the menu item that contains the command.

   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 keyboard shortcuts, for example, **ALT+F** for the **File** menu, or shortcuts keys, for example, **Ctrl+P** to print the active form. Keyboard shortcuts and shortcut keys are displayed in black in the menu. Disabled shortcuts and keys appear in gray.

The Design Console Menu Bar provides four menus: **File**, **Edit**, **Toolbar**, and **Help**. This rest of this section describes the following topics:

- File Menu
- Edit Menu
- Toolbar Menu
- Help Menu

File Menu

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

Menu Item	Action
Print	Print the active form
Login	Log out of Design Console, and then log in again
Exit	Exit Design Console

Edit Menu

The **Edit** menu provides the following 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 operations are described in the following table.

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 Design Console Workspace.

Help Menu

The **Help** menu provides access to the Oracle Identity Manager Design Console Help system and copyright information, as described in the following table.

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

The Design Console Toolbar

The toolbar is a series of buttons below the menu bar. These buttons provide single-click access to frequently used actions. The toolbar buttons always apply to the active form.

Figure 3–2 shows the Design Console Toolbar.

Figure 3–2 Design Console Toolbar

When you hold the mouse over a toolbar button for a few seconds, a tool tip appears containing a description of that button.

The following table describes the toolbar buttons.

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

Design Console Shortcuts

Design Console provides the following keyboard shortcuts to perform functions quickly and provide you with easy access to menu commands.

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.
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.

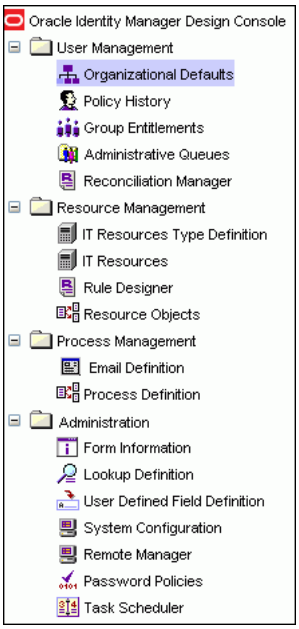
Shortcut Name	Keystroke Combination	Description
Refresh	CTRL+R	Refresh the active form.
Close	CTRL+W	Close the active form.
Delete	CTRL+D	Delete the current record.
Next	Numpad + (plus)	Display the next record, when you have queried more than one record.
Previous	Numpad - (minus)	Display the previous 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 Design Console icon, which appears at the top of the Design Console Explorer.
Lookup	F4	Display the Lookup window for the selected lookup field.
Menu	F10	Activate the **File** menu.

The Design Console Explorer

The Design Console Explorer contains a list of icons that represent forms that you have permission to access.

Figure 3–3 illustrates the Design Console Explorer. Your system administrator can customize the Explorer. Depending on your permissions, you may see different icons in the Explorer. If you want to access form icon that you do not see, contact your System Administrator.

Figure 3–3 Design Console Explorer



> **Tip:** When the System Administrator has changed your permissions, you should refresh the Explorer window, as described in one of the following procedures.

To launch a form:

1. Click the plus icon to the left of the folder that contains the desired form.
2. Double-click the appropriate icon for the form that you want.

   The corresponding form appears in the Design Console Workspace.

> **Tip:** You can adjust the size of the Design Console Explorer by dragging the Split Bar to the right or left. The Split Bar is the vertical line separating the Design Console Explorer from the Design Console Workspace.

To refresh the list of forms:

1. Right-click the Oracle Identity Manager logo at the top of the Oracle Identity Manager Explorer window.
2. The **Refresh Explorer** menu command appears in a pop-up window.
3. Click this command.

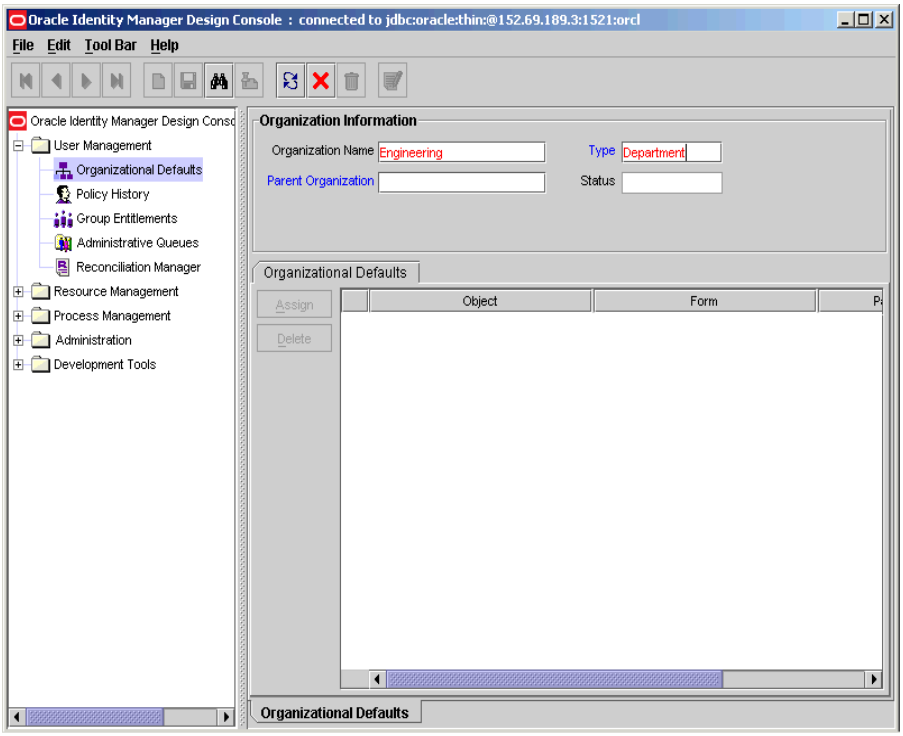
   Design Console refreshes the Explorer with all forms that you can access, including any forms that a System Administrator has recently given you permission to access.

The Design Console Workspace

The Design Console workspace is the region of the main screen that displays forms that you access using the Explorer.

Figure 3–4 illustrates the workspace.

Figure 3–4 Design Console Workspace



If you access multiple forms, Design Console places the active form on top and layers the remaining forms on tabs 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.

Design Console can display each form in two views: a form view and a table view. The differences between the information presented in each view are explained in the following paragraphs.

Form View

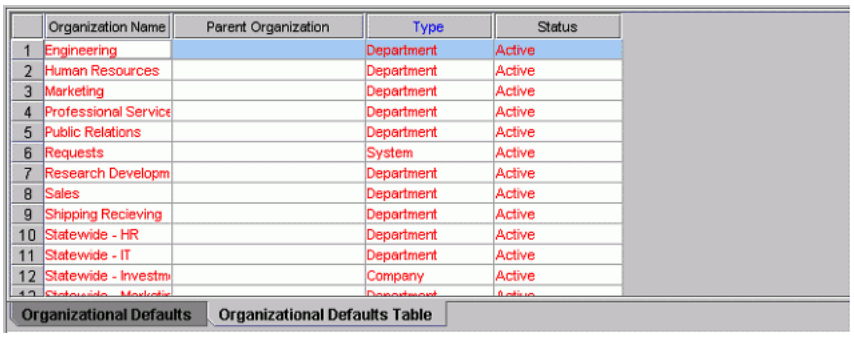
A form view provides detailed information about a single record. The form view appears when a you initially access a form using the Explorer, for example, before you perform a query.

Table View

A table view lists general information about multiple records of a form. When you submit a query that produces more than one result, Design Console displays a table containing the records that match the criteria in the query.

For example, a query of the **Organizations** form may return several records. Both the form and table view tabs of the **Organizations** form can appear. Figure 3–5 illustrates the Table View of Design Console.

Figure 3–5 Table View



The following applies to all table views:

- To select a record in a table view, click it.
- The data associated with a record is displayed in cells.

  Cells are also referred to as fields.
- Forms contain **column headers**, which are a gray box with a label above each column.

  Column headers display the name of the column. If a column has a Lookup dialog box, the column header appears in blue.
- Design Console forms contain **row headers**, which are a gray box with a numeric label at the beginning of each row.

  To view a detailed form view of a record, double-click its row header. To display a record in the form view, select the desired record in the table view, then click the applicable form tab at the bottom of the workspace.
- If a query returns more records than can be displayed in the workspace, a vertical scroll bar appears along the right edge of the table view.

  Click the **Up** or **Down** arrows in the vertical scroll bar to scroll through the records of the table.
- If the table view contains more columns than can be displayed in the workspace, a horizontal scroll bar appears along the bottom edge of the table view.

  Click the **Left** or **Right** arrows in the horizontal scroll bar to reveal additional columns not initially visible in the workspace.
- You can edit record information in the individual cells (fields) of the table view.

  To edit the information in a particular field, click it, and make the desired changes.
- Fields that appear in blue have Lookup dialog boxes.

  You can double-click these fields to access their Lookup dialog box, then select the desired value. When you edit the value in any field, the row header for the corresponding record changes to black. This indicates that data in that field has been changed and must be saved.
- To select consecutive record rows, use the **SHIFT** key.
- To select non-consecutive record rows, use the **CTRL** key.
- To export a record, right-click its row header.

  To select more than one record, press the **SHIFT** key before clicking the row header.

A pop-up dialog box appears.

- Select **Copy to Clipboard** to copy the selected records to the Clipboard.

  You can paste copied records into an Microsoft Excel spreadsheet or a Microsoft Word document.

- To save the record(s) as a tab-delimited file, select **Copy to File**.

- You can control the order in which the records in a table view are displayed 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. A triangle appears beside the column header text. This indicates the direction, ascending or descending order, in which the records were sorted.

4

Basic Functions in Design Console

This chapter describes how to use the basic features of Design Console. Oracle recommends that you review this section before proceeding to later chapters of this manual.

This chapter contains the following sections:

Special Field and Form Types

The behavior of the basic features of Design Console is standard for all forms to enable ease of use. This section describes the standard behaviors and the field and window types in the Design Console main screen.

Data Fields

Data fields are display areas in forms that present information related to a specific record. For example, **First Name** may be a data field on the **Users** form.

The label of a field may be displayed in black or blue.

- A black label indicates that this field is a standard field.

  You can query, create, modify, or delete information in this type of field.

- A blue label indicates that the data in this field is derived from a pre-defined list of values supplied using a Lookup or a Date & Time window.

  When you double-click this type of field, the applicable Date & Time window or Lookup window appears. You can then select a date, time, or a lookup value.

The value of a field may be displayed in black or red.

- If the field value is displayed in black, the data in this field is provided by the user.

  You can query or edit the information in these types of fields.

- If the field value is displayed in red, the data in this field is provided by Oracle Identity Manager.

  Values of this type are read-only. This prevents users from overwriting critical information.

Lookup Fields

A lookup field enables you to search for a value. The following procedure describes how to use lookup fields.

To use lookup fields:

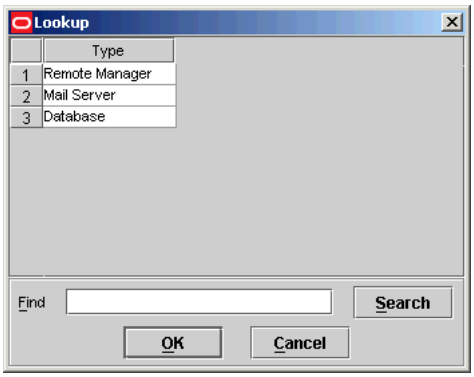
1. If the Lookup dialog box contains a short list of fields, click a field, then click **OK**.

   Alternatively, you can select the field and press the **F4** key.

   Click **Cancel** to close the Lookup window without selecting anything.

   Figure 4–1 displays the Lookup dialog box.

Figure 4–1 The Lookup Dialog Box



2. If the Lookup dialog box contains a long list of values, enter the first few characters of the value you want in the **Find** box, followed by a wildcard (*), then click the **Search** button.

   The Lookup dialog box displays the results that match your search.

Date And Time Fields

The Date & Time window enables you to select a month, year, date, and time. This window appears when you double-click a field that is equipped with it.

To select a date and time:

1. Double-click the field where you want to enter a date and time.

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

   The Date & Time window appears.

2. Click the box.

   From the pull-down menu, 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.

   The Date & Time window disappears. The field that you double-clicked in Step 1 now displays the date and time you selected.

Click **Cancel** to exit without saving.

Box

Box fields are equipped with a list of pre-defined values. When you click a box, its values are displayed. If the list contains more values than can be displayed at one time, a vertical scroll bar appears to the right of the list.

When you select a value, the list disappears, and the selected value appears in the box.

Notes Window

The Notes window enables you to enter supplemental information for a record. When used with adapters, this window also displays the code that Design Console generated while compiling the adapter.

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

> **Note:** In the following procedure, if the Notes button is red, the current record already has a note. To view the note, click the button. You can enter supplemental information in this record. Each entry receives a unique date, time, and user stamp.

To use the Notes window:

1. Query for the desired record.
2. Click the **Notes** button.

   The Notes window appears.
3. Enter information in the text area of the Notes window.
4. Click the icon that represents a man to store your information into the Notes window.

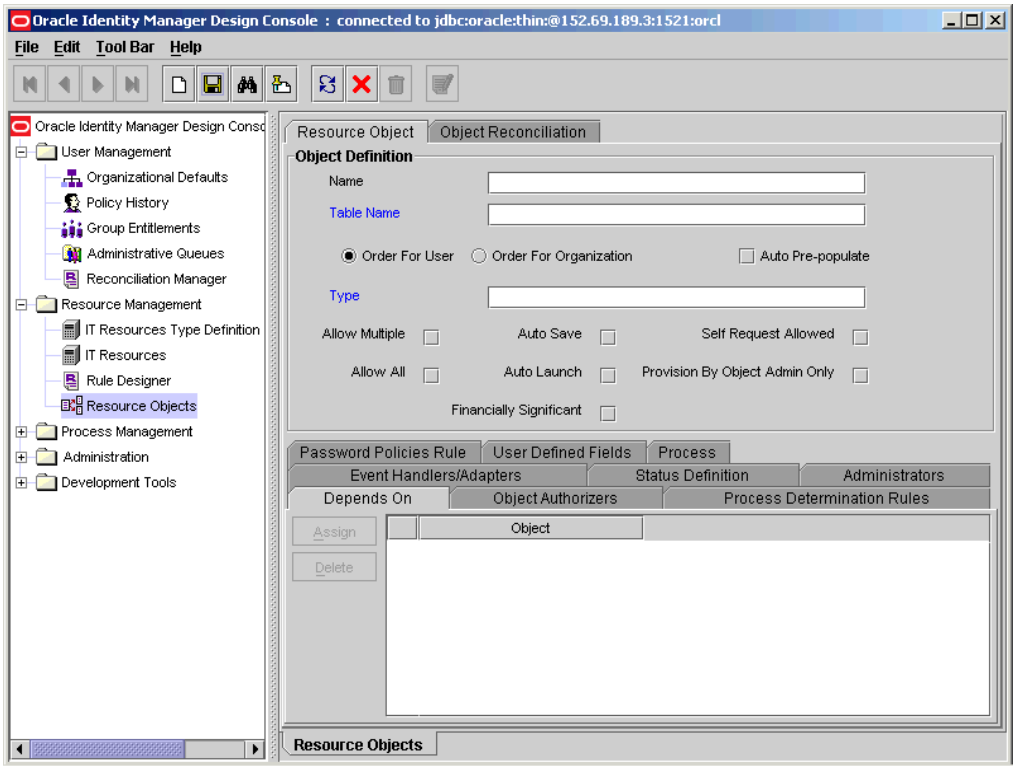
   Or, click **Close** to close the Notes window without saving.
5. From the Toolbar, click the **Save** button.

   The information you entered into the Notes window is saved.

Tabs On Forms

Most Design Console forms contain multiple tabs. The tabs are usually located in the lower region of the form. The tabs display additional information about a record, for example, the users who are employed at an organization, as shown in Figure 4–2.

Figure 4–2 Design Console Design Console - Tab on Forms



Each tab has its own tables and function buttons. Usually, the buttons on a tab are not enabled until the information in the upper portion of the form is saved. The table displayed in the tab enables you to view and edit the records associated with that tab item.

To modify information in a row of a tab's table, either double-click the field that contains the information you want to edit, or double-click the associated row header.

Assignment Windows

The User Form Assignment windows enable you to select and assign available entities to a record. The Assignment window appears when you click the **Assign** button.

The left panel of this window lists items that you can assign to the record, for example, Organization. The right panel lists the items that have already been assigned to the record. 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.

The following are methods for working with this window:

- To select multiple non-consecutive items, hold down the **CTRL** key while selecting items with the mouse.

  For example, you can select the User Group, the IT Resource Type Definition object, and the Form Information object, but not the Process Definition object.

- To select multiple items that are listed consecutively, 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 the right-pointing arrow.

- To unassign one or more items that are assigned already, select it, and click the left-pointing arrow.

When you are done, click **OK**. If you click **Cancel**, all assignment changes you made are discarded.

Performing a Search (or Query)

Design Console enables you to perform searches, also referred to as "queries," for records in the database. Every form in Design Console provides a search function. The search function is also available in lookup fields.

To conduct a search, click the binoculars icon on the toolbar:

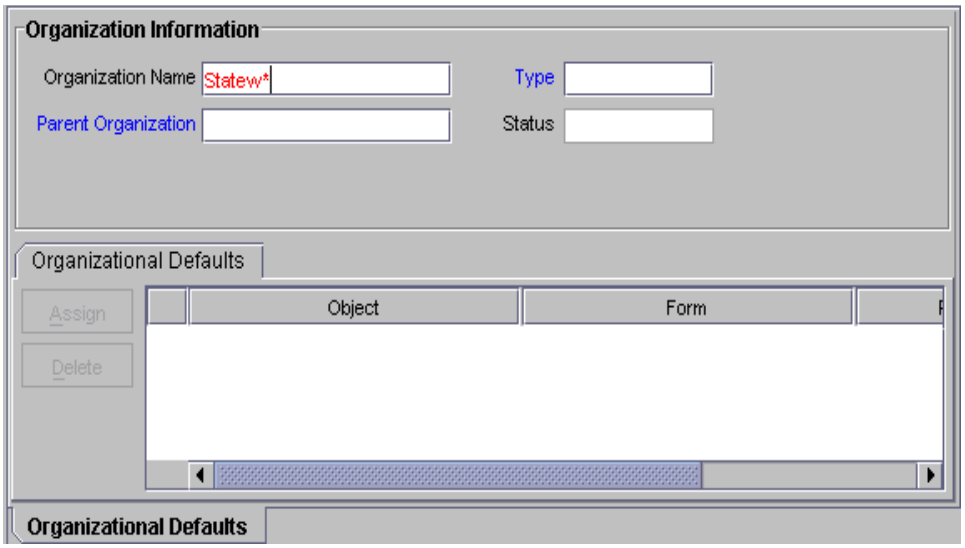
Constructing a Search (or Query) Filter

You can filter the search criteria in a form field. This limits the results that are returned to only the records that match the criteria you entered. If you leave all form fields blank prior to conducting the search, all records in the table are returned.

You can use a wildcard in a search. The asterisk (*) wildcard character represents unspecified portions of search criteria. You can use a wildcard at the beginning, middle, or end of the value that you enter in a field. For example, if you enter B* in the Location field of an Design Console form and execute a search, you retrieve all records with locations that begin with the letter B (for example, Burbank, Boston, Bristol, and so on). If the * character is placed in the middle of a search value, as in Br*on, you retrieve all records that begin with BR and end with ON (for example, Brighton, Boston, and so on) 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, and so on).

In Figure 4–3, a query is performed on the Organizational Defaults form and the Organization Name field is used to filter the search criteria. The filter Statew***;** ensures that only organizations with names that begin with Statew are retrieved.

Figure 4–3 Displaying the Results of a Search Query



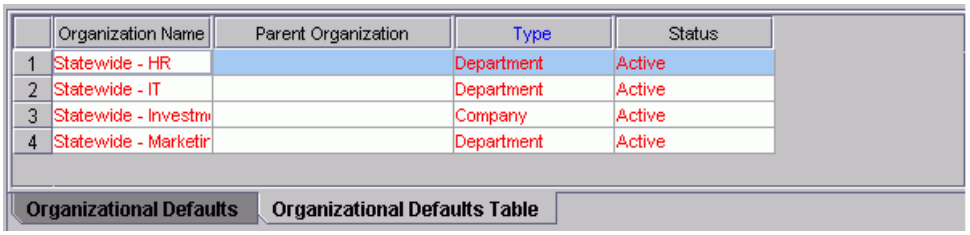
Results of a Search

After you enter criteria in the query fields, click the binoculars symbol 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. Either the record that you are searching for no longer exists in the database, or you should modify your search criteria.
- **One record is returned.** One record in the database matches your search criteria. The Form view displays that record.
- **More than one record is returned.** Multiple records in the database match your search criteria. A Table view appears, listing all records that meet your search criteria. 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



Working With a Set of Query Results

If multiple records in the database match your search criteria, you can view details about each record. Several buttons can assist you when viewing these records in the

Form view. These directional buttons, referred to as VCR buttons, are located in the toolbar. They are described below:

Buttons	Description
	Click this button to display the first record in the result set in the Form view.
	Click this button to display the preceding record according to the display sequence in the Table view. The record appears in the result set in the Form view.
	Click this button to display the next record (according to the display sequence in the Table view) in the result set in the Form view.
	Click this button to display the last record in the result set in the Form view.

Optimizing Query Performance

A query that returns a large result set can require significant time to run and can consume your computer's resources. To optimize performance, employ the following search techniques:

- Define the scope of a search strategy as precisely as possible.

  Enter the most specific information that you can when constructing your query. For example, if the first name of a contact is JOHN and the last name is JACKSON, enter both pieces of information rather than searching only for contacts with the last name JACKSON.

- Use the * wildcard character where possible.

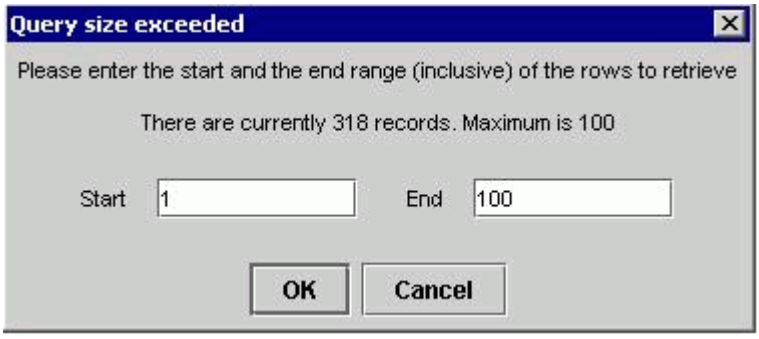
  If you place the * wildcard in front of an alphabetical character (for example, "*A"), this returns fewer records compared to leaving the value in a given field blank.

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

Exceeding the Limit for a Result Set

If you have both read- and write-access to all forms and records in Design Console in the System Configuration form (that is, you are a System Administrator), 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, Design Console displays the Query Size Exceeded dialog box, as shown in Figure 4–5.

Figure 4–5 The Query Size Exceeded Dialog Box



You are prompted to enter a specific range or subset of the result set to be viewed. In Figure 4–5, the maximum result set of 100 has been exceeded. The dialog enables you to display only records 1 through 100.

> **See also:** For more information on the System Configuration form, see "The System Configuration Form" on page 8-14.

5

User Management

This chapter describes managing users in Design Console. It contains the following topics:

Overview

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

This folder contains the following forms:

- **Organizational Defaults**: Use this form to view records that reflect the internal structure of your organization and to designate information related to these entities.
- **Policy History**: Use this form to view user records that your employees require.
- **Group Entitlements**: Use this form to view records for groups of users to whom you may assign some common functionality.
- **Administrative Queues**: Use this form to create and manage mass-assignment privileges for user groups for other Design Console forms.
- **Reconciliation Manager**: Use this form to manage reconciliation events in Oracle Identity Manager.

Organizational Defaults Form

The Organizational Defaults form appears in the User Management folder. You use this form to view records that reflect the structure of your organization and to enter and modify information related to organizational entities. An organization record contains information about an organizational unit in an enterprise hierarchy, for example, a company, department, or branch. A sub-organization is an organization that is a member of another organization, for example, a department in a company.

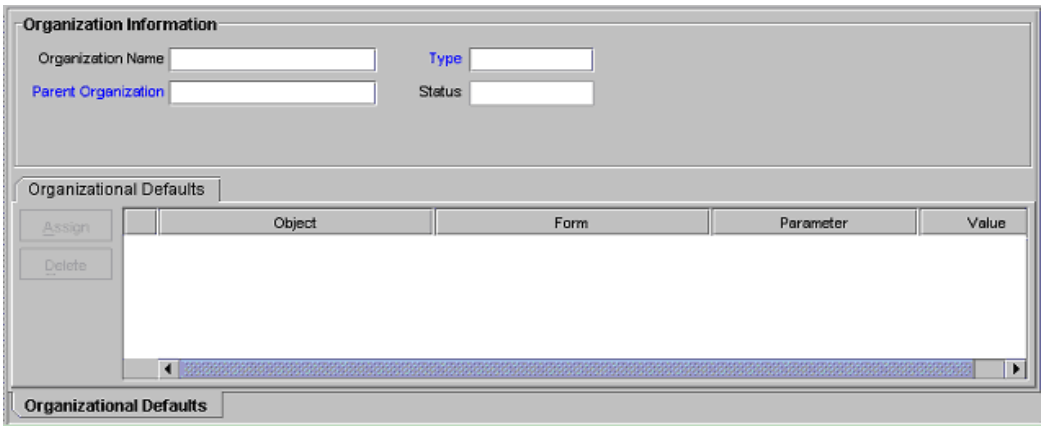
The organization that the sub-organization belongs to is referred to as a parent organization.

You use the Organizational Defaults tab to specify default values for parameters on the custom process form for resources that can be provisioned for the current organization. Each process form is associated with a resource object that is allowed for the organization, or with a resource that has the Allow All check box on the associated Resource Objects form selected.

The values that you provide in the Process Defaults tab become the default values for all users in the organization.

Figure 5–1 illustrates the Organizational Defaults form.

Figure 5–1 The Organizational Defaults Form



The following table describes the data fields of the Organizational Default 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 that this organization belongs to. If a parent organization appears in this field, this organization appears on the Sub Organizations tab for the parent organization. If this field is empty, this organization is a top-level organization.

The Policy History Form

You use the Policy History form to view information about the resources that are allowed or disallowed for a user.

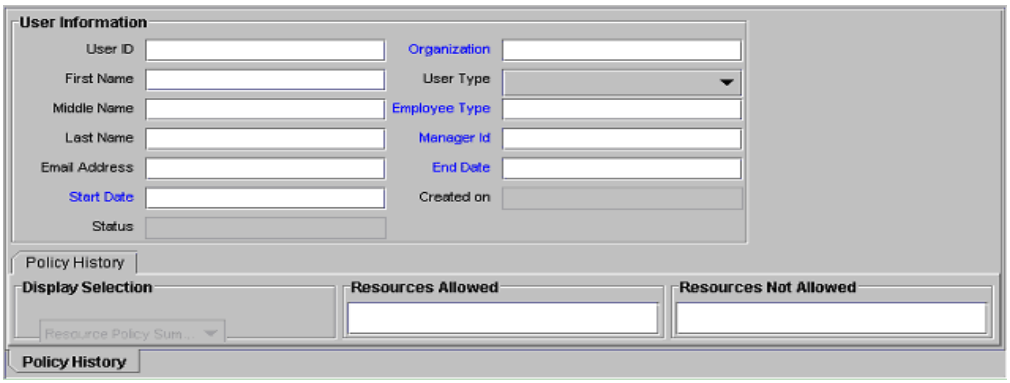
There are two types of users in Oracle Identity Manager:

- **End-User Administrators**: This type of user can access the Design Console and the Administrative and User Console. The System Administrator sets permissions to enable End-User Administrators to access a subset of the forms in the Design Console.
- **End-Users**: This type of user can access only the Administrative and User Console and generally have fewer permissions than End-User Administrators. Only

resource objects that are defined as self-service on the Objects Allowed tab of the user's organization are available for provisioning requests using the Administrative and User Console.

Figure 5–2 illustrates this form.

Figure 5–2 The Policy History Form



The following table describes the data fields of the Policy History 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** and **End-User Administrator**. Only End-User Administrators have access to Design Console.
Employee Type	The employment status of the user at the parent organization (for example, Full-Time, Part-Time, Intern, and so on).
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 when the user record was created.

Policy History Tab

Use this tab to view resource objects that are allowed or disallowed for a user, based on the following:

- Access policies for the user group that the user belongs to
- Resource objects that are allowed by the organization that the user belongs to

The Policy History tab contains a Display Selection region. To organize the contents of this tab, go to the uppermost box in this region and select an item from one of its menus, as follows:

- **Resource Policy Summary**: Displays resource objects that are allowed or disallowed based on the user's organization and applicable access policies.
- **Not Allowed by Org**: Displays only resource objects that are disallowed, based on the user's organization.
- **Resources by Policy**: Displays a second box that contains the access policies for the user groups that the user is a member of.

  Select an access policy from this box to display the resource objects that are allowed or disallowed for the user, based on this access policy.

A tracking system enables you to view resources that are allowed or disallowed for a user, based on the organizations the user is a member of and the access policies that apply to the user.

The resource objects that are allowed for the user appear in the Resources Allowed list. This list represents resource objects that can be provisioned for the user. It does not represent the resource objects that are provisioned for the user.

The resource objects that are disallowed for the user appear in the Resources Not Allowed list.

To view this tracking system:

1. Go to the Policy History tab.
2. Find the **Display Selection** region on this tab.
3. Click the **Policy History** button.

   The User Policy Profile History window appears.

From this window, you can view resources that are allowed or disallowed for a user for the date and time you selected as follows:

- From the **History Date** box, you can select the desired date.
- From the **Display Type** box, you can display resources that are allowed or disallowed based on the organizations the user is a member of, the access policies that apply to the user, or both.
- From the **Policy** box, you can display the access policy that determines what resource objects are allowed or disallowed for the user.

Assigning Group Entitlements

The Group Entitlements form appears in the User Management folder. You use it to create and move forms, and to designate the forms and folders that members of a user group can access through the Explorer.

To work with the Group Entitlements form:

1. Open the Group Entitlements form.

   The User Group Information dialog box appears.
2. In the **Group Name** field, enter the name of the user group.
3. Click **Assign**.

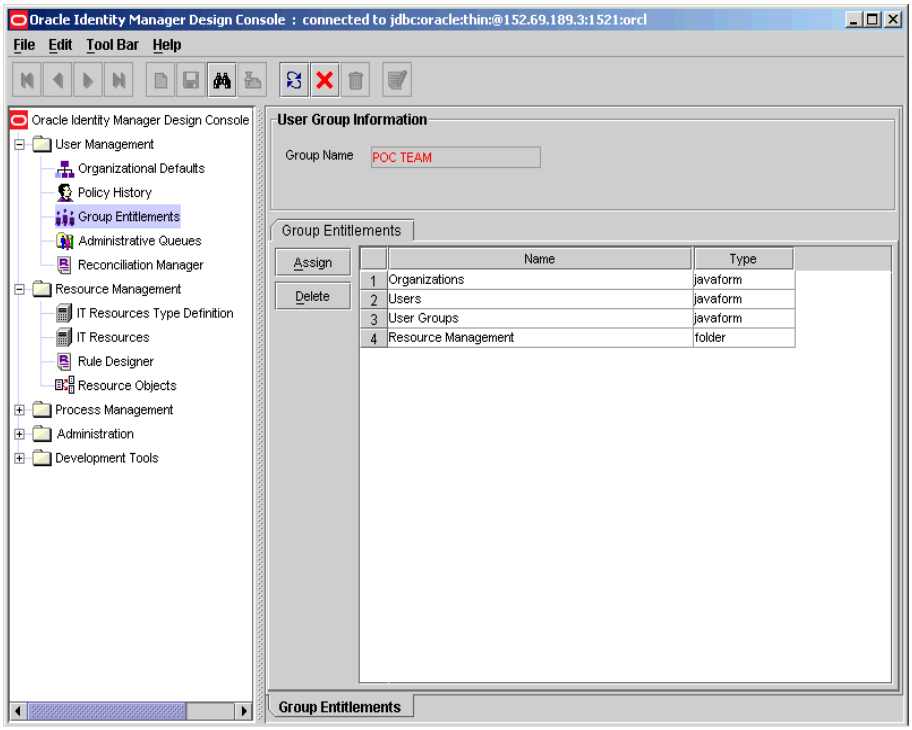
   The User Form Assignment lookup table appears.

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 you are done.

   The User Group Information dialog box appears.



The newly added user forms are listed in a Group Entitlement table. The Group Entitlement Table displays all available user groups. This table shows the name of the user form and the type. In the previous example, there are two types, javaform and folder. A javaform is a Java-based, graphical interface. A folder is a container of one or many javaforms.

Pre-Existing Groups

Oracle Identity Manager provides four default user group definitions:

- System Administrators
- Operators
- All Users
- Self Operators

You can modify the permissions associated with these user groups, and you can create additional user groups.

The System Administrators User Group

Members of the System Administrators user group have full permission to create, edit, and delete records in Oracle Identity Manager, except for system records.

The Operators User Group

Members of the Operators user group can view Organizational Defaults and Policy History forms, and can perform limited functions with these forms.

The All Users User Group

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

A user cannot be removed from the All Users group.

The Self Operators Group

The Self Operators group 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 in the Oracle Identity Manager Administrative and User Console.

Important: Do not modify the permissions associated with the Self Operators user group or assign any users to this group.

The Administrative Queues Form

You assign groups of users to manage a provisioning request using an entity called a queue. A queue is a collection of group definitions. Queues can be nested within other queues.

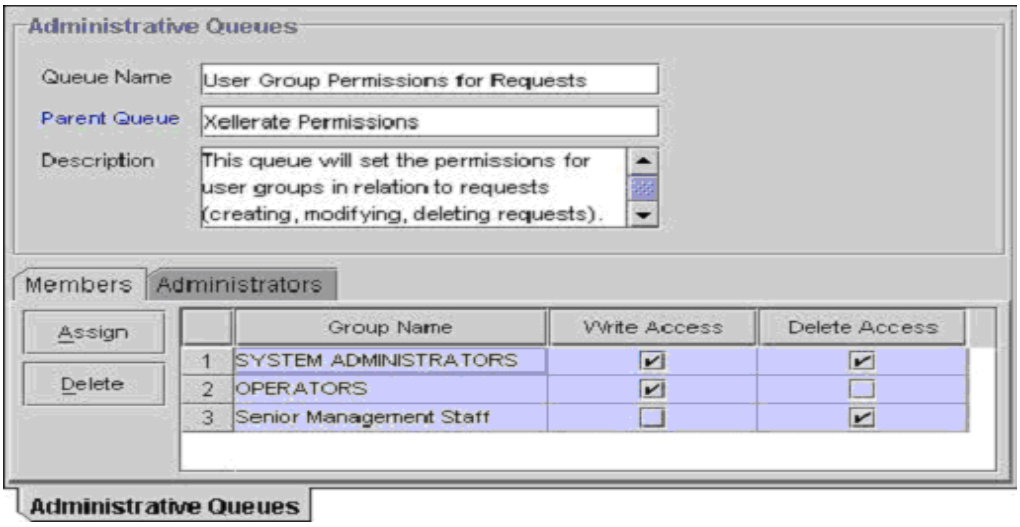
You use the Administrative Queues form to create and manage administrative queues. You assign queues to requests from the Queues tab on the Requests form.

Administrative queues increase the efficiency and manageability of requests. By using an administrative queue, you can accomplish the same goal with only a few mouse clicks. A queue that you assign to one request can be reused for other requests.

A request can specify different administrative privileges for each group in the queue. For example, suppose that you assign a queue with three user groups to a request. The members of the three groups can each have different administrative privileges for the request. The first user group can be allowed to read, modify, and delete the request. The second user group can be allowed to read and modify only, while the third user group can only be able to read and delete the request.

The Administrative Queues form is illustrated in Figure 5–3. This form appears in the User Management folder.

Figure 5–3 The Administrative Queues Form



The following table describes the fields of the Administrative Queues 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.

Creating an Administrative Queue

You can create parent queues and nested queues. The following procedure describes how to create an administrative queue.

To create an administrative queue:

1. Open the Administrative Queue form.
2. In the **Queue Name** field, enter the name of the queue.
3. Double-click the **Parent Queue** lookup field.

   From the lookup dialog box, select the queue that this queue is a member of. If the queue does not belong to another queue (it is a parent queue), proceed to the next step.
4. In the **Description** field, enter information about the queue.
5. Click **Save**.

Tabs on the Administrative Queues Form

After you launch the Administrative Queues form and create a queue, the tabs on this form become functional.

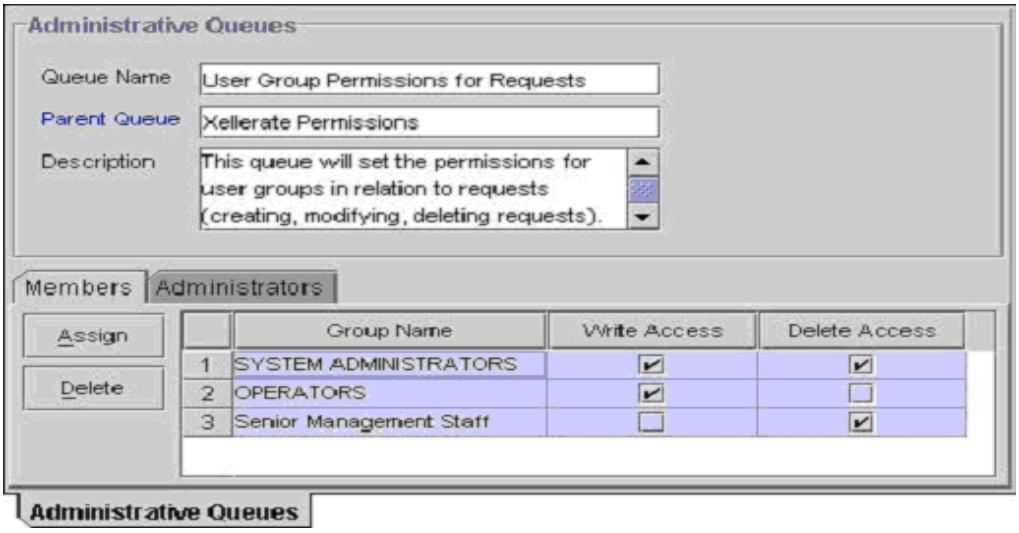
The Administrative Queues form contains the following tabs:

- Members Tab
- Administrators Tab

Members Tab

You use the Members tab to add user groups to, and delete user groups from, the current administrative queue. The Members tab is illustrated in Figure 5–4.

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



In Figure 5–4, the **User Groups Permissions for Requests** queue is configured as follows:

- The **SYSTEM ADMINISTRATORS** user group can read, modify, and delete information in the request.
- The **OPERATORS** user group can read and modify information in the request. The **Delete Access** check box is cleared, so this user group cannot delete the request.
- The **Senior Management Staff** user group can delete the request. The **Write Access** check box is cleared, so this user group cannot modify information in the request.

Assigning a User Group to an Administrative Queue

To assign a user group to a queue:

1. Click **Assign**.

   The Assignment dialog box appears.

2. Select the user group, and assign it to the administrative queue.
3. Click **OK**.

   The user group appears in the **Members** tab.

4. Select the **Write Access** check box to enable a user group to create and modify information in the requests that the administrative queue is assigned to.

   Otherwise, proceed to Step 5.

5. Select the **Delete Access** check box to enable the user group to delete requests that the administrative queue is assigned to.

   Otherwise, proceed to Step 6.

6. Click **Save**.

The user group is assigned to the administrative queue.

Note: By default, groups listed on the **Members** tab have read privileges for the requests that the queue is assigned to.

Removing a User Group From an Administrative Queue

Remove a user group from the administrative queue when that user group can no longer read, modify, or delete information on requests that queue is assigned to.

To remove a user group to an administrative queue:

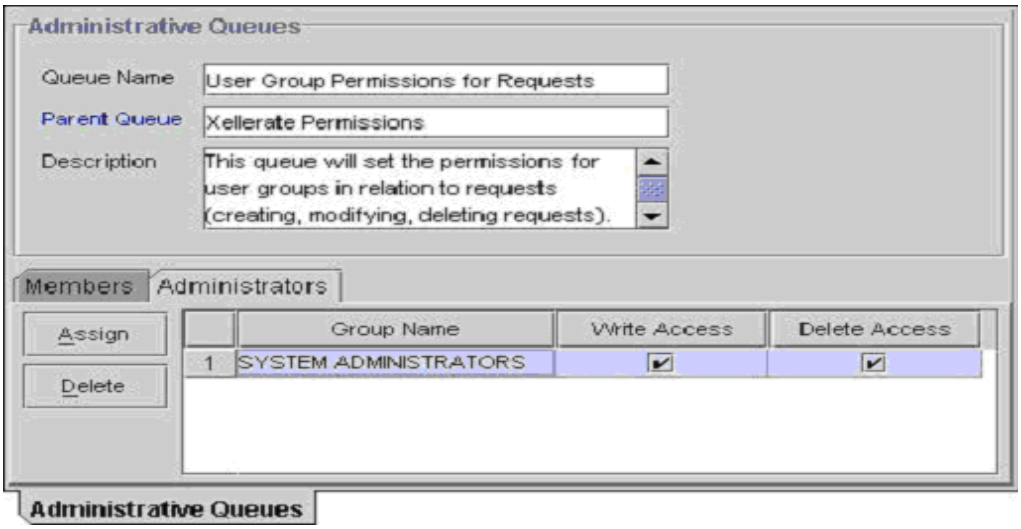
1. Select the user group that you want to remove.
2. Click **Delete**.

   The user group is removed from the administrative queue.

Administrators Tab

You use this tab to select the user groups that can read, modify, and delete the current administrative queue, as illustrated in Figure 5–5.

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



In Figure 5–5, both the **Write Access** and **Delete Access** check boxes are selected for the **SYSTEM ADMINISTRATORS** user group. This allows the user group to read, modify, and delete the **User Groups Permissions for Requests** administrative queue.

Adding a User Group to an Administrative Queue

Adding a user group as to an administrative queue gives the group members administrative privileges.

To add a user group to an administrative queue:

1. Click **Assign**.

   The Assignment dialog box appears.
2. Select the user group, and assign it to the administrative queue.
3. Click **OK**.

The user group appears in the **Administrators** tab.

4. Select the **Write Access** check box to enable the associated user group to read and modify the current administrative queue.

   Otherwise, proceed to Step 5.

5. Select the **Delete** check box to enable the associated user group to delete the current administrative queue.

   Otherwise, proceed to Step 6.

6. Click **Save**.

   The user group is now an administrative group in the administrative queue.

Removing a User Group From an Administrative Queue

You should remove a user group from an administrative queue when the user group can no longer read, modify, or delete the current administrative queue.

To remove an administrator user group from an administrative queue:

1. Select the user group that you want to remove.
2. Click **Delete**.

   The administrator user group is removed from the administrative queue.

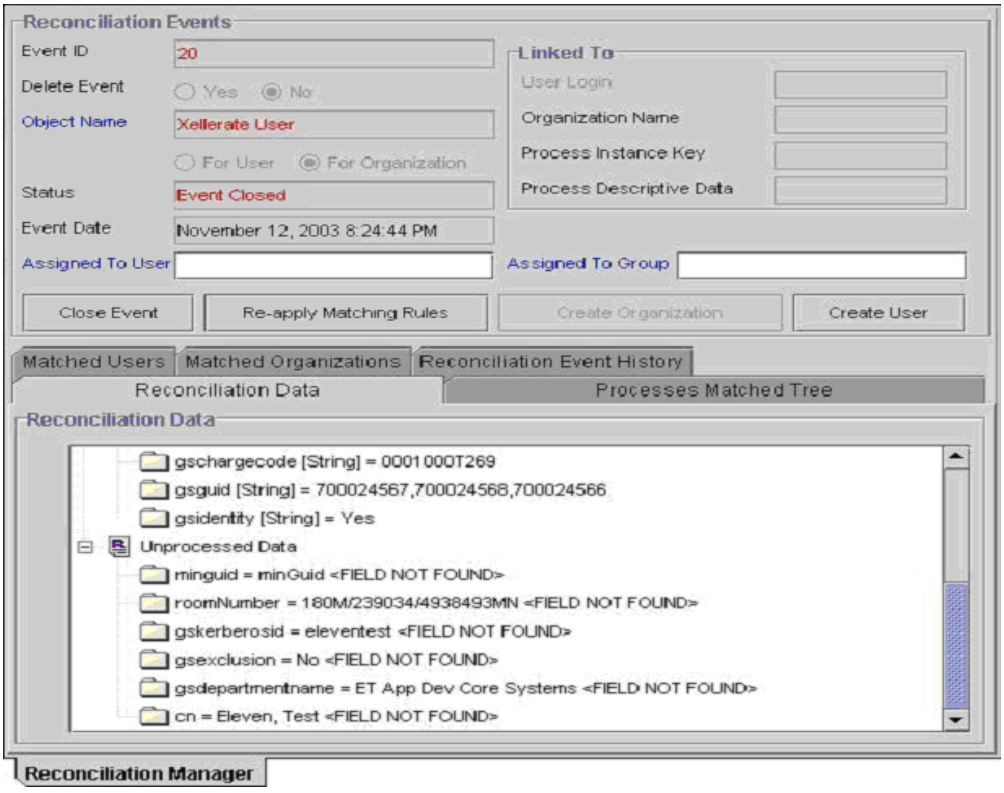
The Reconciliation Manager Form

This form is located in the User Management folder. It enables you to view, analyze, correct, link, and manage information in reconciliation events received from target resources and trusted source. A designated person can manually analyze and link information in reconciliation events, or analysis and linking can be performed automatically by Oracle Identity Manager based on action rules you have defined. These rules are based on whether an event is associated with an existing record, if it represents a new account, or if it can allow the linking of the information in the event to be manually initiated.

The reconciliation classes that you define periodically poll your target resources and trusted source. Any changes on these systems generate reconciliation events that are written to the Reconciliation Manager. Oracle Identity Manager analyzes event information according to mappings defined in a relevant provisioning process.

Figure 5–6 illustrates the Reconciliation Form.

Figure 5–6 The Reconciliation Manager Form



Note: You can use Design Console Task Scheduler form to define a schedule and set timing parameters to govern how often a reconciliation class is run, or to use a third-party scheduling tool to set the polling frequency.

The Reconciliation Manager form works as follows:

- If the information in the event relates to an existing user or organization record, you can use this form to manually link the data in the event to the record.

  Or, you can review information that was automatically linked to the user or organization.

- If the event represents creation of a new employee on a trusted source (user discovery) or provisioning of an existing employee with a new resource (account discovery), you can use this form to manually update Oracle Identity Manager with new data.

  Or, you can review information that was automatically linked to a user. For trusted sources, the data in the event is used to create a new user account. For target resources, the data in the event is used to populate the relevant resource-specific process form.

- If the event represents creation of a new organization on a trusted source (organization discovery) or provisioning of an existing organization with a new resource (account discovery), you can use the form to manually update Oracle Identity Manager with the new data.

Or, you can use the form to review the information that was automatically linked to a organization.

- If the event represents 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 to review an account that was automatically deleted.

  For trusted sources, this deletes the user's Oracle Identity Manager account and revokes all accounts with which that user may have been provisioned on any target resources.

  For target resources, Oracle Identity Manager recognizes that the user's account on that system has been revoked.

The upper portion of the Reconciliation Manager form contains the following items:

Field Name	Description
Event ID	The numeric ID of the reconciliation event.
Delete Event (Yes/No flag)	This display-only field indicates if this is a delete event, that is, the corresponding record has been deleted from the target resource or the trusted source. A value of **Yes** indicates a delete event. If this event is associated with a user account on a target resource, the account is marked as revoked. If the event is associated with a user account, the account is deleted. **Note**: This field is set by Oracle Identity Manager.
Object Name	The target resource or trusted source that is associated with this reconciliation event. For trusted sources, this is the user.
For User/For Organization	Designates if the event for a resource object is associated with a user or organization record.

Field Name	Description
Status	The current status of the reconciliation event: ■ **Event Received**: Indicates that changes were received from the target resource or trusted source, for example, the CreateReconciliationEvent method has been called. The event has not yet received actual data from the target resource or trusted source. ■ **Data Received**: The data that the information from the target resource or trusted source was received. ■ **Users Matched**: The event matches one or more user records, based on reconciliation user-matching rules. ■ **Organizations Matched**: The event matches one or more organization records, based on reconciliation organization-matching rules. ■ **Processes Matched**: The event matches one or more provisioning processes, for example, all the values of key fields in the event match the values of those fields on the process' form. ■ **No Match Found**: Neither the values of key fields on provisioning process forms nor the criteria of any user or organization-matching rules match the event. The event has not been associated with a 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 that are associated with this resource were applied. ■ **Event Linked**: The event has been matched and linked to a particular user or organization record. ■ **Event Closed**: A user manually closed the event by clicking the Close Event button, without its data being linked to a record in Oracle Identity Manager. Once closed, a reconciliation event cannot be reopened. ■ **Required Data Missing**: At least one required data element is missing. If the data for any required fields on the resource definition is not available in the event, this message appears.
Event Date	The date and time that this event was received.
Assigned to User	The user to whom this event has been assigned.
Assigned to Group	The user group to which this event has been assigned.
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 event is linked.
Organization Name	The Oracle Identity Manager ID of the organization record that the event is linked to. 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 that is linked to the event.
Process Descriptive Data	Instance-specific descriptive data for the provisioning process that is defined in the Map Descriptive Field pop-up window in the Process Definition form.
Close Event	This button closes the reconciliation event. If the event is closed, no additional matching attempts or linking can be performed on it.

Field Name	Description
Re-apply Matching Rules	This button reapplies the reconciliation matching rules. This includes both process data and user- or organization-matching rules that are associated with the resource object. If Oracle Identity Manager is not generating satisfactory matches, you can amend and re-apply the resource's reconciliation matching rules, or you can amend the mappings for the provisioning process. Re-applying these rules after editing them may cause different records to appear 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 more likely to be accurate.
Create Organization (Only available on events related to the trusted source)	You use this button to create an organization record in Oracle Identity Manager based on the information in the reconciliation event. Only click this button 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)	You use this button to create a user record in Oracle Identity Manager based on the information in the reconciliation event. Only click this button when you are certain that the reconciliation event represents the creation of a new user on the trusted source.

Viewing and Managing Reconciliation Events

The following procedure describes how to view and manage reconciliation events.

> **Note:** Depending on how you define your reconciliation action rules, Oracle Identity Manager can 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.

To view and manage reconciliation events:

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

   You can also query reconciliation events by their associated resource in the **Object Name** field or status in the **Status** field.

   If you are querying a deleted event, that is, the corresponding record was deleted from the target resource or the trusted source, the **Yes** option for the **Delete Event** flag is selected. Otherwise, the **No** option is selected.
3. After locating the desired reconciliation event, use the tabs of this form to:
   - Correct any unprocessed data.
   - Browse and link to matching provisioning process form instances, or user or organization record candidates.
   - View the audit history of the event.

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

   - L**ink the reconciliation event to a particular provisioning process, user or organization**: This assumes that the event is associated with an existing user or organization record.

To do this, click the **Link** button on the applicable tab. Or, 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 if the event represents the creation of a new user on the trusted source.

  To do this, click the **Create User** button. Or, 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 if the event represents the creation of a new organization on the trusted source.

  To do this, click the **Create Organization** button. Or, 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**: These are rules associated with this resource. Then re-apply the rule to generate more accurate matches.

  To do this, refine the applicable reconciliation rule, save it, then click the **Re-apply Matching Rules** button.

Note: If you refine a reconciliation rule and reapply it or choose to create or link a user or provisioning process or organization, these actions are logged in 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

After locating the reconciliation event that you want to examine, you can use tabs to do the following:

- View any processed or unprocessed data in the event
- View provisioning process, user, or organization matches that were generated
- Link the event to the appropriate record or create a new user

Reconciliation Data Tab

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

Processed Data

The fields in the Processed Data branch are defined on the Reconciliation Fields tab of the associated resource. In the reconciliation event, these fields have been successfully processed, for example, they have not violated any data type requirements. For each successfully processed field, the following is 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 or 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 in its sub-branch) will each have their own values.

Unprocessed Data

The fields listed in the Unprocessed Data branch are reconciliation event items that could not be processed. For example, these can be items that were not defined or that conflicted with the data type set on the Reconciliation Fields tab of the associated resource. For each unprocessed field, the following information appears:

- 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 or 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	The field value is a multi-valued attribute. Only the component fields of a multi-value attribute, not the multi-value field itself, can accept values.
NOT NUMERIC	A numeric field value 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 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 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	This applies only to fields of type multi-value. One or more of the multi-value field's component (child) fields' data is not linked to reconciliation fields.
TABLE ATTRIBUTE LINKAGE MISSING	This applies only to fields of type multi-value. Some of the 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 that this event field was 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 does not attempt to match processes for target resources, or users or organizations for trusted sources, until all fields that were set as required on the Reconciliation Fields tab of the associated resource are successfully processed.

Mapping or Correcting Unprocessed Fields

Use the following procedure to correct or map unprocessed fields in the reconciliation event to the relevant fields as defined on the applicable resource.

To map or correct unprocessed fields:

1. Double-click the unprocessed field.

   For a multi-value field, you may need to map it to the appropriate child process form or check the individual component field.

   For multi-value fields, double-click and correct the component fields.

   The Edit Reconciliation Field Data dialog box appears.

   > **Note:** To map an unprocessed multi-valued component field to one of the multi-valued 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, click **OK**, 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 in the Unprocessed Data branch is updated to reflect the field to which it was linked. A new entry for the field is added to the Processed Data branch.

After the required data elements (on the Object Reconciliation tab of the applicable resource definition) in the reconciliation event are marked as processed on the Reconciliation Data tab, Oracle Identity Manager displays the following:

- For trusted sources:

  All user or organization records that match the relevant data in the reconciliation event, as specified in the logic of all applicable user or organization-matching reconciliation rules that are associated with the resource. These candidates represent accounts on the trusted source for which a potential owner was found in Oracle Identity Manager (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 (that is, 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 in the reconciliation event. This represents an account in the target system for which a possible matching account was found in Oracle Identity Manager (account update).

  If no processes instances match these values, Oracle Identity Manager evaluates the applicable user- or organization-matching reconciliation rules and displays users or organizations that match 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 in Oracle Identity Manager, that is, Oracle Identity Manager is not aware that the user was provisioned with an account on that system, but did find potential owners of the account (account creation). If more than one matching candidate is found, you will usually want an administrator to examine the records and decide which Oracle Identity Manager account to link it to. If no matches are found, there may be a mismatch between the data in your trusted source and the target application. This event may represent a rogue account on the target system or an existing employee was provisioned with a new account on the target system. However, Oracle Identity Manager is unable to decide which user that account is associated with.

Processes Matched Tree (for target resources only)

After all required fields defined on the Reconciliation Fields tab of the associated resource have been processed, the tab displays all provisioning process form instances where the values of all key fields match the values for all key fields in the reconciliation event.

> **Note:** This only occurs for reconciliation events that are associated with target resources. Since the trusted source is linked to the user resource or Organization and its provisioning process, it cannot have a custom process form. As a result, it cannot possess the matches required to populate this tab. For trusted sources, after all required fields are processed, Oracle Identity Manager proceeds immediately to evaluating the user or organization matching rules.

For each matched provisioning process, the following 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. That is, the user who was provisioned with the resource by that instance of the provisioning process.

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

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

If no provisioning processes are listed on this tab, Oracle Identity Manager was unable to match any values in the key fields in the reconciliation event to any values for fields

in process form instances associated with that resource. If this occurs, Oracle Identity Manager then attempts to apply any user- or organization-matching rules that are defined for the resource. If matches are found, they appear on the **Matched Users or Matched Organizations** tab.

Linking a Provisioning Process Instance to the Reconciliation Event

To link a provisioning process instance to the reconciliation event:

1. After you have determined which provisioning process instance to link to the reconciliation event, select it and click **Establish Link**.
2. Oracle Identity Manager updates the relevant process form instance with the information in the reconciliation event according to the mappings defined on the relevant provisioning process.

   It also inserts the **Reconciliation Update Received** task in that process.

Matched Users Tab

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

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

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

For each matching record, Design Console displays the user's ID, first name, and last name.

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

Linking a User Record to the Reconciliation Event

The following procedure describes how to link a user record to a reconciliation event.

> **Note:** The following procedure assumes a record exists. 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 creates a new user record using the information in the reconciliation event.

To link a user record to a reconciliation event:

1. Determine the 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, suppresses 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 instance of the user provisioning process for the user record that the reconciliation event is linked to.

Matched Organizations Tab

This tab displays Oracle Identity Manager organization records that match the data in the reconciliation event, as specified the resource's reconciliation rules.

For trusted sources, Oracle Identity Manager evaluates these rules and displays matching organization records as soon as all required fields (as defined on the Reconciliation Fields tab of the associated resource) are processed.

For target resources, Oracle Identity Manager evaluates these rules and displays matching organization records only after all required fields (as defined on the Reconciliation Fields tab of the associated resource) are processed and no matches have been generated on the Processes Matched Tree tab.

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

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

Linking an Organization Record to the Reconciliation Event

The following procedure describes how to link an organization record to a reconciliation event.

Note: The following procedure assumes a record already exists. In the following procedure, 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 creates a new organization record using the information in the reconciliation event.

To link an organization record to a reconciliation event:

1. After you determine what organization to link to the reconciliation event, select it and click **Link**.

2. If the reconciliation event is for a target resource, Oracle Identity Manager does the following:

   - Creates an instance of the resource's provisioning process for the selected organization, suppresses any adapters associated with the process' tasks, automatically 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 the reconciliation event is for a trusted source, Oracle Identity Manager does the following:

   - 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 that the reconciliation event is linked to.

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 is listed. Oracle Identity Manager tracks and logs the following reconciliation event actions:

- **Event Received**: This action is logged when Oracle Identity Manager receives a reconciliation event.
- **Data Sorted**: The action is logged when the data in a reconciliation event is sorted into processed and unprocessed fields.
- **Rules Reapplied**: The action is logged when a user clicks 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 values of key fields in the reconciliation event.
- **Users Matched**: The action is logged when one or more user records are matched with data in the reconciliation event using user-matching reconciliation rules.
- **Organization Matched**: The action is logged when one or more Oracle Identity Manager organization records are matched with data in the reconciliation event using organization-matching reconciliation rules.
- **Linked to User**: The action is logged when the data in the reconciliation event is linked to a particular user.
- **Linked to Organization**: The action is logged when the data in the reconciliation event is linked to a particular organization.

6

Resource Management

This chapter describes resource management in Design Console. It contains the following topics:

Overview

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

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

> **See also:** This chapter discusses prepopulating adapters and Java tasks. To learn more about adapters and adapter tasks, see the *Oracle Identity Manager Tools Reference Guide*.

The IT Resources Type Definition Form

The IT Resources Type Definition form is in the Resource Management folder. You use the IT Resources Type Definition form to classify IT resource types, for example, AD, MS Exchange, Solaris. Oracle Identity Manager associates resource types with resource objects that it provisions to users and organizations.

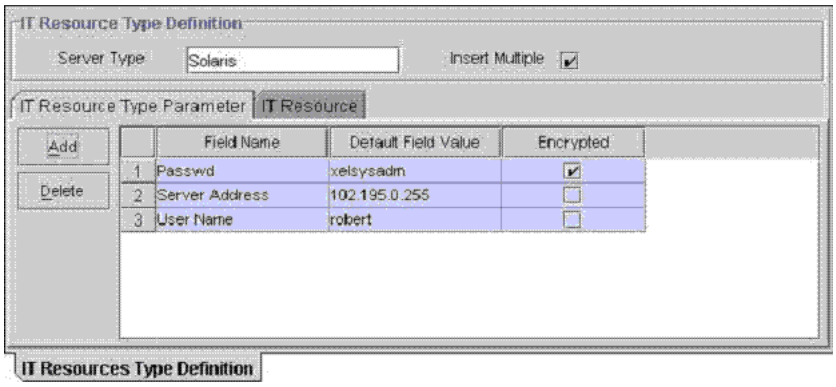
After you define an IT resource type on this form, it becomes available for selection when you define a resource. The type appears in the **Type** field on the IT Resources form.

IT resource types serve as templates for the IT resource definitions that reference them. If an IT resource definition references an IT resource type, the resource inherits all of the parameters and values in the IT resource type. The IT resource type serves as the general IT classification, for example, Solaris. The resource is an instance of the type, for example, Solaris for Statewide Investments.

You must associate every IT resource definition with an IT resource type.

The IT Resources Type Definition form is shown in Figure 6–1.

Figure 6–1 The IT Resources Type Definition Form



The following table describes the fields of the IT Resources Type Definition form.

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

Note: If an IT resource must access an external resource, but it cannot reach that resource using the network, you must associate it with a remote manager. For more information, see the *Oracle Identity Manager Tools Reference Guide*.

Defining a Template (a Resource Type) for IT Resources

The following procedure describes how to define an IT resource type.

To define an IT resource type:

1. Enter the name of the IT resource type in the **Server Type** field, for example, Solaris.
2. To make the IT resource type available for multiple IT resources, check the **Insert Multiple** checkbox.

3. Click **Save**.

   The IT resource type is defined. You can select it from the **Type** field when defining IT resources in the IT Resources form.

Tabs on the IT Resource Type Definition Form

After you save the basic information for a new IT resource type, and when an IT resource type is returned on a query, the fields on the tabs of the IT Resources Type Definition form's lower region are enabled.

The IT Resources Type Definition form contains the following tabs:

- IT Resource Type Parameter tab
- IT Resource tab

IT Resource Type Parameter Tab

You use the IT Resource Type Parameter tab to specify default values and encryption settings for all connection parameters for the IT resource type, as shown in Figure 6–1. Parameters and values on this tab are inherited by all IT resources that reference this IT resource type.

When you define a new parameter, the parameter and its values and encryption settings are added to the current IT resource type and to any new or existing IT resource definitions that reference this IT resource type. For any applicable resource definition, the new parameter appears in the **Parameters** tab of the IT Resources form.

Note: You can customize the values and encryption settings for these parameters within each IT resource.

Adding a Parameter to an IT Resource Type

The following procedure describes how to add a parameter to an IT Resource Type.

To add a parameter to an IT Resource Type:

1. Click **Add**.

   A new row appears in the **IT Resource Type Parameter** tab.

2. In the **Field Name** field, enter the name of the parameter.

3. In the **Default Field Value** field, enter a default value.

   This value is inherited by all IT resources that reference this IT resource type

4. Select or clear the **Encrypted** checkbox.

   This checkbox determines if this parameter's value is be masked, that is, represented with **** symbols, in a form field.

   If you want the parameter's value to be masked, select this checkbox.

5. Click **Save**.

Removing a Parameter From an IT Resource Type

The following procedure describes removing a parameter from an IT Resource Type.

To remove a parameter from an IT Resource Type:

1. Highlight the parameter you want to remove.

2. Click **Delete**.

   The parameter and its associated value are removed from the IT resource type and from IT resource definitions that reference this type.

IT Resource Tab

This tab displays IT resources that reference a selected IT resource type. All IT resources on this tab share the same parameters, but the values can be unique 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. You use this form to view and configure IT resources. IT resource definitions usually represent hardware, for example, a server or a computer where one or more resources reside. Each IT resource definition represents an instance of an IT resource type.

During a provisioning event, resource objects reference IT resource definitions. The definition specifies where the resource is located and how to connect to it. A resource object must be associated with an IT resource definition.

You can map the variables of an Oracle Identity Manager adapter to the values of any parameters for an IT resource. The parameters can represent information about the hardware, for example, a server domain name or the ID of the user who accesses this IT resource.

> **See also:** For more information about adapters and their mappings, see the *Oracle Identity Manager Tools Reference Guide*.

The following table describes the fields of the IT Resources form.

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

Defining an IT Resource

The following procedure describes how to define an IT Resource.

To define an IT Resource:

1. Enter the name of the IT resource in the **Name** field.
2. Double click the **Type** lookup field, and in the Lookup dialog box, select the IT resource type to associate with this IT resource.

   You define the IT resource types using the IT Resource Type definition form.
3. Click **OK**.
4. If the IT resource is to be accessed using a remote manager, that is, if the IT resource type was defined as a remote manager, double-click the **Remote Manager** lookup field, and in the Lookup dialog box select a remote manager.

   If the IT resource will not be accessed using a remote manager, proceed to Step 6.
5. Click **OK**.
6. Click **Save**

   The saved IT resource appears on the **IT Resource** tab of the IT Resources Type Definition form for the associated IT resource type. The parameters and default values for the IT resource classification type appear in the **Parameters** tab.
7. Optionally, to specify IT resource-specific values for the parameters on the **Parameters** tab, select the **Value** field for the parameter you want to edit, enter the new value, and click **Save**.

Setting Access Permissions to an IT Resource Instance Parameter

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

To set access permissions:

1. Click the **Administrators** tab.

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

   For example, you can assign **G2** as an administrative group for the **ramone** IT Resource instance.
3. Click a checkbox for the following permissions:

Permission	Description
Read	When checked, the administrative group indicated by the Group Name can read the current IT Resource Instance.
Write	When checked, the corresponding Group Name can read and modify the current IT Resource Instance parameter values.
Delete	When checked, the associated administrative group can delete the current 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. A rule can be assigned to a specific resource object or process, or a rule can apply to all resource objects or processes.

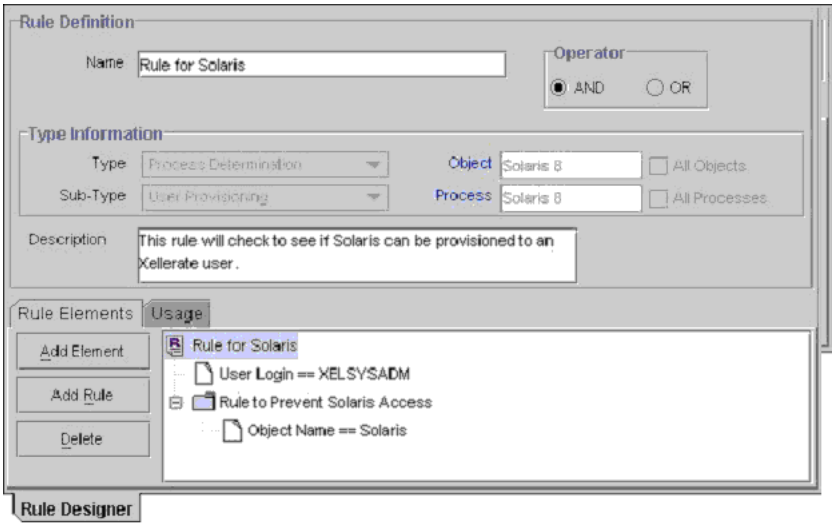
The following are examples of rule usage:

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

> **Tip:** For more information about prepopulate adapters, see the *Oracle Identity Manager Tools Reference Guide*.

The Rule Designer form shown in Figure 6–2 is located in the Resource Management folder. You use this form to create and manage rules that are used with resources.

Figure 6–2 Rule Designer Form



There are four types of rules:

General: Enables Oracle Identity Manager to add a user to a user group automatically and to determine the password policy that is assigned to a resource object.

Process Determination: Determines the approval process for a request, and the approval and provisioning processes for a resource object.

Task Assignment: Specifies the user or user group that is assigned to a process task.

Prepopulate: Determines what prepopulate adapter is executed for a form field.

A rule contains the following items:

A rule element: Consists of an attribute, an operator, and a value. In Figure 6–2, the attribute is **User Login**, the operator is **==**, and the value is **XELSYSADM**.

A nested rule: If one rule must be placed inside another rule for logic purposes, the internal rule is known as a nested rule. In Figure 6–2, a **Rule to Prevent Solaris Access** is nested in a **Rule for Solaris**.

An operation: When a rule contains multiple rule elements or nested rules, an operation shows the relationship among the components. In Figure 6–2, if the **AND**

operation is selected, 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.

The following table describes the fields of the Rule Designer form.

Field Name	Description
Name	The rule's name.
AND/OR	These radio buttons specify the operation for the rule. To stipulate that a rule is successful only when all the outer rule elements and nested rules are true, select the **AND** radio button. To indicate that a rule is successful if any of its outer rule elements 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. In 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 within the **Rule to Prevent Solaris Access** rule.
Type	The rule's classification status. A rule can belong to one of four types: ■ **General**: Enables Oracle Identity Manager to add a user to a user group automatically and determines the password policy that is assigned to a resource object. ■ **Process Determination**: Determines the standard approval process that is associated with a request, and the approval and provisioning processes that are selected for a resource object. ■ **Task Assignment**: Determines what user or user group is assigned to a process task. ■ **Prepopulate**: Determines what prepopulate adapter is used for a form field.
Sub-Type	A rule of type **Process Determination**, **Task Assignment**, or **Prepopulate** can be categorized into one of four sub-types: ■ **Organization Provisioning**: Classifies the rule as a provisioning rule. It determines the organization for which a process is provisioned, a task is assigned, or the prepopulate adapter is applied. ■ **User Provisioning**: Classifies the rule as a provisioning rule. It is used to determine the user for which a process is provisioned, a task is assigned, or a prepopulate adapter is applied. ■ **Approval**: Classifies the rule as an approval rule. It is used to approve the provisioning of resources to users or organizations. ■ **Standard Approval**: Classifies the rule as a standard approval rule. It is used to approve a request. For **Task Assignment** or **Prepopulate** rule types, the Approval and Standard Approval items do not appear in the **Sub-Type** box. The **Sub-Type** box is disabled for a **General** rule type.
Object	The resource object that this rule is assigned to.
All Objects	If you select this check box, the rule can be assigned to all resource objects.
Process	The process that this rule is assigned to.
All Processes	If you select this check box, the rule can be assigned to all processes.

Field Name	Description
Description	Explanatory information about the rule.

Creating a Rule

The following procedure describes how to create a rule.

> **Caution:** In the following procedure, note that the radio buttons do not apply to rule elements within nested rules. For example, in Figure 6–2 the **AND** operation applies to the **User Login==XELSYSADM** rule element and the **Rule to Prevent Solaris Access** nested rule. But this operation has no bearing on the **Object Name != Solaris** rule element in the **Rule to Prevent Solaris Access** rule.

To create a rule:

1. Open the Rule Designer form.
2. In the **Name** field, enter the name of the rule.
3. To stipulate that a rule is successful only when all of its rule elements or nested rules are true, select the **AND** radio button.

   To indicate that a rule is successful if any of its rule elements or nested rules are true, select the **OR** radio button.
4. Click the **Type** box, and in the custom menu select the classification status (**General**, **Process Determination**, **Task Assignment**, or **Prepopulate**) to associate with the rule.

   For **Process Determination**, click **Sub-Type** and select the classification status (**Organizational Provisioning**, **User Provisioning**, **Approval**, or **Standard Approval**) to associate with the rule.

   For **Task Assignment** or **Prepopulate**, click **Sub-Type** and select the classification status (**Organization Provisioning** or **User Provisioning**) to associate with the rule.

   If you select **General** from the **Type** box, proceed to Step 7.
5. To associate the rule with a single resource object, double-click the **Object** lookup field, and in the Lookup dialog box select a resource object.

   If you want the rule to be accessible to all resource objects, select the **All Objects** check box.
6. To assign a rule to one process, double-click the **Process** lookup field, and from the Lookup dialog box select the process to associate with the rule.

   > **Caution:** The only processes that appear in this Lookup window are ones that are associated with the resource object you selected in Step 5.

   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 5 by selecting the **All Processes** check box, this rule is accessible by every process that is associated with the selected resource object.

7. In the **Description** field, enter explanatory information about the rule.
8. Click **Save**.

   The rule is created and the tabs of this form become functional.

Tabs on the Rule Designer Form

After 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:

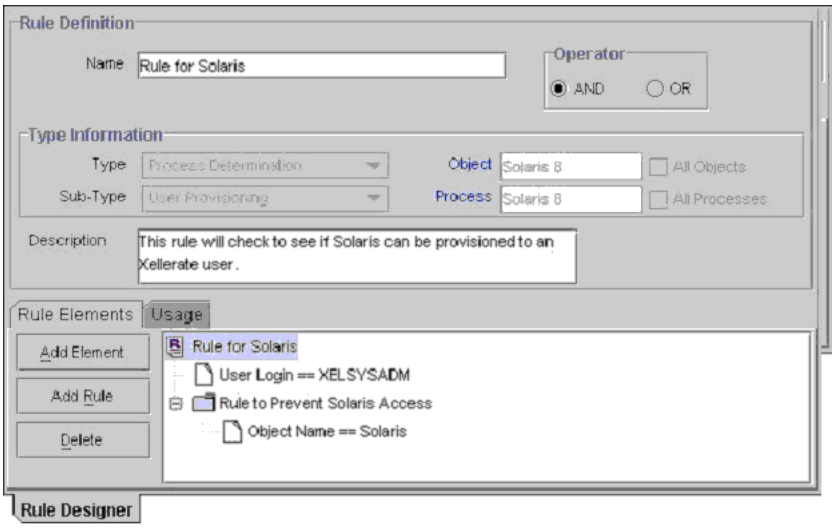
- Rule Elements tab
- Usage tab

Each of these tabs is discussed in the following sections.

Rule Elements Tab

From this tab, you can create and manage elements and nested rules for a rule. For example, in Figure 6–3, the **Rule for Solaris** contains the **User Login==XELSYSADM** rule element. It also has a nested **Rule to Prevent Solaris Access**. 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



The rule in Figure 6–3 can be applied to a provisioning process for the Solaris resource object. After this resource object is assigned to a request, the rule is triggered. If the target user's login is **XELSYSADM**, and the name of the resource object is **Solaris**, the Solaris resource object is 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 describe 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

Adding a Rule Element to a Rule

The following procedure describes how to add a rule element to a rule.

To add a rule element to a rule:

1. Click **Add Element**.

   The Edit Rule Element dialog box appears.

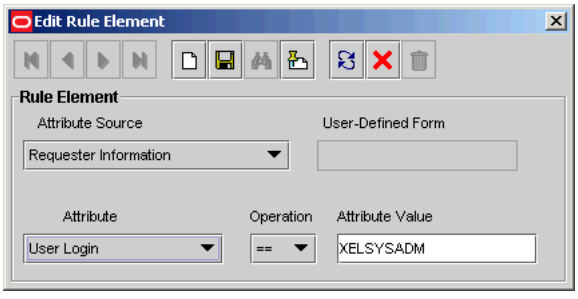
   The custom menus in the boxes on the Edit Rule Element dialog box reflect the items in the **Type** and **Sub-Type** boxes of the Rule Designer form.

   The following table describes the data fields in the Edit Rule Element dialog box.

Name	Description
Attribute Source	From this 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 in the adjacent box. **Note**: If Object Data or Process Data do not appear in the **Attribute Source** box, the **User-Defined Form** field will be empty.
Attribute	From this box, select the attribute for the rule.
Operation	From this 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.

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

Figure 6–4 Edit Rule Element Window -- Filled



In this example, if the Login ID of the target user is **XELSYSADM**, the rule element is true. Otherwise, it is false.

> **See also:** For more information on what parameters to select, see "Rule Elements Tab" on page 6-9.

3. From the Toolbar of the Edit Rule Element dialog box, click **Save**, then click **Close**.

   The rule element appears in 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.

Adding a Nested Rule to a Rule

The following procedure describes how to nest a rule within a rule.

> **Caution:** In the following procedure only rules of the same type and sub-type as the parent rule appears in the Select Rule window.

To add a nested rule:

1. Click **Add Rule**.

   The Select Rule dialog box appears.

2. Select the desired nested rule and click **Save**.

3. Click **Close**.

   The nested rule appears in 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.

Removing a Rule Element or Nested Rule From a Rule

The following procedure describes removing a rule element or a nested rule.

To remove a rule element or nested rule from a rule:

1. Highlight the rule element or nested rule that you want to remove.

2. Click **Delete**.

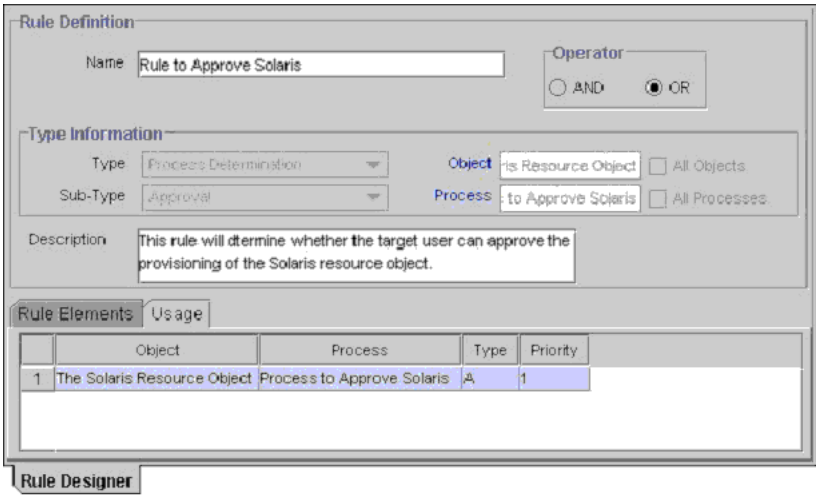
   The rule element or nested rule is removed from the rule.

Usage Tab

This tab appears on the Rule Designer form. The information in the Usage tab reflects the rule's classification type. For example, if a rule type is **Pre-Populate**, the user-created field that this rule is applied to appears in this tab.

Figure 6–5 illustrates the Usage tab.

Figure 6–5 Usage Tab of the Rule Designer Form



This tab displays the following items:

- The password policy, resource object, process, process task, auto-group membership criteria, user group, Oracle Identity Manager form field, and pre-populate adapter associated with a rule.
- A one-letter code, signifying the rule's classification type (A=Approval, P=Provisioning).

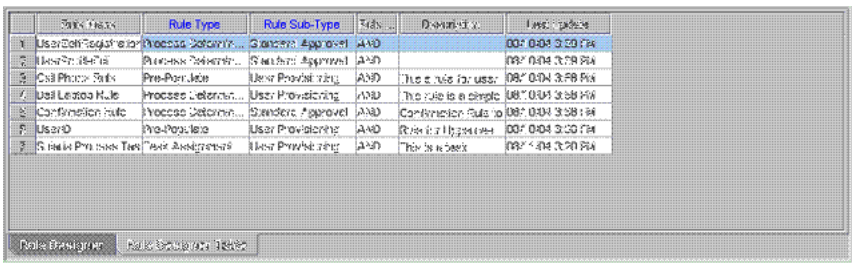
  This code appears for process determination rules only.
- The rule's priority number.

In Figure 6–5, the **Rule to Approve Solaris** 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**. 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 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	The name of the rule.
Rule Type	A rule can belong to one of four types: ■ **General**: Enables Oracle Identity Manager to add a user to a user group automatically and determines the password policy that is assigned to a resource object. ■ P**rocess Determination**: Determines the standard approval process that is associated with a request, and the approval and provisioning processes that are selected for a resource object. ■ T**ask Assignment**: Determines what user, user group, or both are assigned to a process task. ■ **Pre-Populate**: Determines what pre-populate adapter is executed for a given form field.
Rule Sub-Type	A rule of type **Process Determination**, **Task Assignment**, or **Pre-Populate** can be categorized into one of four sub-types: ■ **Organization Provisioning**: Classifies the rule as a provisioning rule. You use this to determine the organization for which a process is provisioned, a task is assigned, or the pre-populate adapter is applied. ■ **User Provisioning**: Classifies the rule as a provisioning rule. You use this to determine the user for which a process is provisioned, a task is assigned, or a pre-populate adapter is applied. ■ **Approval**: Classifies the rule as an approval rule. It is used to approve the provisioning of resources to users or organizations. ■ **Standard Approval**: Classifies the rule as a standard approval rule. It is used to approve a request.
Rule Operator	The relationship between the attribute and the attribute value (**==** or **!=**)
Description	Explanatory information about the rule.
Last Updated	The date when the rule was last updated.

The Resource Objects Form

The Resource Objects form is located in the Resource Management folder. You use this form to create and manage the resource objects for the Oracle Identity Manager resources that you want to provision for organizations or users. Resource object definitions serve as templates when provisioning the resource. However, how the resource is approved and provisioned depends on the design of the approval and provisioning processes that you link to the resource object.

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 that is associated with this resource. (This is actually the name of the table that represents the form.)
Order For User/Order For Organization	Use these radio buttons to determine if 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 will be populated by Oracle Identity Manager or a user. This applies to the following kinds of forms: ■ Forms that are associated with the resource object ■ Forms with fields that have pre-populate adapters attached to them If the **Auto Pre-Populate** check box is selected, after the associated custom form appears, the fields with pre-populate adapters are populated with data. If this check box is cleared, a user must populate the fields by clicking the **Pre-Populate** button on the toolbar. **Important**: This setting does not control the triggering of the pre-populate adapter. It determines if the contents resulting from the execution of the adapter appear in 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**: 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 contains business-related processes. ■ **System**: Oracle Identity Manager uses this type of resource object internally. **Do not** modify system resource objects without first consulting Oracle.
Allow Multiple	Designates if the resource may be provisioned more than once to a user or organization. If it is selected, the resource object can be provisioned more than once per user or organization.
Auto Save	By selecting this check box, Oracle Identity Manager saves the data in any resource-specific form that was 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. This is required because the user will not be able to access the form. **Note**: This checkbox is only relevant if you have created a form for the provisioning of the resource object.

Field Name	Description
Self Request Allowed	By selecting this check box, users as well as the System Administrator can request the resource object for themselves. **Note**: This functionality only applies to Oracle Identity Manager Design Console. It is not applicable to 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 automatically initiates the provisioning process when 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.

Creating a Resource Object

The following procedure describes how to create a resource object.

To create a resource object:

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, select the table that represents the form that will be associated with the resource object.
4. 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.

   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**) to associate 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 be unable to access the form.

Set this checkbox only if you have created a form for provisioning the resource object.

---

9. If you want the System Administrator to be able to request the resource object for himself or herself, select the **Self Request Allowed** check box.

   Otherwise, proceed to Step 10.

10. To provision the resource object 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 sets all resource objects to Auto Launch, even though this checkbox is cleared.

---

12. To restrict the user groups that can provision this resource object to groups that appear in the **Object Authorizers** tab of the Resource Objects form, select the **Provision by Object Admin** Only check box.

This applies to resource objects that are provisioned directly or by assignment to a request.

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:

- Depends On Tab
- Object Authorizers Tab
- Process Determination Rules Tab
- Event Handlers and Adapters Tab
- Status Definition Tab
- Administrators Tab
- Password Policies Rule Tab
- User-Defined Fields Tab
- Process Tab
- Object Reconciliation Tab

Depends On Tab

From this tab, you can select resource objects that Oracle Identity Manager must provision before provisioning the current resource object. If Oracle Identity Manager can provision the current resource object without first provisioning a resource object that appears in the **Depends On** tab, you must remove that resource object from the tab.

The following topics are related to the Depends On tab:

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

Selecting a Dependent Resource Object

The following procedure describes how to select a dependent resource object.

To select a dependent resource object:

1. Click **Assign**.

   The Assignment dialog box appears.

2. Select the resource object, and assign it to the request.

3. Click **OK**.

   The dependent resource object is selected.

Removing a Dependent Resource Object

The following procedure describes how to remove a dependent resource object.

To remove a dependent resource object:

1. Highlight the dependent resource object that you want to remove.
2. Click **Delete**.

   The resource object is removed from the **Depends On** tab.

Object Authorizers Tab

Use this tab to specify user groups that are the Object Authorizers for this resource. You can select users who are members of the Object Authorizers groups as targets for task assignments.

Each user group on the Object Authorizers tab has a priority number. When a task assignment target is **Object Authorizer user with highest priority**, Oracle Identity Manager uses the priority number to determine what user to assign to a task. The priority number can also be referenced when a task assigned to a group is escalated due to lack of action. You can increase or decrease the priority number for any user group on this tab.

For example, suppose that you configure members of the SYSTEM ADMINISTRATORS user groups to be Object Authorizers. Also suppose that 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 the user does not complete the process task in a user-specified time, Oracle Identity Manager reassigns the task to the user with the next highest priority in the SYSTEM ADMINISTRATORS group.

> **See also:** For more information on task assignment rules and process tasks, see "The Rule Designer Form" on page 6-5 and "Assignment Tab of the Editing Task Window" on page 7-31.

The following sections discuss the following:

- Assigning a user group to a resource object
- Removing a user group from a resource object
- Changing the priority number for a user group

Assigning a User Group to a Resource Object

The following procedure describes how to assign a user group to a resource object.

To assign a user group to a resource object:

1. Click **Assign**.

   The Assignment dialog box appears.
2. Select a user group, and assign it to the resource object.
3. Click **OK**.

   The user group is selected.

Removing a User Group From a Resource Object

The following procedure describes how to remove a user group from a resource object.

To remove a user group from a resource object:

1. Highlight the desired user group.
2. Click **Delete**.

   The user group is removed from the **Object Authorizers** tab.

Changing a User Group's Priority Number

The following procedure describes changing a user group's priority number.

To change a user group's priority number:

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.**

   To increase or decrease a user group's priority number by more than one, click the appropriate button repeatedly. For 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 changed to the value you selected.

Process Determination Rules Tab

A request is a mechanism for provisioning resources to users or organizations. A user interacts with a request to approve the provisioning of resources to target users or organizations. Each request must have a resource object assigned to it. Each resource object consists of one or more provisioning processes and one or more approval process.

A resource object acts as a template when the resource is provisioned to users or organizations. This template can be linked to multiple approval and provisioning processes. Oracle Identity Manager uses process determination rules to select an approval and provisioning process when a resource is requested or directly provisioned.

Process determination rules provide the following criteria:

- What approval and provisioning process to select when a resource is requested
- What provisioning process to select when a resource is provisioned directly

Each approval process and provisioning process usually has a process determination rule. Each rule and process combination has a priority number that indicates the order in which Oracle Identity Manager will evaluate it.

If the condition of a rule is false, Oracle Identity Manager evaluates the rule with the next highest priority. If a rule is true, Oracle Identity Manager executes the process associated it. For example, when a resource is requested or provisioned directly, Oracle Identity Manager evaluates a **Rule to See if Solaris is Needed** and **Rule to Check Provisioning of Solaris for IT Dept**. Both rules have the highest priority. If the conditions of these rules are true, Oracle Identity Manager executes the processes associated with them—in this example, these are the **Check if Solaris is Needed** approval process and the **Provision Solaris for IT Dept**. provisioning process.

As a variation of the example, if the resource is requested or provisioned directly and the **Rule to Check Provisioning of Solaris for IT Dept**. rule is 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 **Provision Solaris for Devel**. provisioning process associated with that rule.

Adding a Process Determination Rule to a Resource Object

The following procedure describes how to add a process determination rule to a resource object.

To add a process determination rule to a resource object:

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. In the adjacent column, double-click the **Processes** lookup field.
6. From the Lookup dialog box, select the desired process, and assign it to the rule.
7. Click **OK**.
8. Enter a numeric value in the **Priority** field.

   This determines the order in which Oracle Identity Manager evaluates the rule and process combination.
9. Click **Save**.

   The rule and 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 and process combination.
2. Click **Delete**.

   The rule and process combination is removed from the resource object.

Event Handlers and Adapters Tab

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 that must be completed automatically.

When this occurs, you must assign 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.

When an event handler or adapter that 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 triggers the adapter, and the associated provisioning process is executed automatically.

Assigning an Event Handler or Adapter to a Resource Object

The following procedure describes how to assign an event handler to an adapter or 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 appears.

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 Tab

You use this tab to set provisioning status for a resource object. A provisioning status indicates the status of a resource object throughout its lifecycle, until it is provisioned to the target user or organization. You can view the provisioning status of a resource object from the **Status** region of the Currently Provisioned tab.

Every provisioning status of a resource object is associated with a task status for the relevant provisioning process. Oracle Identity Manager selects the provisioning process when the resource object is assigned to a request. For example, if the **Provision for Developers** process is selected, and a task in 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.

A resource object the following pre-defined statuses:

- **Waiting**: This resource object depends on other resource objects that have not yet been provisioned.
- **Revoked**: The resources represented by the resource object are provisioned to target users or organizations that have been permanently de-provisioned from using the resources.
- **Ready**: This resource object either does not depend on any other resource objects, or all resource objects upon which this resource object depends are provisioned.

  After a resource is assigned to a request and the resource object's status is **Ready**, Oracle Access Manager evaluates the process determination rules to determine the approval and provisioning processes. When this happens, the status of the resource object changes to **Provisioning**.
- **Provisioning**: The resource object is assigned to a request, and an approval process and a provisioning process have been selected.

- **Provisioned**: The resources represented by the resource object are 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 that 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 are provisioned to the target users or organizations and these users or organizations have access to the resources.
- **Disabled**: The resources represented by the resource object are provisioned to the target users or organizations, but these users or organizations have temporarily lost access to the resources.

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

For example, suppose that 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 there are, Oracle Identity Manager launches the approval and provisioning processes of the 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 sections discuss how to add a provisioning status to a resource object and remove a provisioning status from a resource object.

Adding a Provisioning Status to a Resource Object

The following procedure describes how to add a provisioning status to a resource object.

To add a provisioning status to a resource object:

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.

Removing a Provisioning Status from a Resource Object

The following procedure describes removing a provisioning status from a resource object.

To remove a provisioning status from a resource object:

1. Highlight the desired provisioning status.
2. Click **Delete**.

   The provisioning status is removed from the resource object.

Administrators Tab

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

When the **Write** check box is selected, the corresponding user group can modify the current resource object. When the **Delete** check box is selected, the associated user group can delete the current resource object.

For 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.

Assigning a User Group to a Resource Object

The following procedure describes how to assign a user group to a resource object.

To assign a user group to a resource object:

1. Click **Assign**.

   The Assignment dialog box appears.
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.

Removing a User Group from a Resource Object

The following procedure describes how to remove a user group from a resource object.

To remove a user group from a resource object:

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 Tab

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 evaluate the rule using the next highest priority. If this rule is true, Oracle Identity Manager applies 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.

Adding a Password Policy Rule to a Resource Object

The following procedure describes how to add a password policy rule to a resource object.

To add a password policy rule to a resource object:

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. In 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.

Removing a Password Policy Rule From a Resource Object

The following procedure describes how to remove a password policy from a resource object.

To remove a password policy rule from a resource object:

1. Highlight the desired password policy rule.
2. Click **Delete**.

   The password policy rule is removed from the resource object.

User-Defined Fields Tab

You use this tab to view and access user-defined fields that were created for the Resource Objects form. Once a user-defined field is created, it appears on this tab and can accept and supply data.

> **See also:** For instructions on how to create user-defined fields on existing Oracle Identity Manager forms, see "The User Defined Field Definition Form" on page 8-7.

Process Tab

The **Process** tab displays all approval and provisioning processes that are associated with the current resource object. The **Default** check boxes on this tab indicate what approval or provisioning processes are the defaults for the resource.

> **Note:** You create approval and provisioning processes and associate them 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 example, suppose that the **Solaris** resource object has one approval processes assigned to it and one provisioning processes (**Provision Solaris for Devel.**) associated with it. The **Provision Solaris for Devel**. has been designated as the default provisioning process for this resource object.

Object Reconciliation Tab

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 in 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
```

Adding a Reconciliation Field

The following procedure add a fields from the target system or trusted source to the list of fields that are to be reconciled with information in Oracle Identity Manager. For a trusted source, this must be the **user** resource definition.

> **Note:** Before Oracle Identity Manager can successfully perform reconciliation with an external target resource or 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.

To add a reconciliation field:

1. Click **Add Field**.

   The Add Reconciliation Field dialog box appears.

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 in 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 in a reconciliation event will not prevent matching from occurring.

5. Click **Save**.

   The field will be available for mapping in the resource's default provisioning process.

Deleting a Reconciliation Field

Use the following procedure to remove a target system field from the list of fields that are to be reconciled with information in Oracle Identity Manager. For a trusted source, this must be the **user** resource definition.

To delete a reconciliation field:

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 in 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

Rule Condition	Possible Rule Actions
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

See Also: "Assignment Tab of the Editing Task Window" on page 7-31 for a description of the classification types for the users and groups listed in the preceding table

Adding a Reconciliation Action Rule

The following procedure describes adding a reconciliation action rule

To add a reconciliation action rule:

1. Click **Add Field**.

   The **Add a new Action Rule** dialog box appears.

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.

Deleting a Reconciliation Action Rule

The following procedure describes deleting a reconciliation action rule

To 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 and 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 and 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 process management with Design Console. It contains the following topics:

Overview

The Process Management folder provides System Administrators with tools for creating and managing Oracle Identity Manager processes and e-mail templates.

This folder contains the following forms:

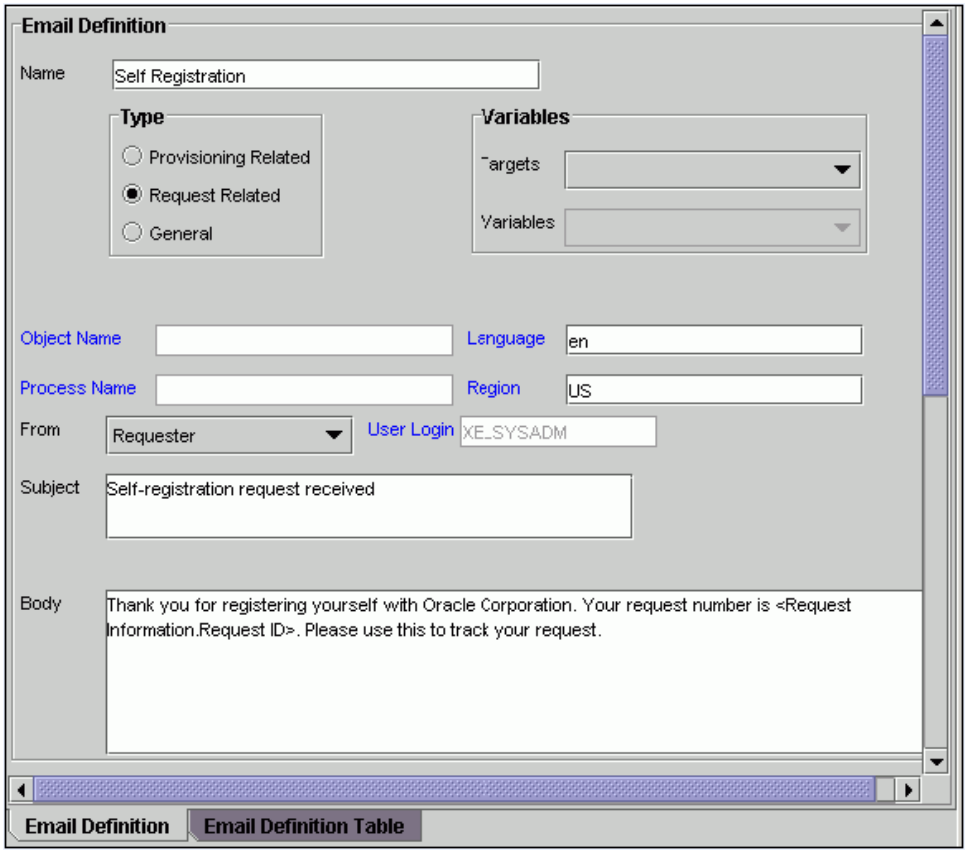
- **Email Definition**: This form enables a System Administrator to create templates for e-mail notifications.
- **Process Definition**: This form is used to create and manage approval and provisioning processes. It also allows you to launch the Workflow Definition Renderer that displays your workflow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

The Email Definition Form

The Email Definition form, as shown in Figure 7–1, is located in the Process Management folder. You use this form to create templates 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



You apply Email definitions through the **Assignment** tab of the Process Definition form.

In Figure 7–1, an email definition has been created. After the request represented by the **Request ID** email variable is approved, an email notification is sent from user **SOLO** to the user who created the request or to the requester.

Specifying the Email Server

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

> **Tip:** For more information, see "The System Configuration Form" on page 8-14, and "The IT Resources Form" on page 6-4.

To specify the email server:

1. Launch the System Configuration form.
2. Query for the **Email Server** property, and ensure that it is set to the name of the resource asset instance that represents your e-mail server.
3. Open the IT Resources form and query for the **Email Server** IT resource or another name for the resource asset that is associated with your mail server.
4. Once this IT resource appears, specify the IP address of the e-mail server and the name and password of the user who validates the usage of this server.

The Email Definition Form

The following table describes the fields of the Email Definition form.

Field Name	Description
Name	The name of the email definition.
Type	This region contains three radio buttons for the following: ■ Whether to categorize the email definition as related to a request or a provisioning process. ■ Whether to associate a variable for the email definition with a request or a provisioning process. ■ Whether to associate a variable for the email definition with a general process. To classify the email definition as a provisioning definition, or to associate the email variable with a provisioning process, select the **Provisioning Related** radio button. To categorize the email definition as a request definition, or to associate the email variable with a request, select the **Request Related** radio button. To categorize the email definition as a general announcement, 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 email definition is related. **Note**: Leave this lookup field empty to make the email definition 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 email 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.
Language	From this lookup field, select the language that is associated with the e-mail definition.
Region	From this lookup field, select the region that is associated with the language in the e-mail definition.
Targets	Select the source of the variable for the email 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 in this box reflect the radio button you select from the Type region.
Variables	From this box, select the variable for the email definition (for example, Request Name). The variables, which appear in this box, reflect the items you select from the Targets box. **Note**: For more information on e-mail variables and their parameters, refer to "EMail Variables" on page A-8.
From	Currently, two types of users can be selected from this box: ■ **Requester**: The user who created the request. ■ **User**: Any Oracle User with an email address, which appears in the **Contact Information** tab of their Users form.
User Login	The ID of the user in the From region of the email notification. **Note**: If the User item does not appear in the From box, the **User Login** field is disabled.

Field Name	Description
Subject	The title of the email definition.
Body	The content of the email definition.

Creating an Email Definition

The following procedure describes creating an email definition.

To create an email definition:

1. Open the Email Definition form.
2. In the **Name** field, type the name of the mail definition.
3. If the email definition is to be used with a provisioning process, select the **Provisioning Related** radio button. When the email 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 **Email Server** property on the System Configuration form.

4. Double-click the **Language** lookup field and select a language to associate with this e-mail definition.
5. Double-click the **Region** lookup field and select a region to associate with the e-mail definition language.

   Note: E-mail notification is based on the locale that was specified when you first installed Oracle Identity Manager.

6. Click **Save**.

   The remaining data fields of the Email Definition form are now operational.

7. To associate this email definition with a particular resource object, from the Lookup dialog box, double-click the **Object Name** lookup field and select the resource object that is associated with the provisioning process to which this e-mail definition is related.

   Leave this lookup field empty to make the email definition available for use with all resource objects.

8. Double-click the **Process Name** lookup field.

   From the Lookup dialog box, select a provisioning process that is assigned to the resource object you selected in Step 7. 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.

9. Click the **From** 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** box.

10. Optional. If you selected the User option in the **From** box, double-click the **User Login** lookup field.

    From the Lookup dialog box, select the ID of the user who appears in the From region of the email notification.

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

11. Add information in the **Subject** field.

    This field contains the title of the email definition.

12. Add information in the Body text area.

    This text area contains the contents of the email definition.

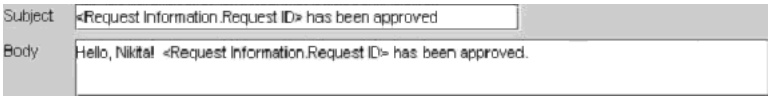
13. When necessary, populate the Subject field and Body text area with email variables.

    The following table describes the email variables that you can customize for the email definition.

Name	Description
Type	These radio buttons specify if a variable for the email definition will be related to a provisioning process or a request. To associate the email variable with a provisioning process, select the **Provisioning Related** radio button. To relate the variable to a request, select the **Request Related** radio button.
Targets	From this box, select the source of the variable for the email definition. For example if you want to use the **Request Name** variable, the source to select would be **Request Information**.
Variables	From this box, select the variable for the email definition, for example, **Request Name**.

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

14. Create an email 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.

15. Click **Save**.

    The email definition is created.

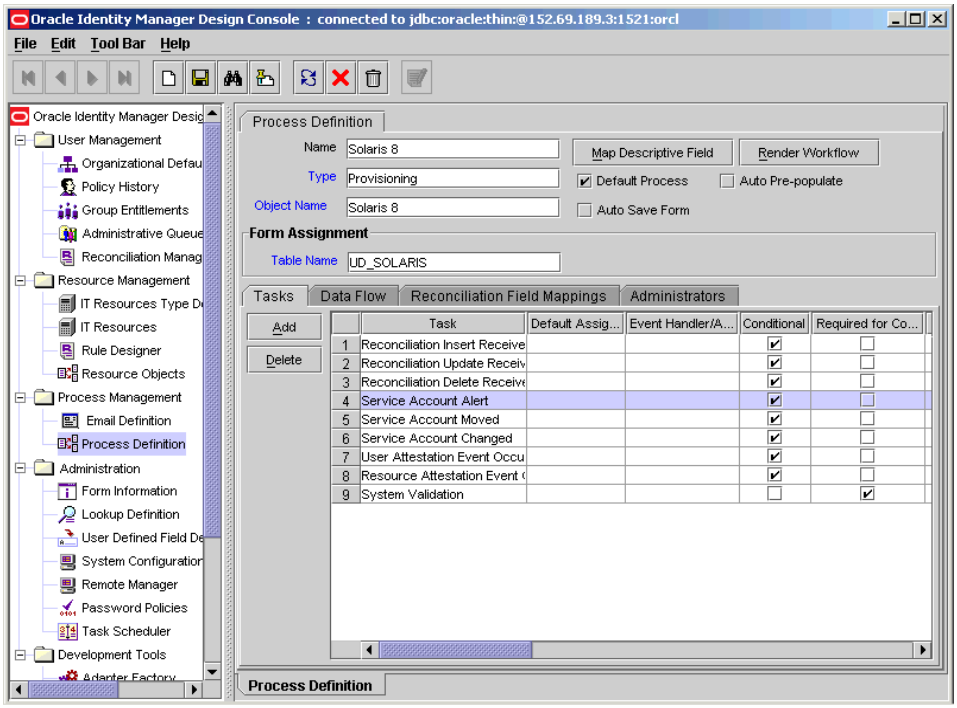
The Process Definition Form

A process is the mechanism for representing a logical workflow for approvals or provisioning in Oracle Identity Manager. Process definitions consist of tasks. Process tasks represent the steps that you must complete to fulfill the purpose of a process. For example, in an approval process, the tasks can represent individual approvals that are required for an action can take place. In a provisioning process, tasks are used to enable a user or organization to access the target resource.

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

Note: You can also use this form to manage the standard approval process associated with the Request object.

Figure 7–2 The Process Definition Form



In Figure 7–2, the **Solaris 8** provisioning process is created and assigned to the **Solaris 8** resource object.

The following table describes the fields of the Process Definition form.

Field Name	Description
Name	The name of the process.

Field Name	Description
Type	The classification type of the process definition. A process definition can be categorized as an Approval or a Provisioning process.
Object Name	The name of the resource object to which the process will be assigned.
Map Descriptive Field	Click this button to select a field that will be used as an identifier of the process definition after an instance is assigned to a resource object.
Render Workflow	Click this button to launch a web browser and display the current workflow definition using the Workflow Renderer tool.
Default Process	This check box determines if the current process is the default approval or provisioning process for the resource object with which it is associated. Select the check box to set the process 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. It will only be invoked if a process selection rule causes it to be chosen.
Auto Save Form	This check box designates 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. Select this check box to automatically save the data in the custom process form without 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. Clear this check box to 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 are populated by Oracle Identity Manager or a user. Two types of forms are affected: ■ Forms that are associated with the process ■ Forms that contain fields with pre-populated adapters attached to them 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, a user must populate these fields by clicking the **Pre-Populate** button on the toolbar or by manually entering the data. **Important**: This setting does not control the triggering of the pre-populate adapter. It only determines if the contents resulting from the execution of the adapter appear in the associated form field(s) because of Oracle Identity Manager or a user. For more information on pre-populate adapters, see the *Oracle Identity Manager Tools Reference Guide*. **Note**: 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 that represents the form that is associated with the process definition.

Creating a Process Definition

The following procedure describes how to create a process definition.

To create a process definition:

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 to make this the default approval or provisioning process for the resource object to which it is assigned.

   If you do not want the current process definition to be the default, proceed to Step 6.
6. Optional. Select the **Auto Save Form** check box to suppress the display of the provisioning process' custom form and automatically save the data in it.

   This setting is only applicable to provisioning processes.

   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, see the *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, see the *Oracle Identity Manager Tools Reference Guide*.

   ---
8. Double-click the **Table Name** lookup field.

   From the Lookup window that appears, select the table that represents the form associated with the process definition.
9. Click **Save**.

   The process definition is created and the **Map Descriptive Field** button is enabled. If you click this button, the Map Descriptive Field dialog box appears.

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 in this window and be available for selection.

10. click the **Render Workflow** button to 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

After 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 Tab
- Data Flow Tab
- Reconciliation Field Mappings Tab
- Administrators Tab

Each of these tabs is described in the following sections.

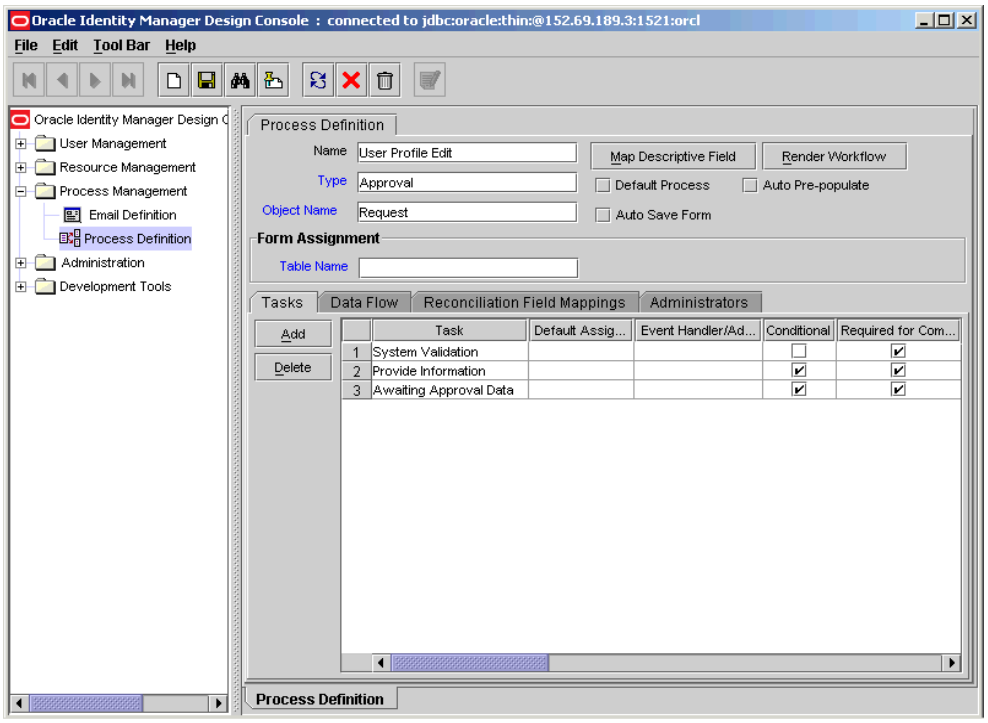
Tasks Tab

You use this tab 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)

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

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



For example, the **Solaris 8** process definition can consist of 15 process tasks.

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

Adding a Process Task

Process tasks represent the steps that you must complete in a process. The following procedure describes how to add a process task.

To add a process task:

1. Click **Add**.

   The Creating New Task dialog box appears.

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.

Editing a Process Task

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

Deleting a Process Task

To delete a process task:

1. Highlight the process task that you want to delete.

2. Click **Delete**.

The process task is removed from the process definition.

Data Flow Tab

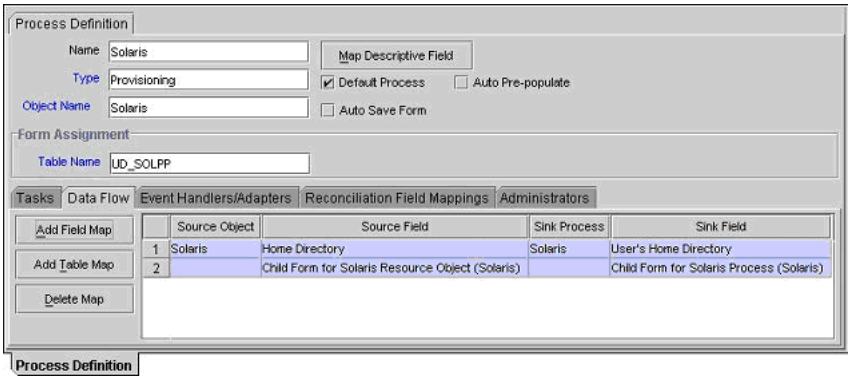
You use this tab to define the data flow between the following items:

- The fields of a parent resource form that is attached to a resource object definition and the fields of a parent process form that is attached to a provisioning process definition
- The fields of a parent resource form and the fields of a child of the parent process form.
- The fields of a child resource form and the fields of a child process form

This tab is relevant only if parent resource and process objects have custom resource forms attached to them.

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

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



To map the flow of data between the fields of a parent resource form and a child process form, or between the fields of a child resource form and a child process form, you must assign a child resource form to the custom resource form, and assign a child process form to the custom process form.

> **See also:** For more information on custom process or resource forms and assigning child forms to parent forms, see "The Form Designer Form" on page 9-2.

After you define a resource object form for the parent resource object and a process form for the parent provisioning process and assign child forms to each form, you can establish mappings between the form fields, with two restrictions. Field values on the process form cannot be mapped back to resource form fields, and field values on a child resource form cannot be mapped to fields in the parent process form.

Figure 7–4, shows two data flows:

- 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.

The following sections describe how to map the following:

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

The following also describes how to break the mapping between two data fields.

Mapping a Parent Resource Form Field to a Process Form Field

The following procedure describes how to 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:

1. Click **Add Field Map**.

   The Define Data Flow dialog box appears.

2. From the **Data Source** box, select the desired data field of the parent resource form.
3. From the **Data Sink** 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.

Mapping a Child Resource Form Field to Child Process Form Field

The following procedure describes how to map the data in a field on a child resource form to a field in a child process form

To map a data field from a child resource form to a child process form:

1. Click **Add Table Map**.

   The Add Data Flow Table Mapping dialog box appears.

2. From the **Resource Object Child Table** box, select the table names of the child resource form.
3. From the **Process Child Table** 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 appears.

6. From the **Table Mapping** box, select the desired table name of the child resource form.
7. From the **Data Source** box, select a data field of the child process form.
8. From the **Data Sink** box, select the target data field of the child process form.

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

The following procedure describes how to break a mapping.

To break a mapping:

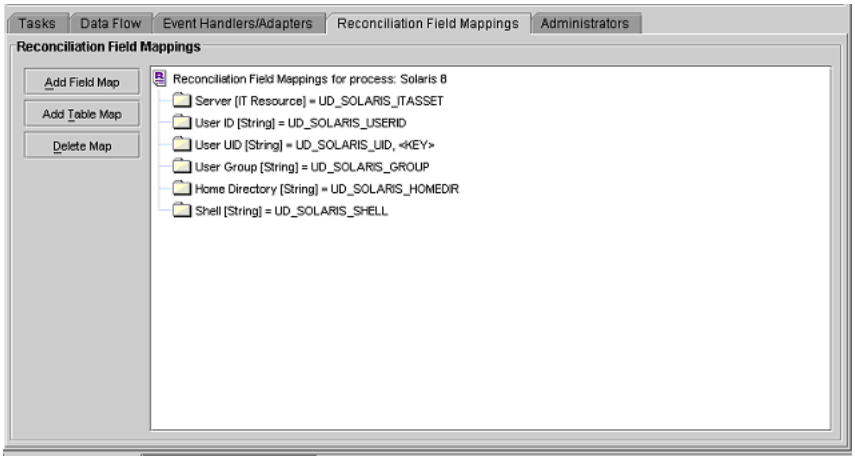
1. Highlight the data fields, which contain a mapping you want to sever.
2. Click **Delete Map**.

   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 Tab

You use the Reconciliation Field Mappings tab shown in Figure 7–5 to define a relationship between data elements in a target system or trusted source and fields in Oracle Identity Manager.

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



Only fields that you define in the **Reconciliation Fields** tab of the associated resource are available for mapping. Using a reconciliation event, these mappings determine what fields in Oracle Identity Manager to populate with information from the target system. For target resources (not trusted sources), you can use this tab to indicate what fields are key fields. Key fields determine what values on the process form and the reconciliation event must be the same to generate a match on the **Processes Matched Tree** tab of the Reconciliation Manager form.

For each mapping, the following information appears:

- Name of the field, as defined on the **Reconciliation Fields** tab of the associated resource, on the target system or 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**, and **IT resource**.
- **For trusted sources**: For user discovery, mapping of the data in the trusted source field to the name of a field on the users form, or for organization discovery, mapping of the data in the trusted source field to the name of a field on the Oracle Identity Manager Organizations form.

  If you are performing 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.
- **For target resources**: Indicator designating if the field is a key field in the reconciliation for this target resource.

  For provisioning processes to match a reconciliation event data, the key field values in their process forms must be the same as those in the reconciliation event.

Mapping a Target Resource Field to Oracle Identity Manager

You can map the fields on a target resource or trusted source, as defined on the **Reconciliation Fields** tab of the associated resource definition, to applicable fields in Oracle Identity Manager. These mapping determine what fields in Oracle Identity Manager are updated in a reconciliation event. These mappings occur when you click one of the following on the Reconciliation Manager form:

- The **Create User** or **Create Organization** button
- The **Link** button on the **Matched Users** or **Matched Organizations** tab
- The **Establish Link** button on the **Processes Matched Tree** tab

For user discovery on a trusted source, you define the fields to be mapped from the **User** resource to fields in the User provisioning process. The fields (that is, the user attributes) to which you will map your trusted source fields are derived from the Users form.

For organization discovery on a trusted source, you define fields to be mapped from the **Oracle Identity Manager Organization** resource to fields in the **Oracle Identity Manager Organization** provisioning process. The fields (that is, the organization attributes) to which you will map your trusted source fields are derived from the **Organizations** form.

After 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.

Mapping a Single Value Field

The following procedure describes how to map a single value.

To map a single value field:

1. Click **Add Field Map**.

   The Add Reconciliation Field Mappings dialog box appears.

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 evaluates if the value of this field on the provisioning process form matches the value of the field in 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 does not require the value of this field to match the process form and reconciliation event for process matching.

Note: To set a field 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 or fields is applied the next time a reconciliation event is received from the target resource or trusted source.

Mapping 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 appears.

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 appear” OR “only child table appears”).

4. Double-click **Process Data Field** and 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 compares the field value on the provisioning process child form with the field value in the reconciliation event. All matching processes appear on the **Processes Matched Tree** tab of the Reconciliation Manager form. If you clear this checkbox, the value of this field does not have to match on the process form and reconciliation event for process matching. Ensure that at least one component (child) field of each multi-valued field is set as a key field. This enhances the quality of the matches generated on the **Process Matched Tree** tab.

Note: Key fields 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.

Deleting a Mapping

This procedure is used to delete a mapping that has been established between a field in Oracle Identity Manager and a field on the target system or trusted source as defined on the **Reconciliation Fields** tab of the associated resource definition.

To delete a mapping:

1. Access the provisioning process definition for the associated resource.
2. Select the **Reconciliation Field Mappings** tab.
3. Select the field mapping you wish to delete.
4. Click **Delete Map**.

   The mapping for the selected field is deleted.

Administrators Tab

You use this tab to select the user groups that can view, modify, and delete the current process definition.

On this tab, when the **Write** check box is selected, the corresponding user group can read and modify the current process definition. When the **Delete** check box is selected, the associated user group can delete the current process definition.

For example, a **SYSTEM ADMINISTRATORS** user group can be configured to view, modify, and delete the **Solaris 8** process definition.

Assigning a User Group to a Process Definition

The following procedure describes how to assign user group privileges.

To assign a user group:

1. Click **Assign**.

   The Groups window appears.
2. Select the unassigned group, and assign it to the process definition.
3. Click **OK**.

   The user group appears in the **Administrators** tab.
4. To enable this user group to view, or modify, or view and modify the current process definition, double-click the corresponding Write check box.

   Otherwise, proceed to Step 5.
5. To enable this user group 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.

Removing a User Group From a Process Definition

The following procedure describes how to remove user group privileges.

To remove a user group:

1. Highlight the user group that you want to remove.
2. Click **Delete**.

   The user group is removed from the process definition.

Modifying Process Tasks

To modify a process task for a process definition, 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:

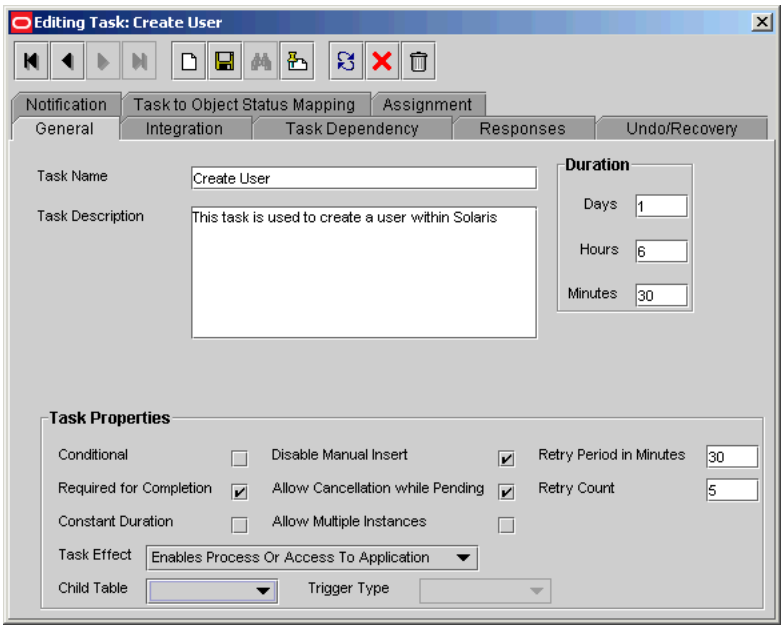
- General Tab
- Integration Tab
- Task Dependency Tab
- Responses Tab
- Undo/Recovery Tab
- Notification Tab
- Task to Object Status Mapping Tab
- Assignment Tab of the Editing Task Window

General Tab

You use this tab to set high-level information for the task that you want to modify. For this example, the **Create User** task is used to create a user in the Solaris environment.

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



The following table describes the fields of the General 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 determines if a condition must met to add the current process task to the process. Select this check box to prevent the process task from being added to the process unless a condition has been met. Clear this check box to not require the condition to be met for the process task to be added to the process.
Required for Completion	This check box determines if the current process task must be completed for the process to be completed. Select this check box to require the process task to have a status of Completed before the process can be completed. Clear this check box to ensure that the status of the process task does not affect the completion status of the process.
Constant Duration	N/A
Task Effect	From this box, select the process action you want to associate with the task, for example, disable, enable. A process can enable or disable a user's access to a resource. When the disable action is chosen, all tasks associated with the disable action are inserted. **Note**: If you do not want the process task to be associated with a particular process action, select **NONE** from the box.

Field Name	Description
Disable Manual Insert	This check box determines if a user can manually add the current process task to the process. Select this check box to prevent the process task from being added to the process manually. Clear this check box to enable a user to add the process task to the process.
Allow Cancellation while Pending	This check box determines if the process task can be cancelled if its status is Pending. Select this check box to allow the process task to be cancelled if it has a Pending status. Clearing this check box to prevent the process task from being cancelled if its status is Pending.
Allow Multiple Instances	This check box determines if the process task can be inserted into the current process more than once. Select this check box to enable multiple instances of the process task to be added to the process. Clear this check box to enable the process task to be added to the current process only once.
Retry Period in Minutes	If a process task is Rejected, this field determines the interval before Oracle Identity Manager inserts a new instance of that task with a status of Pending. In Figure 7–6 on page 7-18, **30** appears in the Retry Period in Minutes text box. If the Create User process task is rejected, in **30** minutes Oracle Identity Manager adds a new instance of this task and assigns it a status of Pending.
Retry Count	How many times Oracle Identity Manager retries a rejected task. In Figure 7–6 on page 7-18, **5** is displayed in the Retry Count text box. If the Create User process task is rejected, Oracle Identity Manager adds a new instance of this task, and assign it a status of Pending. When this process task is rejected for the fifth time, Oracle Identity Manager no longer inserts a new instance of it.
Child Table/ Trigger Type	These boxes specify the action that Oracle Identity Manager performs in the child table of a 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** box, select the child table of the custom form where Oracle Identity Manager will perform an action. From the Trigger Type box, specify the action that Oracle Identity Manager is to perform in the child table. These actions include: ■ **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**: If the custom process form does not have any child tables associated with it, the **Child Table** box will be empty. In addition, the Trigger Type box will be disabled.

Modifying a Process Task's General Information

The following procedure describes how to modify a process task's general information.

To modify the general information for a process task:

1. Double-click the row header of the task you want to modify.

   The Editing Task dialog box appears.

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, you must specify the condition to be met for the task to be added to the process.

6. When you want the completion status of the process to depend 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. To prevent a 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. To enable a user to cancel the process task if its status is Pending, select the **Allow Cancellation while Pending** check box.

   Otherwise, proceed to Step 9.

9. To allow this task to be inserted multiple times in a single process instance, select the **Allow Multiple Instances** check box.

   Otherwise, proceed to Step 10.

10. Click the **Task Effect** box.

    From the custom menu that appears, select one of the following:

    - **Enable Process or Access to Application**. If a resource is reactivated using the enable function, all tasks with this effect are inserted into the process. If you select this option, you must also check the **Allow Multiple Instances** check box.
    - **Disable Process or Access to Application**. If a resource is deactivated using the disable function, all tasks with this effect are inserted into the process. If you select this option, you must also check the **Allow Multiple Instances** check box.
    - **No Effect**. This is the default process action associated with all tasks. If this option is selected, the task is only 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**).

    For this to occur, enter a value in the **Retry Period in Minutes** field. This designates the time in minutes that Oracle Identity Manager waits before adding this process task instance.

    In the **Retry Count** text box, enter the number of times Oracle Identity Manager will retry a rejected task. For example, suppose **3** appears in the **Retry Count** text box. If the task is rejected, Oracle Identity Manager adds a new instance of this task, and assigns it a status of Pending. After this process task is rejected for the fourth time, Oracle Identity Manager no longer inserts a new instance of the process task.

    Note: If either **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** box, select the child table of the custom form where Oracle Identity Manager will perform an action.

    From the **Trigger Type** box, specify the action that Oracle Identity Manager will perform in the child table. These actions include the following:

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

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.

For example, suppose that 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 that precedes each variable name.

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

See also: 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.

Assigning an Adapter or Event Handler to a Process Task

The following procedure describes how to assign an adapter or event handler to a process task.

Important: If you assign an adapter to the process task, the adapter will not work until you map the adapter variables correctly. See "Mapping Adapter Variables" on page 7-23 for details.

To 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 appears, 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.

Mapping Adapter Variables

The following procedure describes how to map adapter variables.

> **Tip:** For more information on which items to select in this procedure, see the *Oracle Identity Manager Tools Reference Guide*.

> **Caution:** 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, it is not triggered during a field update.

To map an adapter variable:

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.
4. From the Data Mapping for Variable window's Toolbar, click **Save**.
5. Click **Close**.

The mapping status for the adapter variable changes from N to Y. This indicates that the adapter variable has been mapped.

Removing an Adapter or Event Handler From a Process Task

The following procedure describes removing an adapter or event handler from a process task.

To remove an adapter or event handler from a process task:

1. Click **Remove**.

   A confirmation dialog box appears.

2. Click **OK**.

   The event handler or adapter is removed from the process task.

Task Dependency Tab

You use the **Task Dependency** tab to determine the logical flow of process tasks in 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 a user can trigger the current process task.

- Assign **dependent** tasks to a process task.

  Oracle Identity Manager or a 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 so that 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 so that the current task's completion status no longer has any bearing on triggering the dependent tasks.

For example, the **Create User** process task does not have any preceding tasks. Oracle Identity Manager triggers this task whenever the task is inserted into a process (for example, when an associated resource is requested). The **Create User** process task has seven dependent tasks. Prior to completion of this process task, each dependent task will have a status of **Waiting**. Once this task achieves a status of Completed, each of these process tasks are assigned a status of **Pending**, and Oracle Identity Manager can trigger them.

Assigning a Preceding Task to a Process Task

The following procedure describes assigning a preceding task to a process task.

To 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.

Removing a Preceding Task from a Process Task

The following procedure describes removing a preceding task from a process task.

To remove a preceding task from a process task:

1. Highlight the preceding task that you want to delete.
2. From the Preceding Tasks region, click Delete.

   The preceding task is removed from the process task.

Assigning a Dependent Task to a Process Task

The following procedure describes assigning a dependent task to a process task.

To 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.

Removing a Dependent Task from a Process Task

The following procedure describes removing a dependent task from a process task.

To 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 Tab

You use the Responses tab to do the following:

- Define the response codes that can be received in conjunction with the execution of a particular process tasks. You can use response codes to represent specific conditions on the target system.
- Define the conditional tasks that are launched if a response code is received during execution of this process task. These tasks are called generated tasks.
- Remove a response from a process task.
- Remove a generated task from a process task.

For example, when a **Create User** process task is **Completed**, the **SUCCESS** response is activated. This response displays a dialog box with the message "The user was

created successfully." In addition, Oracle Identity Manager triggers the **Enable User** 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.

Adding a Response to a Process Task

The following procedure describes how to add a response to a process task.

To 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. In the **Responses** region, click **Add**.

   A blank row appears in 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.

Removing a Response From a Process Task

The following procedure describes how to remove a response from a process task.

To 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.

Assigning a Generated Task to a Process Task

The following procedure describes how to assign a generated task to a process task.

To 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.

Removing a Generated Task From a Process Task

The following procedure describes how to remove a generated task from a process task.

To 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 Tab

You use the Undo/Recovery tab for the following:

- To define process tasks that are triggered when the current process task is cancelled. These process tasks are known as undo tasks.
- To remove an undo task from a process task, when it is no longer valid.
- To define process tasks that are triggered when the current process task is rejected. These tasks are called recovery tasks.
- To remove a recovery task from a process task.

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

> **Note:** When the current process task is rejected, Oracle Identity Manager triggers any recovery tasks that are assigned to the process task. If you select the Complete on Recovery check box, Oracle Identity Manager changes the status of the current process task from **Rejected** to **Unsuccessfully Completed** upon completion of all recovery tasks that are generated. This enables Oracle Identity Manager to trigger other dependent process tasks.

The following sections describe how to assign an undo and recovery task to the current process task, and how to remove an undo and recovery task from the current process task.

Assigning an Undo Task to a Process Task

The following procedure describes how to assign an undo task to a process task.

To 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. In 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.

Removing an Undo Task From a Process Task

The following procedure describes how to remove an undo task from a process task.

To 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.

Assigning a Recovery Task to a Process Task

The following procedure describes how to assign a recovery task to a process task.

To 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.

Removing a Recovery Task From a Process Task

The following procedure describes how to remove an recovery task from a process task.

To remove an 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 Tab

You use this tab to designate the email notification to be generated when the current process task achieves a particular status. A separate email notification can be generated for each status a task can achieve. If an email notification is no longer valid, you can remove it from the **Notification** tab.

For example, when the **Create User** process task achieves a status of **Completed**, Oracle Identity Manager sends the **Process Task Completed** email notification to the user who is to be provisioned with the resource. If the Create User process task is rejected, the Process Task Completed email notification is sent to the user and the user's manager.

Note: Oracle Identity Manager can only send an email notification to a user if you first create a template for the email message using the Email Definition form.

See "The Email Definition Form" on page 7-1 for details.

The following sections describe how to assign email notifications to a process task and remove email notifications from a process task.

Assigning an EMail Notification to a Process Task

The following procedure describes how to assign an email notification to a process task.

To assign an email 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 appears.
2. Click the **Notification** tab.
3. Click **Assign**.

   The Assignment dialog box appears.
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 -mail notification.
7. Select the check boxes that represent the users who will receive the email notification.

   Currently, an email 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 email notification is assigned to the process task.

Removing an E-Mail Notification From a Process Task

The following procedure describes how to remove an email notification from a process task.

To remove an email 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 Tab

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.

The following sections describe how to map a process task status to a provisioning status and unmap a process task status from a provisioning status.

Mapping a Process Task Status to a Provisioning Status

The following procedure describes how to map an process task status to a provisioning status.

To map an 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 in the Task to Object Status Mapping tab.

6. Click **Save**.

   The process task status is mapped to the provisioning status.

Unmapping a Process Task Status From a Provisioning Status

The following procedure describes how to unmap an process task status from a provisioning status.

To unmap an 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 in 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 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 example, if 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 is assigned to the user named **RLAVA** and the task is 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 evaluates the criteria of the **Solaris Process Tasks - Group** rule. If that rule's criteria are satisfied, the task is assigned to the **SYSTEM ADMINISTRATORS** user group and the task is 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 6-5. 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 Unmentioned 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 in 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.

The following sections describe adding a task assignment rule to a process task and how to remove it from the process task.

Adding a Rule to a Process Task

The following procedure describes how to add a rule to a process task.

To 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 in 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.

Removing a Rule From a Process Task

The following procedure describes how to remove a rule from a process task.

To 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

Administering Oracle Identity Manager with Design Console

This chapter describes how to use Design Console to administer Oracle Identity Manager. It contains the following topics:

Overview

The Design Console Administration folder provides System Administrators with tools for managing Oracle Identity Manager administrative features. This folder contains the following forms:

- **Form Information**: You use this form 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 in the Design Console Explorer.

- **Lookup Definition**: You use this form to create and manage lookup definitions. A lookup definition represents a lookup field and the values you can access from that lookup field.

- **User Defined Field Definition**: You use this form to create and manage user-defined fields.

  A user-defined field enables you to store additional information for Design Console forms.

- **System Configuration**: You use this form to define and set the value of properties that control the behavior of the Client and/or Server.

  You can specify the users and user groups that a property value applies to, or you can specify that the value applies to all users.

- **Remote Manager**: You use this form to display information about the servers that Oracle Identity Manager uses to communicate with third-party programs.

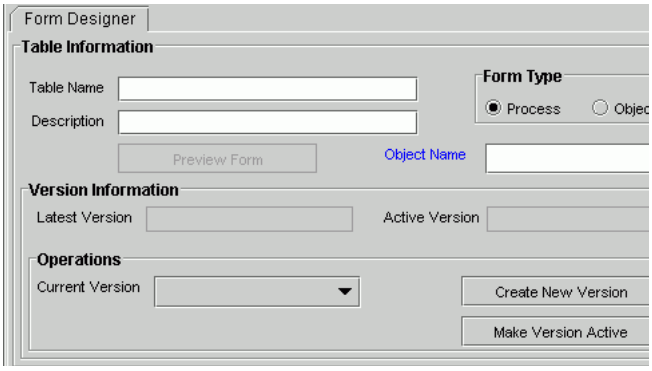
  These servers are known as remote managers.

- **Task Scheduler**: You use this form to set up the schedules that determine when scheduled tasks are to be run.

The Form Information Form

The Form Information form, shown in Figure 8–1, is located in the Design Console Administration folder. You use this form to specify the class name, the label that appears in the Design Console Explorer, the form type, form icon, and Help to be associated with an Oracle Identity Manager form. You can also use this form to modify the folders and folder items that appear in the Design Console 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 in the Oracle Identity Manager Explorer. For forms of the **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 Design Console Explorer.
Context Sensitive Help URL	The URL of the online Help topic that appears if the user presses **F1** when this form is active.

Adding an Oracle Identity Manager Form or Folder

The following procedure describes how to add a form or folder.

To add an Oracle Identity Manager form or folder:

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 Design Console Explorer in the **Description** field.

   For forms of type **childform**, 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** 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 in 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**.

     Tip: For more information on the Oracle Identity Manager Administrative and User Console, refer to *Oracle Identity Manager Administrative and User Console Guide*.
5. Enter the name of the icon or graphic image file to be used in the Design Console 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 file is displayed if the user presses **F1** when the form is active.
7. Click **Save**.

   The form is added and a system-generated ID for the form or folder appears in the **Key** field.

Modifying the Design Console Explorer

The Design Console 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

A lookup definition represents one of the following:

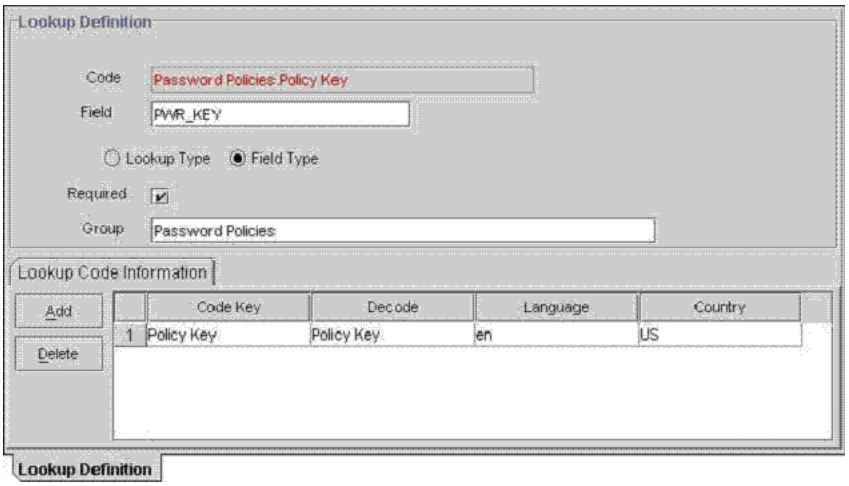
- The name and description of a text field
- A lookup field and the values that are accessible from that lookup field by double-clicking it
- A box, and the commands that can be selected from that box

These items, which contain information pertaining to the text field, lookup field, or 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
- A user-created form or tab built using the Form Designer form

The Lookup Definition form shown in Figure 8–2 is located in the Design Console Administration folder. You use this form to create and manage lookup definitions.

Figure 8–2 The Lookup Definition 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 box field will be accessible.

Field Name	Description
Lookup Type/Field Type	These radio buttons designate if the lookup definition is to represent a text field, a lookup field, or a box. If you select 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 box, along with the values that are to be accessible from that lookup field or 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 box. This cannot be changed. However, you can add or modify the values that are accessible from the lookup field or box. For forms or tabs that are user-defined, the user determines whether the lookup definition represents a lookup field or a 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 Tab" 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 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.

The following sections describe how to create a lookup definition.

Creating a Lookup Definition

To create a lookup definition:

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 box field will be accessible.
4. If the lookup definition is to represent a lookup field or box, select the **Lookup Type** radio button.

   See the table that appears earlier in this section for more information.

   If the lookup definition is to represent a text field, select the **Field Type** radio button.
5. Optional. To save the contents of this form or tab only when the field or 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.

You must follow naming conventions for the text you enter into the **Code**, **Field**, and **Group** text boxes.

Tip: For more information on the naming conventions, see "The Lookup Definition Form" on page 8-4.

7. Click **Save**.

   The lookup definition is created. The associated text field, lookup field, or box will 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. You use this tab to create and manage detailed information on the selected lookup definition. This information includes the names, descriptions, language codes, and country codes of a value pertaining to the lookup definition. These items are known as **lookup values**.

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

Creating and Modifying a Lookup Value

The following procedure describes how to create and modify a lookup value.

Caution: For internationalization purposes, you must provide both a language and country code for a lookup value.

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

To create or modify a lookup value:

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 in 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 in the lookup field or 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 one of the following:

   - The items that appears in a lookup window after the user double-clicks the corresponding lookup field
   - The commands that are to be displayed in the associated 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 now reflects the settings you have entered.

Deleting a Lookup Value

To delete a lookup value:

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.

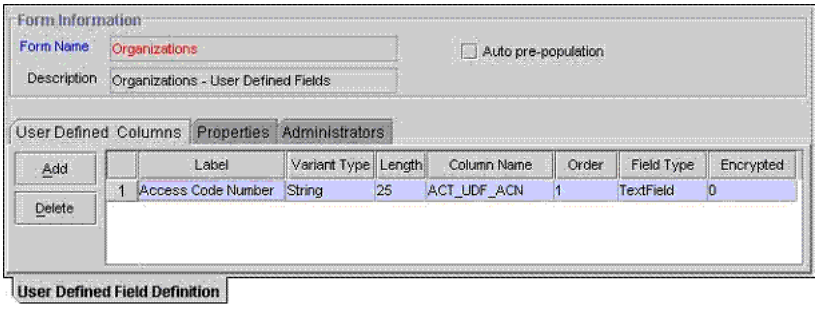
The User Defined Field Definition Form

You may need to augment the fields that Oracle Identity Manager provides by default. You can create new fields and add them to various Oracle Identity Manager forms. These fields are known as **user-defined fields**.

User-defined fields appear on the **User Defined Fields** tab of the form that appears in the **Form Name** data field. For example, Figure 8–3 shows an **Access Code Number** user-defined field added to the **User Defined Fields** tab of the Organizations form.

The User Defined Field Definition form shown in Figure 8–3 appears in the Design Console Administration folder. You use this form 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



The following table describes the data fields of the User Defined Field Definition form.

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

The following section describes how to select a target form for user-defined fields.

Selecting the Target Form for a User-Defined Field

The following procedure describes how to select the target form for a user-defined field.

To select the target form for a user-defined field:

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

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

The User Defined Field Definition form contains the following tabs:

- User Defined Columns Tab
- Properties Tab

- Administrators Tab

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

User Defined Columns Tab

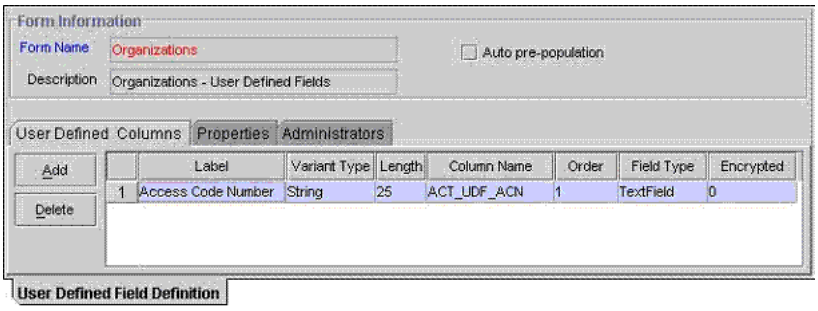
You use this tab to do the following:

- 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.

  The field's order number determines the order in which a user-defined field appears on a form. In Figure 8–4, the **Access Code Number** user-defined field has an order number of **1**, so it appears first on the **User Defined Fields** tab of the Organizations form.
- Determine if the information that is associated with the user-defined field is encrypted when it is exchanged between the client and the server.
- Remove a user-defined field.

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



The following sections describe 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.

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

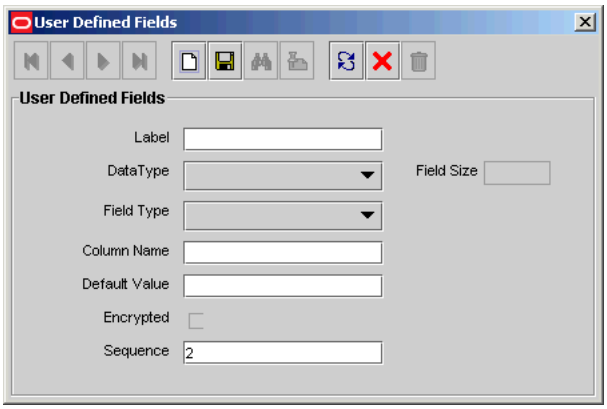
The following procedure describes how to add a user-defined field to a form.

To add a user-defined field:

1. Click **Add**.

   The User Defined Fields dialog box appears, as shown in Figure 8–5.

Figure 8–5 The User Defined Fields Dialog Box

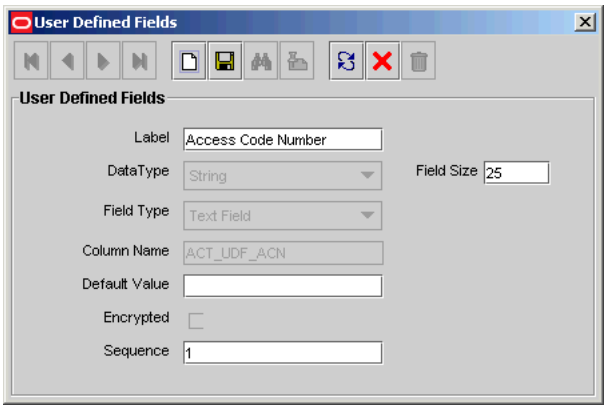


Field Name	Description
Label	The label for the user-defined field. This label appears next to the user-defined field on the **User Defined Fields** tab of the target form. The maximum length for a label is 30 characters.
Data Type	From this box, select one of the following data types for the user-defined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

Field Name	Description
Field Type	From this box, select one of the following field types for the user-defined field: ■ Text Field. The field appears on the **User Defined Fields** tab of the target form as a text field. ■ Lookup Field. The field appears on the **User Defined Fields** tab of the target form as a Lookup field. ■ Combo Box. The field appears on the **User Defined Fields** tab of the target form as a box. ■ Text Area. The field appears on the **User Defined Fields** tab of the target form as a text area. ■ Password Field. The 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 field appears on the **User Defined Fields** tab of the target form as a check box. ■ Date Field with Dialog. This 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 in this box reflect the data type that is displayed in the **Data Type** box.
Column Name	The name of the user-defined field that is recognized by the database. **Note**: This name consists of a *<TABLE NAME_UDF_>* prefix, followed by the label that is associated with the user-defined field. For example, 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 in **Column Name** field cannot contain any spaces.
Default Value	This value appears in a user-defined field on the target form.
Encrypted	This check box determines if the information that appears in the associated user-defined field is encrypted when it is exchanged between the client and the server. Select this check box to encrypt the information displayed in the user-defined field. Clear this check box to not encrypt the information in the user-defined field.
Sequence	This field represents the order in which the user-defined field appears on the 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



In Figure 8–6, 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 in the **User Defined Columns** tab. Once the target form is launched, this user-defined field usually appears in the **User Defined Fields** tab of that form. Since the user-defined fields for a user pertain to the user's profile information, they are displayed in the **User Profile** tab of the **Users** form.

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

The following procedure describes how to remove a user-defined field.

To remove a user-defined field:

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

   The user-defined field is removed.

Properties Tab

You use this tab to assign properties and property values to the data fields that appear on the **User Defined Fields** tabs of various Oracle Identity Manager forms.

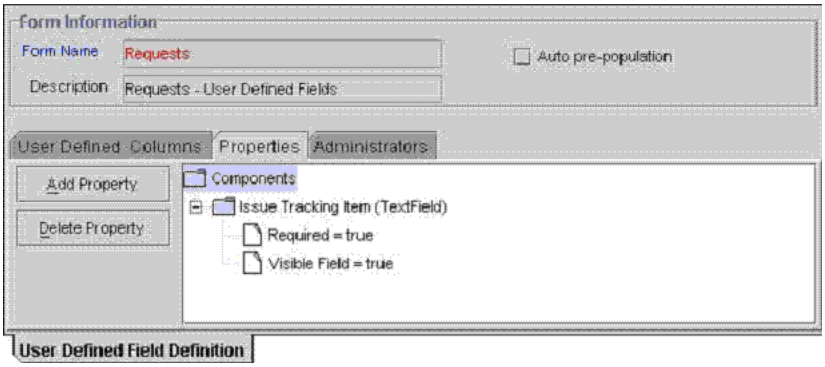
For this example, the **User Defined Fields** tab of the **Requests form** displays one data field: **Issue Tracking Item**. This data field contains the following properties:

- **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 in the **User Defined Fields** tab. In addition, this field needs to be populated for the form to be saved.

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



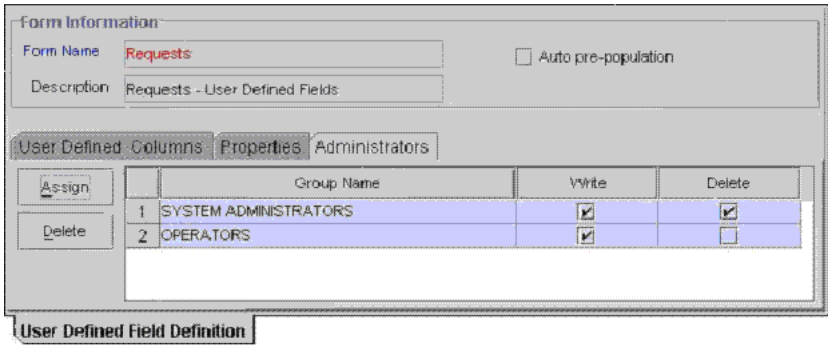
The following section describes how to add and remove a property and property value to a data field.

> **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 Tab

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



You use this tab to specify the user groups that have administrative privileges over the current record of the User Defined Field Definition form. The **Write** and **Delete** check boxes on this form designate if these administrative groups can modify, delete, or modify and delete information bout the current user-defined field (UDF) definition.

The following sections describe 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.

Assigning Administrative Privileges to a User Group for a UDF Definition

The following procedure describes how to assign administrative privileges to a user group for a UDF definition.

To assign administrative privileges:

1. Click **Assign**.

The Assignment dialog box appears.

2. Select the user group, and assign it to the UDF definition.
3. Click **OK**.

   The user group appears in the **Administrators** tab.
4. To enable this user group to view and modify information pertaining to the current definition, double-click the corresponding **Write** check box.

   Otherwise, proceed to Step 5.
5. To enable this user group to delete information in 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.

Removing Administrative Privileges From a User Group for a UDF Definition

The following procedure describes how to remove administrative privileges from a user group for a UDF definition.

To remove administrative privileges:

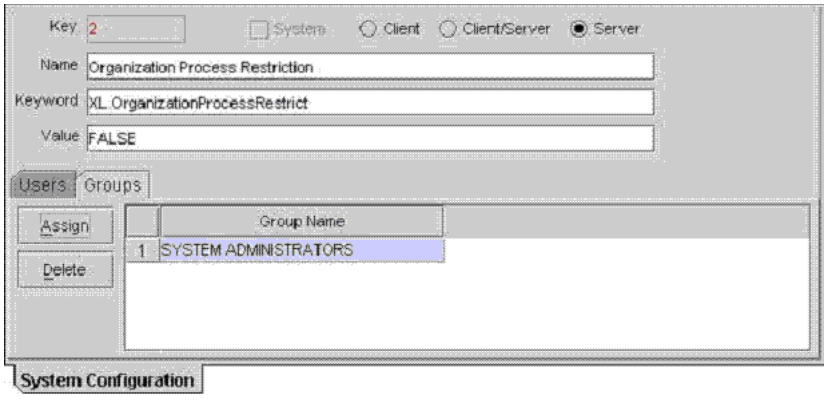
1. Highlight the user group that you want to remove.
2. Click **Delete**.

   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 Design Console Administration folder. You use this form to define and set the value of properties that control the behavior of Oracle Identity Manager. You can specify the users and user groups that a property value applies to, or you can specify that a property value applies 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 designates if this instance of the property definition applies to all users in Oracle Identity Manager, that is, it is a system-wide instance, or only to selected users and user groups. Select this check box to apply this setting to all users. The **Users** and **Groups** tabs will be disabled. Clear this check box to specify that an instance of the property applies to certain users and groups. **Note**: The **System** check box is disabled if the **Server** radio button (described below) is selected.
Client **Client/Server** **Server** (Radio buttons)	These radio buttons designate if this instance of the property definition applies to the client, the server, or both. Select the **Client** radio button to apply property value only to the client. Select the **Client/Server** radio button to apply the property value to both the client and server. Select the **Server** radio button to apply the property value only to the server. Selecting this option disables the **System** checkbox. 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.
Keyword	The property's unique ID. This must be identical for each instance of this property. For example, if you want 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 server, see "System Properties" on page A-16.
Value	The value for this instance of the property definition. This value is applied to the users and groups assigned to this instance of the property unless the **System** checkbox is selected, denoting that the instance applies to all users.

The following sections describe how to define instances of property definitions, assign users or groups to these instances, and remove the user or group from this instance.

Creating and Editing an Instance of a Property Definition

The following procedure describes how to create or edit a property definition.

To create a new instance or edit an existing instance of a property definition:

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:** Oracle recommends 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.
4. Designate whether you want 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. If this is the case, 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.

The following section describes how to assign users and groups to this instance.

Assigning a User or Group to an Instance of a Property Definition

The following procedure describes how to assign a user or a group to a property definition.

> **Caution:** If this is a system-wide instance (that is, 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.

To assign a user or group to an instance of a property definition:

1. Access the System Configuration form.
2. Query for the instance of the property definition you wish to assign to a user or group.

   > **Tip:** To learn more about the various property definitions to which you can assign users and groups, refer to "System Properties" on page A-16.

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 appears.

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.

Removing a User or Group From an Instance of a Property Definition

When you remove a user or group from an instance of a property definition, the property is no longer associated with the user or group.

To remove a user or group from an instance of a property definition:

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.

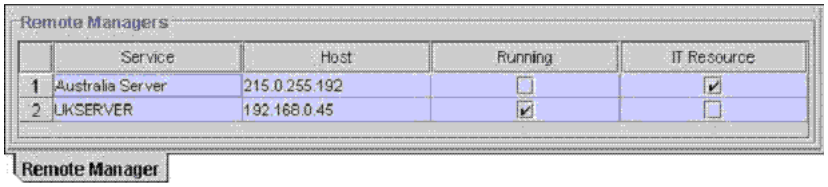
The Remote Manager Form

The Remote Manager is a lightweight network server that enables you to integrate with target systems whose APIs do not have the ability to communicate over a network, or that have network awareness but are not secure. The Remote Manager works as a server on the target system, and an Oracle Identity Manager server works as its client. 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 shown in Figure 8–10 is located in the Design Console Administration folder. It displays 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, you can define 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 or resources 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 or resources that Oracle Identity Manager can use.

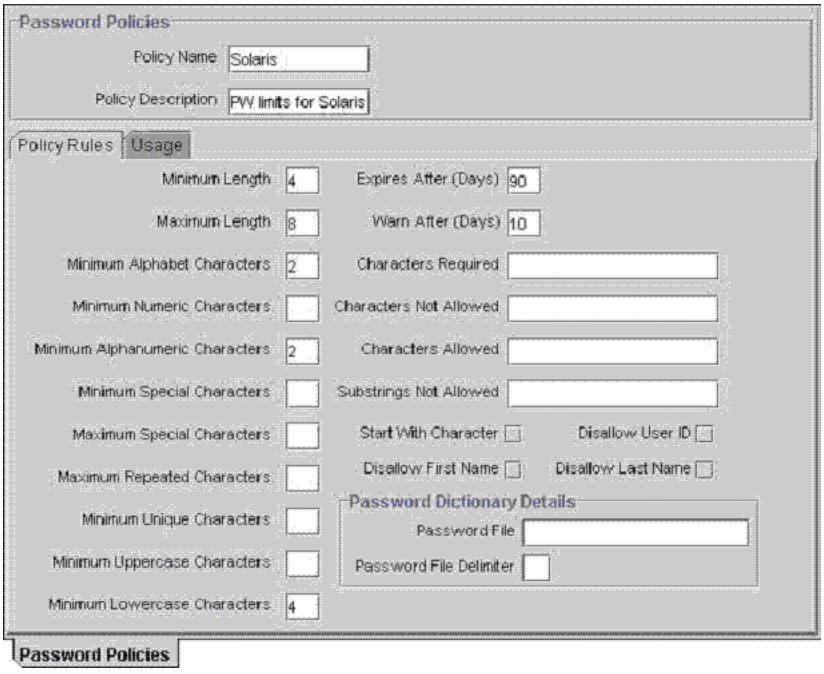
Note: To learn how the Remote Manager form is used with other Oracle Identity Manager forms, see the *Oracle Identity Manager Tools Reference Guide*.

The Password Policies Form

The Password Policies form shown in Figure 8–11 is located in the Design Console 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



The following table describes the data fields of the Password Policies form.

Field Name	Description
Policy Name	The password policy's name.
Policy Description	Explanatory information about the password policy.

The following section describes how to create a password policy.

Creating a Password Policy

The following procedure describes how to create a password policy.

> **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 and 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.

To create a password policy:

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.

Tabs on the Password Policies Form

After 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 Tab
- Usage Tab

The following sections describes these tabs.

Policy Rules Tab

You use this tab to specify criteria for your password policy, for example, a password's minimum and maximum length.

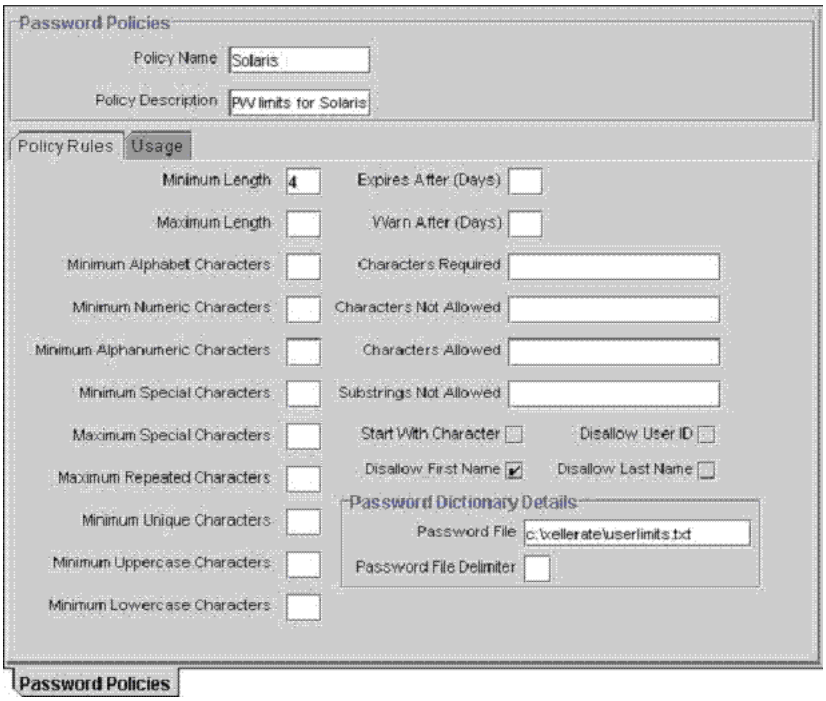
You can use either or both of the following methods to set password restrictions:

- Enter information in the appropriate text boxes or select the desired check boxes. For example, to indicate that a password must have a minimum length of four characters, type **4** into the **Minimum Length** text box. Or, 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.

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



The following section describes the data fields of the **Policy Rules** tab. These are the fields into which you will specify the password limitations.

The following table describes the data fields of the Policy Rules tab.

> **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.

Field Name	Description
Minimum Length	The fewest number of characters that a password can have for it to be valid. For example, if you enter **4** 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 you enter **8** in the **Maximum Length** text box, the password is be accepted if it has more than eight characters.

Field Name	Description
Minimum Alphabet Characters	The fewest number of letters that a password can have for it to be valid. For example, if you enter **2** in the **Minimum Alphabet Characters** text box, the password is not 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. For example, if you enter **1** in the **Minimum Numeric Characters** text box, the password must have at least one number.
Minimum Alphanumeric Characters	The fewest number of letters *or* digits that a password can have for it to be valid. For example, if you enter **6** in the **Minimum Alphanumeric Characters** text box, the password must be have at least six letters or numbers.
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 you enter **1** in the **Minimum Special Characters** text box, the password must have at least one non-alphanumeric character.
Maximum Special Characters	The highest number of non-alphanumeric characters that a password can have for it to be valid. For example, if you enter **3** appear in the **Maximum Special Characters** text box, the password is not 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. For example, if you enter **2** in the **Maximum Repeated Characters** text box, the password is not accepted if more than two characters are repeated. For example, RL112211 would not be a valid password because 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. For example, if you enter **1** in the **Minimum Unique Characters** text box, the password is not accepted if every character of the password is repeated at least once. For example, **1a23a321** would not be a valid password because 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 you enter **8** in the **Minimum Uppercase Characters** text box, the password is not 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. For example, if you enter **8** in the **Minimum Lowercase Characters** text box, the password is not accepted if it has fewer than eight lowercase letters.

Field Name	Description
Expires After (Days)	The maximum number of days for which a password is valid. For example, if you enter **30** 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. For example, suppose that you enter **30** in the **Expires After (Days)** text box, and **10** 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 you enter **x** in the **Characters Required** text box, the password is accepted only if it contains an "x".
Characters Not Allowed	The characters that a password must not have for it to be valid. For example, if you enter **!** in the **Characters Not Allowed** text box, the password is not accepted if it contains an "!".
Characters Allowed	The characters that a password can have for it to be valid. For example, if you enter % in the **Characters Allowed** text box, the password is 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. For example, if you enter **IBM** in the **Substrings Not Allowed** text box, the password is not accepted if it contains the letters "I", "B", and "M", in successive order.
Start With Character	This check box specifies if 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 is accepted even if it does not begin with a character.
Disallow First Name	This check box specifies if 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 specifies if 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 specifies if 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 is accepted, even if it contains the user's last name.

Field Name	Description
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.

The following sections describe how to specify the criteria (or rules) for the password policy.

Setting the Criteria for a Password Policy

The following procedure describes how to set the criteria for a password policy.

To 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.

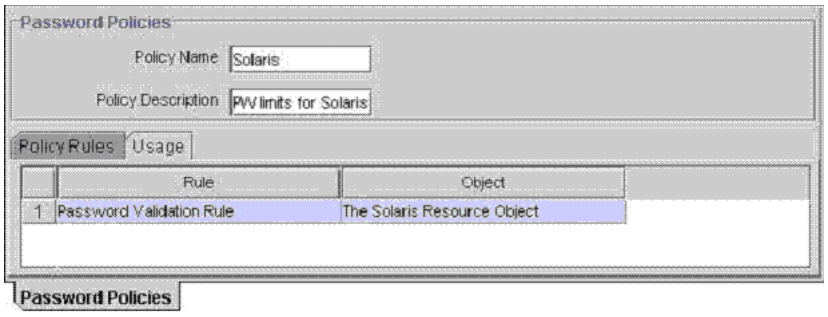
Usage Tab

You use this tab to view the rules and resource objects that are associated with the current password policy.

For example Figure 8–13 shows the **Solaris** password policy and the **Password Validation Rule** have been assigned to **The Solaris Resource Object**.

Figure 8–13 illustrates the Usage tab of the Password Policies form.

Figure 8–13 The Usage Tab of the Password Policies Form



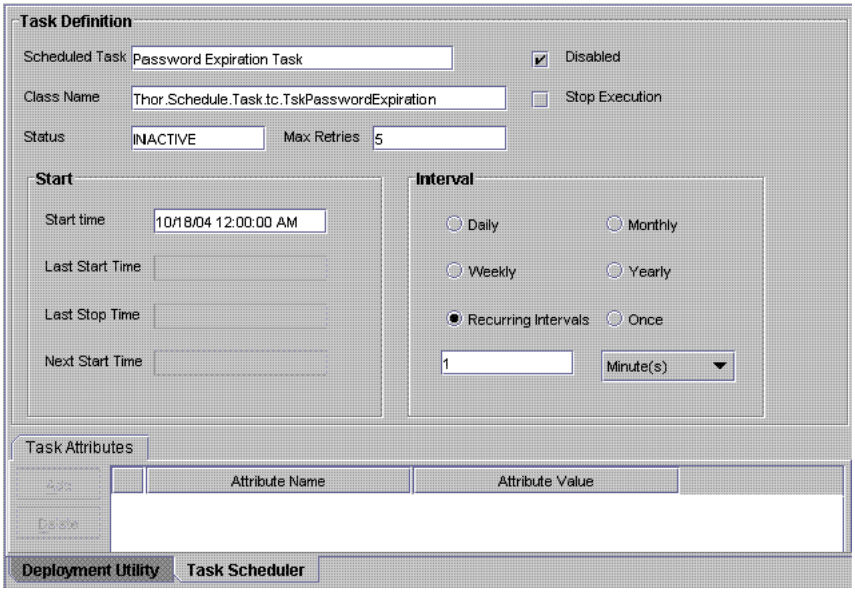
Tip: For more information on the relationship between password policies and resource objects, see "Password Policies Rule Tab" on page 6-24.

The Task Scheduler Form

The Task Scheduler form shown in Figure 8–14 is located in the Administration/Job Scheduling Tools folder. You use this form 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.

Field Name	Description
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 successfully task will not run again (the **Once** radio button is selected). ■ **ERROR**. A problem occurred while the task was being executed.
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.

Field Name	Description
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 box.
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.

Creating a Scheduled Task

In addition to creating a scheduled task, if the task needs attributes, you must set them. Otherwise, the scheduled task is not functional.

When an existing task attribute is no longer relevant, you must remove it from the scheduled task.

The following procedure describes how to create a scheduled task. Later procedures show how to add an attribute to a scheduled task and remove a task attribute from the scheduled task.

To create a scheduled task:

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, set the interval by entering a value into the text field below the radio button, then select a unit of measure from the adjacent box.
8. Click **Save**.

   The scheduled task is created. In addition, **INACTIVE** is displayed in 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.

Adding a Task Attribute

The following procedure describes how to create a task attribute.

To add a task attribute:

1. Click **Add**.
2. In the **Attribute Name** field, enter the name of the task attribute.
3. In the **Attribute Value** field, type the attribute's value.
4. From the Toolbar, click **Save**.

   The task attribute is added to the scheduled task.

Removing a Task Attribute

The following procedure describes how to remove a task attribute.

To remove a task attribute:

1. Highlight the task attribute that you want to remove.
2. Click **Delete**. The attribute is removed from the scheduled task.

Deleting a Custom Scheduled

This section describes how to delete a custom scheduled task.

> **Note:** You cannot delete any internal scheduled tasks, such as Password Expiration Task, that are installed with Oracle Identity Manager.

To delete a scheduled task:

1. Access the **Task Scheduler** form.
2. Enter the name of the scheduled task in the **Scheduled Task** field and click the binoculars button or press **Ctrl**+**Q**. The scheduled task opens in the Task Definition form.

3. In the Task Definition form, remove any existing task attributes by following the instructions in "Removing a Task Attribute" on page 8-27.
4. Click the **Delete** button on the toolbar or press **Ctrl**+**D**. A warning message displays, informing you that the current record will be deleted.
5. Click **OK** to delete the scheduled task.

9

Development Tools

This chapter describes the full suite of development tools in Design Console. It contains the following topics:

Overview

Design Console provides a suite of development tools that enable system administrators or developers to customize Oracle Identity Manager. This folder contains the following forms:

- **Adapter Factory**: You use this form to create and manage the code that enables Oracle Identity Manager to communicate with any IT Resource by connecting to that resource's API.

  This code is known as an adapter.

- **Adapter Manager**: You use this form to compile multiple adapters simultaneously.
- **Form Designer**: You use this form to create process and resource object forms that do not come packaged with Oracle Identity Manager.
- **Error Message Definition**: You use this form to create the error messages that appears in dialog boxes when certain problems occur while using Oracle Identity Manager.

  This form also 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**: This folder provides System Administrators and developers with tools for managing event handlers and data objects in Oracle Identity Manager.

  This folder contains the following forms:

  – **Event Handler Manager**: You use this form 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.

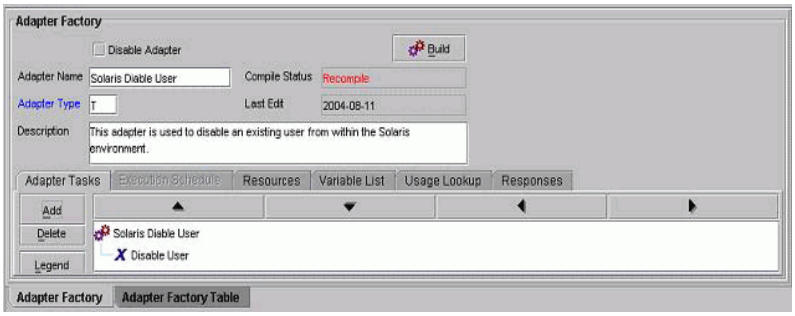
- **Reconciliation Rules**: You use this form to create and manage reconciliation rules in Oracle Identity Manager.

The Adapter Factory Form

Adapters extend the internal logic and functionality of Oracle Identity Manager. In addition, they interface with any IT Resource by connecting to that resource's API.

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.

Figure 9–1 The Adapter Factory Form

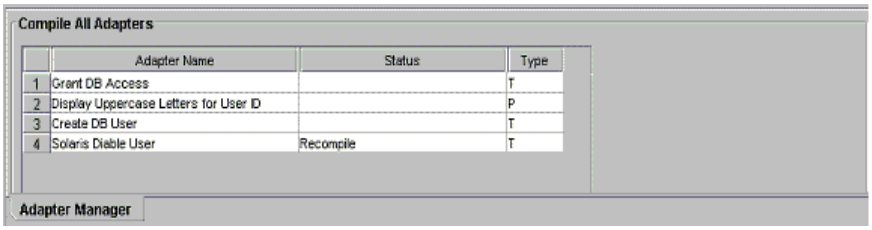


Tip: For more information on adapters or the Adapter Factory, refer to *Oracle Identity Manager Tools Reference Guide*.

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

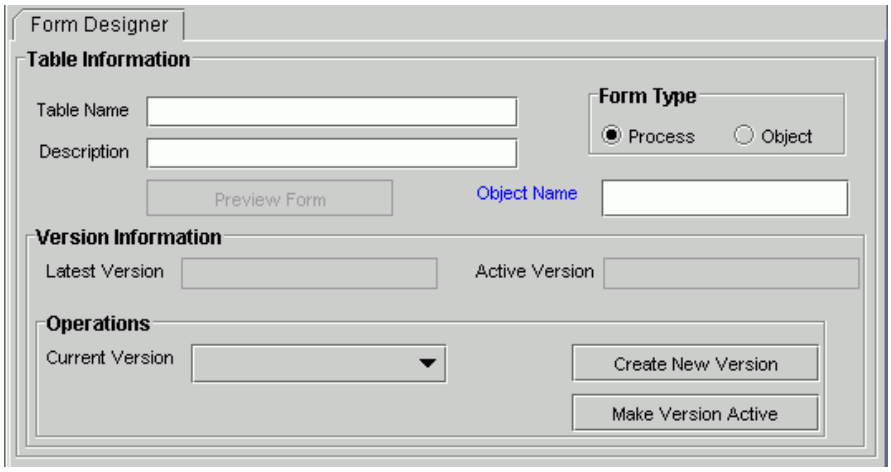
The information required to provision resources to a target user or organization cannot always be retrieved from an existing Oracle Identity Manager form. You can use the Form Designer form in the Development Tools folder to create a form with fields that contain the relevant information. After creating the form, you assign it 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.

The following are reasons, listed in order of importance, why Oracle Identity Manager displays a resource object or process form that a user creates using the Form Designer form:

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.

For 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 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 a **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**.
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 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).

The following section describes how to create a form.

Creating a Form

The following procedure describes how to create a form.

To create a form:

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. 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:

- Additional Columns Tab
- Child Table(s) Tab
- Object Permissions Tab
- Properties Tab
- Administrators Tab
- Usage Tab
- Pre-Populate Tab
- Default Columns Tab
- User Defined Fields Tab

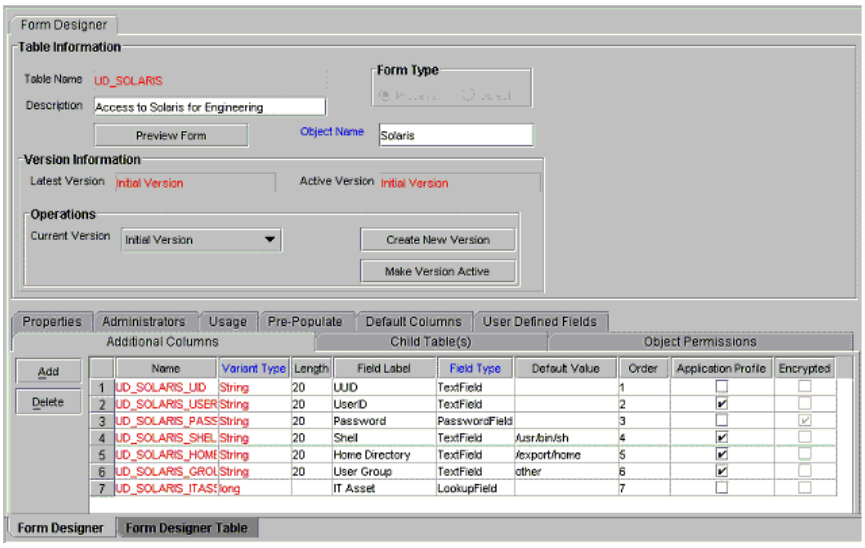
Each of these tabs is described in the following sections.

Additional Columns Tab

You use tab 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 displays the Additional Columns tab of the Form Designer Form.

Figure 9–4 The Additional Columns Tab of the Form Designer Form



The following table describes the data fields.

Name	Description
Name	The name of the data field that appears in the database and is recognized by Oracle Identity Manager. **Note**: This name consists of the **<TABLENAME_>** prefix followed by the name of the data field. For example, if the name 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 that appears in the database, and that 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 in 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 in 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 in 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 box that appears in the Property Value text box. For more information on adding a property value to a data field, refer to "Adding a Property and Property Value to a Data Field" on page 9-14. ■ **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 box (a combo box). A user can select an item from the box, and save this selection to the database.
Default Value	This value appears in the associated data field after the form is generated and if no other default value was 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 that 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 designates if the most-recent value of this field should appear on the Object Profile tab of the Users form after 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 determines if the information, which appears in 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 in the data field is 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 is not encrypted when it is transmitted between the server and the client.

The following sections describe 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.

Adding a Data Field to a Form

The following procedure describes how to add a data field to a form.

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 is encrypted in the database.

When creating a data field of password (field type) with the Encrypted option selected, the value appears as asterisks (*) in the Administrative and User Console and the data is encrypted in the database.

To add a data field to a form:

1. Click **Add**.

   A blank row appears in 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 consists of the <**TABLENAME**_> prefix, followed by the name of the data field.

   For example, 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 that 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 box.

   Tip: For more information on data types, refer to the table that appears earlier in this section.
7. In the Default Value field, enter the value that appears in the associated data field once the form is generated, and if no other default value has been specified.

   Tip: 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 in 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.

Removing a Data Field From a Form

The following procedure describes removing a data field from a form.

To remove a data field from a form:

1. Delete all properties that are associated with the data field you want to remove by following the instructions in "Removing a Property and Property Value From a Data Field" on page 9-17.
2. Highlight the data field that you want to remove.
3. Click **Delete**. The data field is removed from the form.

Child Table(s) Tab

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 contains the data fields that are required by another form. It 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. For example, 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).

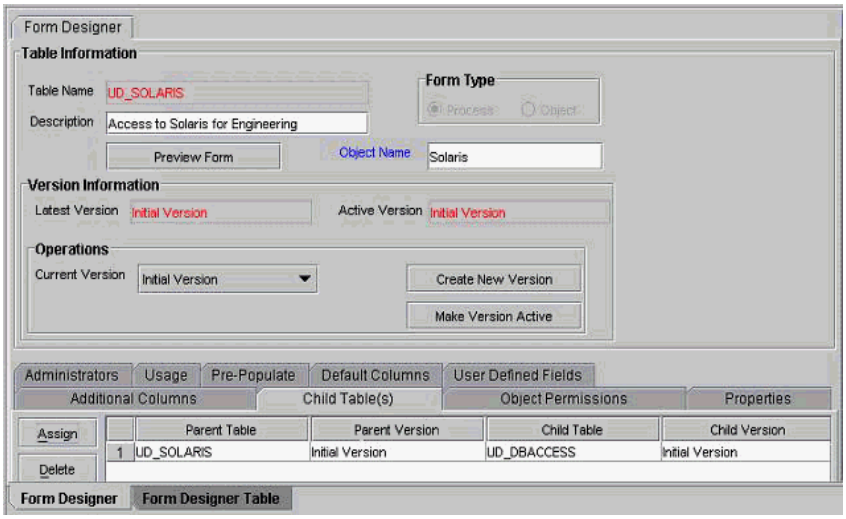
If you use a child table for one form, and then decide that you want to apply it to another form, Design Console enables you to do so. Simply remove the child table from the first form, and assign it to the target form. This way, the child table that you assign to one form can be reused for all forms created with the Form Designer form.

You can configure Oracle Identity Manager to perform one of the following actions in 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.

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



Note: For more information on setting up Oracle Identity Manager to insert, edit, or delete a value from in a column of a child table, refer to "The Process Definition Form" on page 7-6.

For example, suppose that the **UD_SOUTH** child table is assigned to the **Results of 1Q 2004 Sales** form (represented by the **UD_SALES2** table name). After this form is launched, the data fields in the **UD_SOUTH** child table appear in the form.

The following sections describe how to assign a child table to a form and 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.

Assigning a Child Table to a Form

The following procedure describes how to assign a child table to a form.

> **Important:** If the form that is represented by the child table has not been made active, it will not appear in the Assignment window. As a result, you cannot assign it to the parent form.

To assign a child table to a form:

1. Click **Assign**.

   The Assignment window appears.

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.

Removing a Child Table From a Form

To remove a child table from a form:

1. Highlight the child table that you want to remove.
2. Click **Delete**.

   The child table is removed from the form.

Object Permissions Tab

You use this tab to select the user groups that can add, modify, and remove information from a custom form when it is instantiated.

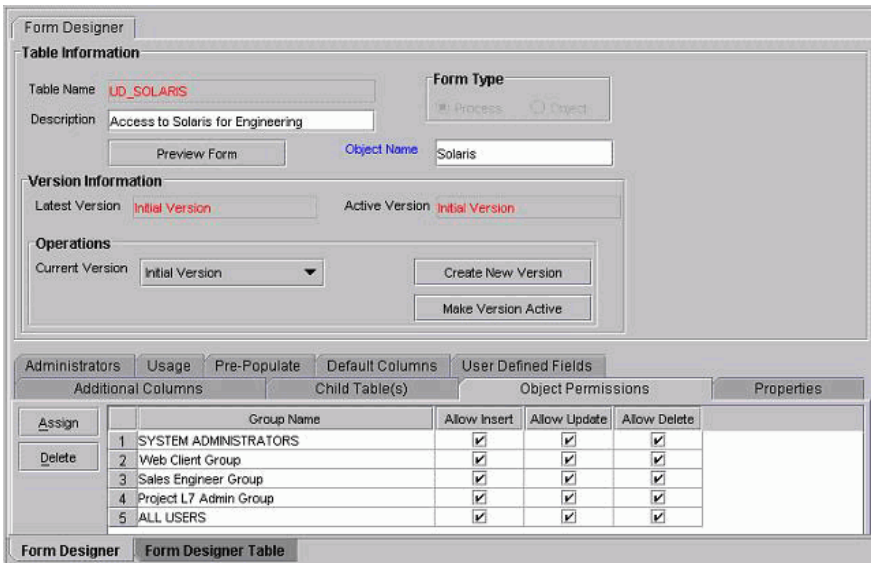
When the **Allow Insert** check box is selected, the corresponding user group can add information into the fields of the user-created form. If this check box is cleared, the user group cannot populate the fields of this form.

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.

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).

Figure 9–6 displays the Object Permissions tab of the Form Designer Form.

Figure 9–6 The Object Permissions Tab of the Form Designer Form



For example, suppose the **SYSTEM ADMINISTRATOR**S 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.

The following section describes how to assign a user group to a user-created form and remove a user group from a user-created form.

Assigning a User Group to a User-Created Form

To assign a user group to a user-created form:

1. Click **Assign**.

   The Assignment dialog box appears.

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.

Removing a User Group From a User-Created Form

To remove a user group from a user-created form:

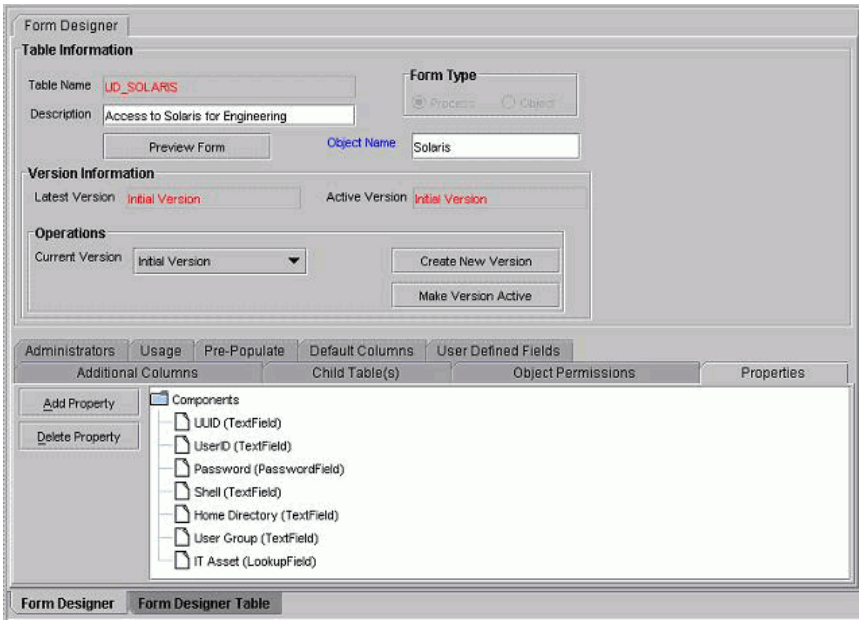
1. Highlight the user group that you want to remove.
2. Click **Delete**.

   The user group is removed from the user-created form.

Properties Tab

Figure 9–7 displays the Properties Tab of the Form Designer Form. You use this tab to assign properties and property values to the data fields that appear on the form that is created through the Form Designer form.

Figure 9–7 The Properties Tab of the Form Designer Form



For example, suppose that the **Results of 1Q 2004 Sales** form has 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 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 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.

The following sections describe how to add a property and property value to a data field, and how to remove them from the data field.

Note:

The Properties tab is 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.

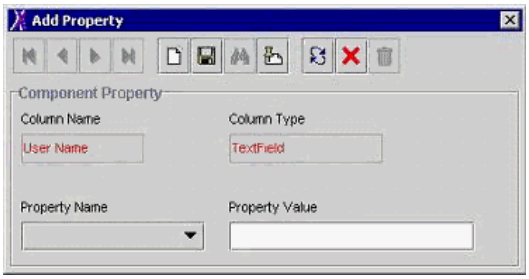
Adding a Property and Property Value to a Data Field

To add a property and property value to a Data Field:

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 appears, 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 in the Column Name field). In addition, the data type of this field is a text field.

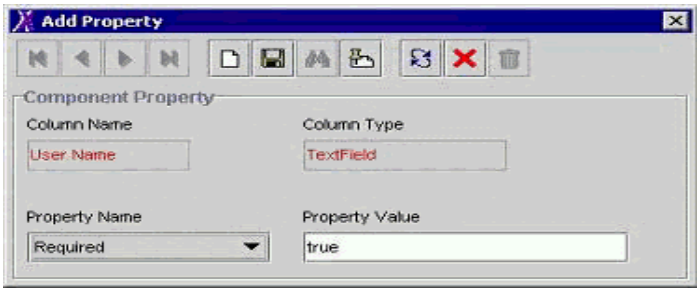
The following table will help you understand the various regions of the Add Property dialog box.

Name	Description
Column Name	The name of the data field.
Column Type	The data type of the data field.
Property Name	From this 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 in the Property Name box.

Note: The menu items displayed in the Property Name 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.

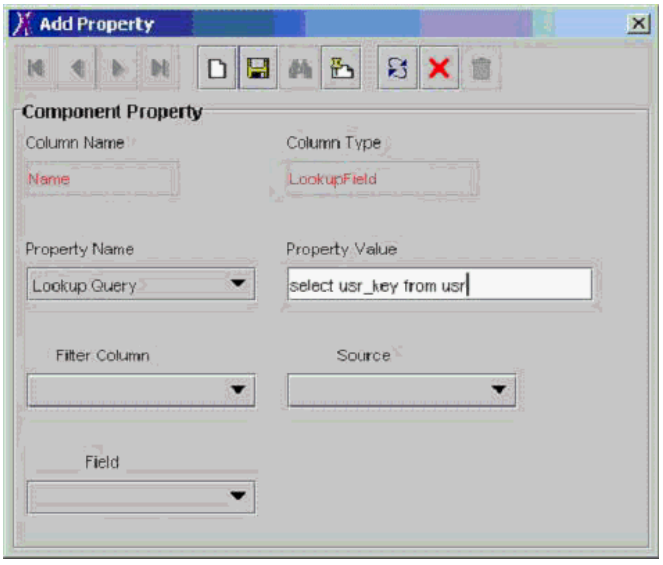
Adding a Property and Property Value for Customized Look Up Query

To add a property and property value for customized lookup query:

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 appears, 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 in the **Column Name** field). In addition, the data type of this field is a lookup field.

The 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 describes the 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.

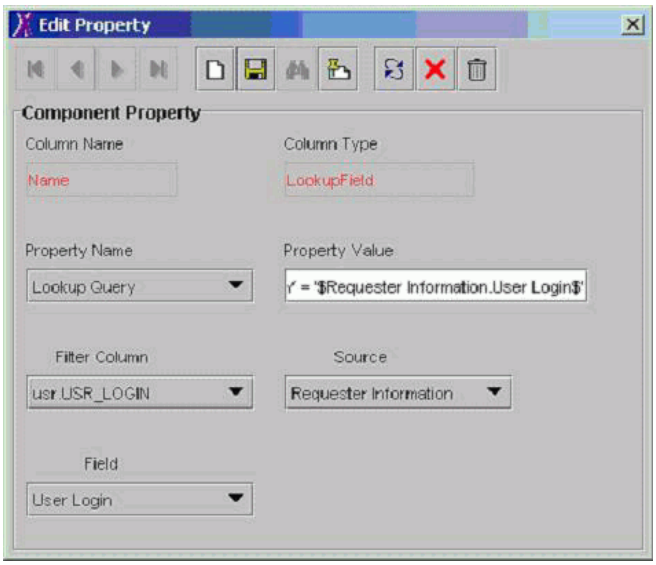
Name	Description
Column Name	The name of the data field.
Column Type	The data type of the data field.
Property Name	From this box, select the property for the data field.
Property Value	In this text box, enter the property value, which is associated with the property that appears in the P**roperty Name** 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 in the **Filter Column** 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 in the **Property Name** box reflect the data type of the selected data field.

Also, the **Source** and **Field** boxes of the Add Property dialog box are applicable only when **Lookup Query** appears in 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



Removing a Property and Property Value From a Data Field

To remove a property and property value from a data field:

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 Tab

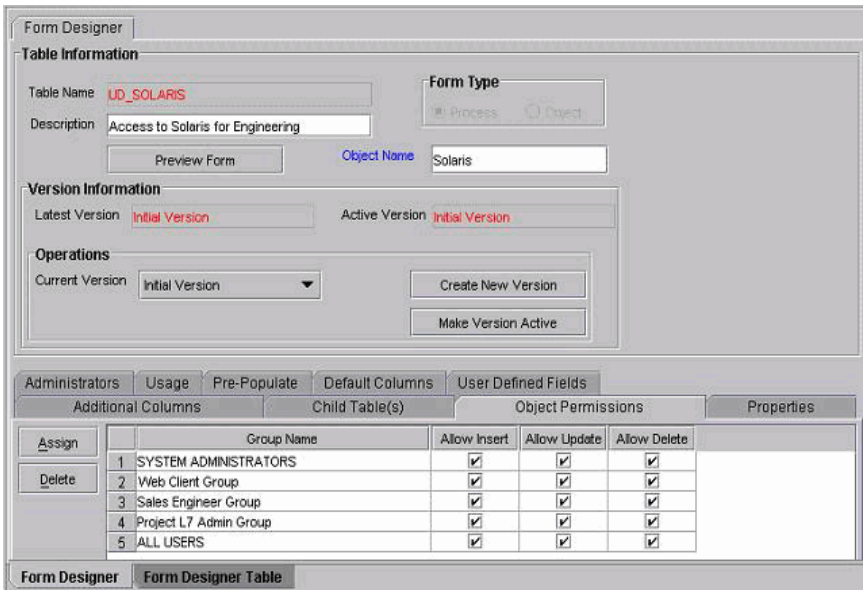
This tab is used to select the user groups that can view, modify, and delete the current record of the form that was created by a user using the Form Designer form.

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.

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.

Figure 9–12 displays the Administrators tab of the Form Designer Form.

Figure 9–12 The Administrators Tab of the Form Designer Form



The following sections describe 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.

Assigning 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 appears.

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.

Removing User Group Privileges for a Record of a User-Created Form

To remove administrative privileges from a user group for a record of a user-created form:

1. Highlight the user group that you want to remove.

2. Click **Delete**.

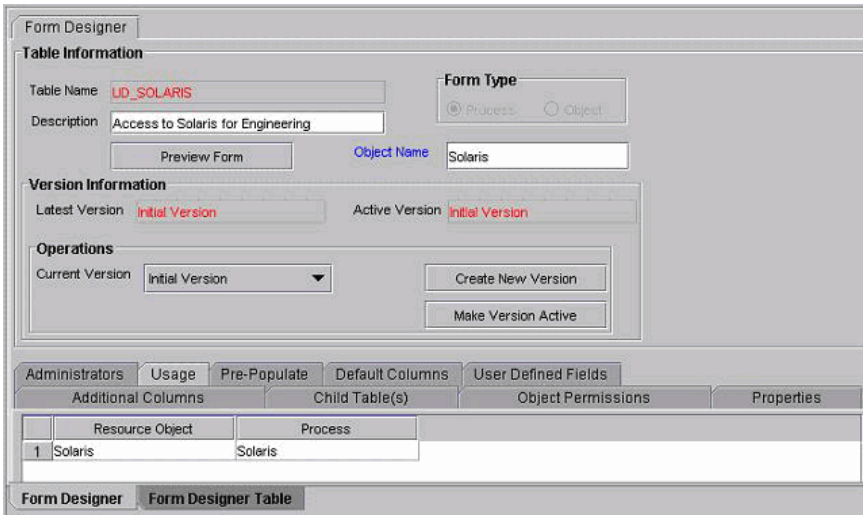
The user group no longer has administrative privileges for this record of the user-created form.

Usage Tab

In this tab, you can see the resource objects and/or processes to which the current form has been assigned.

Figure 9–13 displays the Usage tab of the Form Designer Form.

Figure 9–13 The Usage Tab of the Form Designer Form



For 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 Tab

You use this tab is to do the following:

- 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 Tab

A form that is created 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 Tab

This tab is used to view and access any user-defined fields that were 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.

Creating 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.

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** 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 appears.
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. From this toolbar, click **Close**.

   The additional version of the form is created. When you click the Current Version 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.

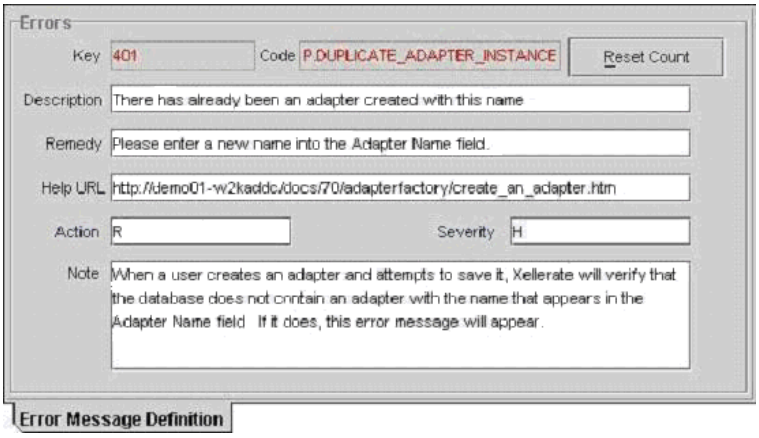
The Error Message Definition Form

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.

The following section describes how to create an error message.

Creating an Error Message

When you create an error message, Oracle Identity Manager populates the **Key** field with a unique identification number. When a condition arises that causes the error message to appear, the text in the **Description** field appears in a dialog box.

The following procedure describes how to create an error message.

> **Tip:** After you create an error message definition, to reset the count of how many times the error message has appeared, click the **Reset Count** button. This resets the count to 0.

To create an error message:

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, enter explanatory information about the error message.
9. Click **Save**.

   The error message is created.

10

Business Rule Definition

This chapter describes the Business Rule Definition of Design Console. It contains the following topics:

Overview

The Development Tools/Business Rule Definition folder provides System Administrators and developers with tools 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

This form appears in the Development Tools/Business Rule Definition folder. You use this form 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 that Oracle Identity Manager can recognize it.

There are two types of event handlers:

- Event handlers that are created through the Adapter Factory form. These begin with the letters "adp." They are known as adapters.
- Event handlers that are created internally in Oracle Identity Manager. These begin with the letters "tc." They are referred to as system event handlers.

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 as follows:

- **Pre-Insert**: Before information is added to the database

- **Pre-Update**: Before information is modified in 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 in the database
- **Post-Delete**: After information is removed from the database

Figure 10–1 displays the Event Handler Manager form.

Figure 10–1 Event Handler Manager Form

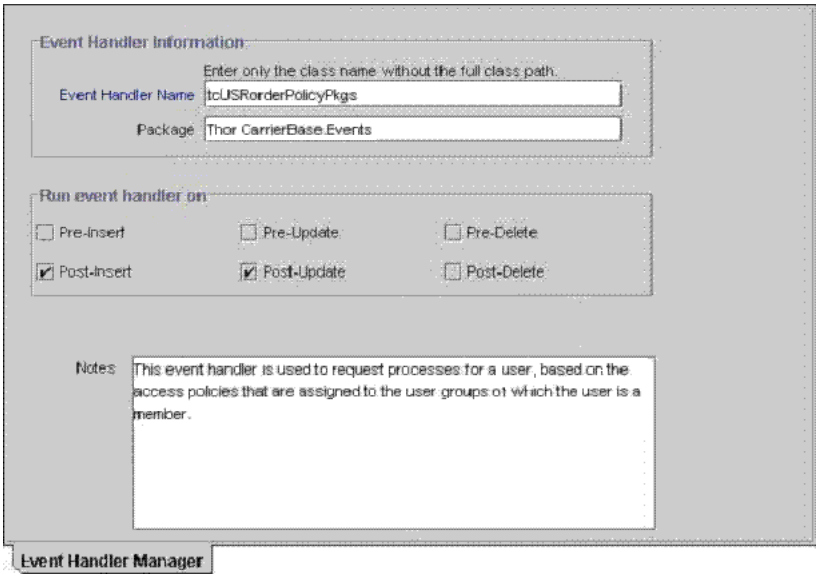


Table 10–1 describes the data fields of Event Handler Manager form.

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.
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 in 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 in the database.

Table 10–1 (Cont.) Data Field

Field Name	Descriptions
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.

The following sections describe how to create and modify event handlers.

Note: To 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.

Caution: Any event handler that begins with the letters "adp" is associated with adapters, and should not be modified. However, you can modify system event handlers. These event handlers that begin with the letters "tc".

Adding or Modifying an Event Handler

To add or modify an event handler:

1. Open the Event Handler Manager form.
2. To add an event handler to Oracle Identity Manager, enter the name of the event handler into the **Event Handler Name lookup** field.

   To 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 want to edit.
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.

   You can schedule an event handler 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 is triggered at that time, for example, on pre-insert. It signifies that the event handler can run at that time.
5. In the **Notes** area, add or edit explanatory information about the event handler.
6. Click **Save**.

   The event handler is added or modified.

The Data Object Manager Form

The Data Object Manager form appears in the Development Tools/Business Rule Definition folder. You use this form to do the following:

- Assign a rule generator adapter, entity adapter, or an event handler to an object that can add, modify, or delete data in the database.

  This type of object is known as a data object.

  Schedule the adapter or event handler to run according to a schedule (pre-insert, pre-update, pre-delete, post-insert, post-update, or post-delete).

  Organize the order in which Oracle Identity Manager triggers adapters or event handlers that belong to the same execution schedule.

  View 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.

  > **Tip:** For more information on adapter variables, rule generator adapters, and entity adapters, refer to the *Oracle Identity Manager Tools Reference Guide*.

Figure 10–2 displays the Data Object Manager form.

Figure 10–2 Data Object Manager Form

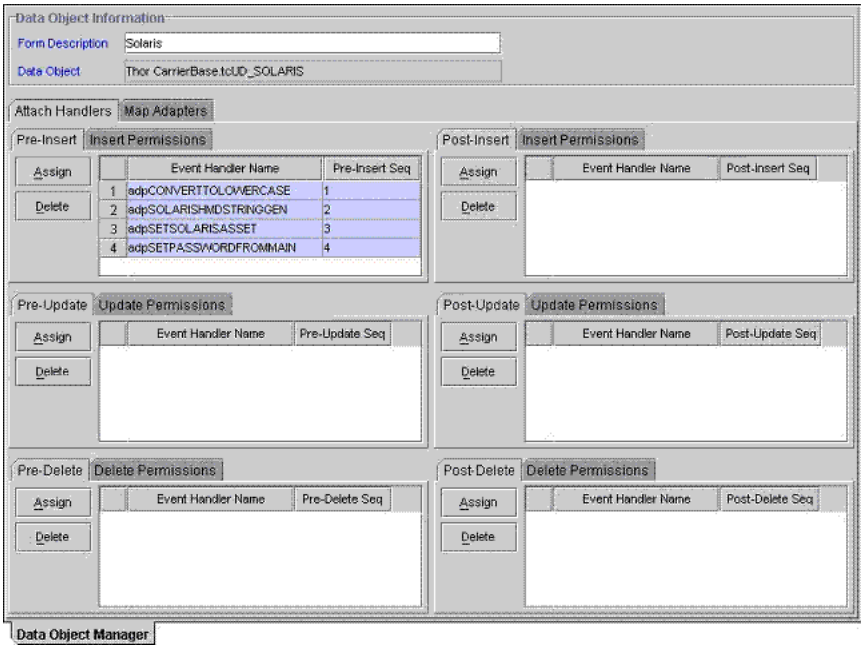


Table 10–2 describes the data fields of the Data Object Manager form.

Table 10–2 Data Field

Field	Description
Form Description	The name of the form that 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.

The following section describes how to select the target data object to which a rule generator adapter, entity adapter, or event handler will be assigned.

Selecting a Target Data Object

To select a target data object:

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

After 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 described in the following sections.

Attach Handlers Tab

You use this tab to select the rule generator adapters, entity adapters, or event handlers that will be assigned to or removed from a data object. This includes the foloowing:

- Specifying when Oracle Identity Manager triggers the assigned event handlers or adapters (on pre-insert, pre-update, pre-delete, post-insert, post-update, or post-delete).
- Setting the order in which Oracle Identity Manager triggers 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 example, Oracle Identity Manager can trigger the `adpCONVERTTOLOWERCASE`, `adpSOLARISHMDSTRINGGEN`, `adpSETSOLARISASSET`, and `adpSETPASSWORDFROMMAIN` adapters on pre-insert. Based on the sequence numbers of these adapters, Oracle Identity Manager triggers 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 sections discuss these procedures:

- Assigning an event handler, rule generator adapter, or entity adapter to a data object
- Organizing the execution schedule of event handlers or adapters
- Removing an event handler, rule generator adapter, or entity adapter from a data object

Assigning an Event Handler or Adapter to a Data Object

To assign an event handler or adapter:

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 appears.

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.

Organizing the Execution Schedule of Event Handlers or Adapters

To organize the execution schedule:

1. Highlight the event handler or adapter whose execution schedule you wish to change.
2. Click **Assign**.

   The Assignment dialog box appears.

3. Highlight the event handler or adapter.
4. If you click **Up**, the selected event handler or adapter will switch places and sequence numbers with the event handler or adapter that precedes it.

   If you click **Down**, the highlighted event handler or adapter will trade places and sequence numbers with the event handler or adapter that follows it.

5. Repeat Steps 3-4 until all event handlers and adapters have the appropriate sequence numbers.
6. Click **OK**.

   The event handlers and adapters will now be triggered in the proper order for the execution schedule or schedules that you organized.

Removing an Event Handler or Adapter From a Data Object

To remove an event handler or adapter:

1. Highlight the desired event handler or adapter.
2. Click **Delete**.

   The event handler or adapter is removed.

Map Adapters Tab

The Map Adapters tab becomes operational only after you assign a rule generator adapter or entity adapter to the data object.

You use this tab to map the variables of a rule generator or entity adapter to their proper source and target locations. For example, suppose the **adpSOLARISUSERIDGENERATOR** adapter has three variables: firstname, Adapter return value, and lastname. If a "Y" appears in the Mapped column for each adapter variable, this signifies that all three variables are 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 successfully compiled and all of its variables are mapped correctly.
- **Mapping Incomplete**: This adapter has successfully compiled, but at least one of its variables has been not mapped correctly.
- **Mapping Incomplete**: This adapter has successfully compiled, but at least one of its variables has been not mapped correctly.

For more information on compiling adapters and mapping its variables, see 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. You use this form to define rules that are invoked at the following times:

- When Oracle Identity Manager attempts to determine which user or organization record is associated with a change on a trusted source. These rules are evaluated as soon as all required fields in the reconciliation event are processed on the Reconciliation Data tab of the Reconciliation Manager form.
- When Oracle Identity Manager attempts 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 are evaluated only when all required fields in the reconciliation event are processed on the Reconciliation Data tab of the Reconciliation Manager form, and no processes were matched to the event on the Processes Matched Tree tab of the same form.

As mentioned, rules defined using this form are 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 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.

Defining a Reconciliation Rule

The following procedure describes how to define a reconciliation rule.

Note: In the following procedure, 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, you can only set this checkbox after Oracle Identity Manager has selected the **Valid** system checkbox. The **Valid** checkbox is only be selected after you have created at least one rule element and Oracle Identity Manager has determined that the logic of this rule element is valid.

To define reconciliation rules for user or organization matching:

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, all elements (and rules if they are 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.

Adding a Rule Element

To define individual elements in a reconciliation rule:

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 appears.
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 examines 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. The following are valid operators:

   - **Equals**: If you select this option, 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.

6. Select a value from the **Attribute** menu. The values in this menu are the fields that were 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 fields associated with parent tables of the resource's custom process form are available for selection in the **Attribute** field.

7. 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, after 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

8. Set the **Case-Sensitive** check box.

   For the rule element to be satisfied, if this check box is selected, the value selected in the **Attribute** field must exactly match the capitalization of the value being evaluated in the reconciliation event record. If this check box is cleared, 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.

9. Click **Save**.

10. 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.

11. Repeat this entire procedure for each rule element you wish to add to the rule.

Note: Ensure that the Active checkbox is selected.

Nesting a Rule Within a Rule

You can nest an existing rule within a rule. Oracle Identity Manager evaluates the criteria of the nested rule in the same manner as any other element of the rule.

Note: Only reconciliation-related rules that are associated with the same resource object are available for selection in the dialog box.

To nest a rule within a rule:

1. Access the rule to which you want to add another rule.
2. Click **Add Rule** on the Rule Elements tab.
3. The Rule Choice lookup dialog box appears.

   Locate and select the desired rule.
4. Click **OK**.

   The selected reconciliation rule is added to rule.
5. Repeat steps 2-4 for each rule you wish to nest in the rule.

Deleting a Rule Element or Rule

To delete a rule element or a rule:

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 activities performed in the application. You can customize the level of information that is placed in these log files, the location where these log files reside, and the frequency of archiving the information in these files using configuration files. Oracle Identity Manager also provides logs files that contain standard error and standard out messages.

You can use the logs files created by Oracle Identity Manager to track activities being performed in the various modules (for example, adapter factory, task scheduler) of the application and monitor error messages and queries performed against the database. Both of these activities can be helpful when troubleshooting potential problems or testing anticipated application behavior.

You can control the following:

- The level of information, that is, greater or lesser amount of detail, that is written to the logs.
- Whether the logs are periodically archived and, if so, if 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.

Log file locations and properties are controlled by a properties file named log.properties, which is located in the <XL_DC_HOME>/xlclient/config/ directory.

Setting Log Levels

Oracle Identity Manager uses log4j for logging. Logging levels for Design Console are configured in the <XL_DC_HOME>\xlclient\config\log.properties logging properties file. By default, all Oracle Identity Manager components are configured to output at the Warning level. You can change the log level universally for all components or for an individual component, such as Design Console.

Oracle Identity Manager components are listed in the <XL_DC_HOME>\xlclient\config\log.properties file in the XELLERATE section, for example:

```
log4j.logger.XELLERATE=WARN
log4j.logger.XELLERATE.DDM=DEBUG
log4j.logger.XELLERATE.ACCOUNTMANAGEMENT=DEBUG
log4j.logger.XELLERATE.SERVER=DEBUG
log4j.logger.XELLERATE.RESOURCEMANAGEMENT=DEBUG
log4j.logger.XELLERATE.REQUESTS=DEBUG
log4j.logger.XELLERATE.WORKFLOW=DEBUG
log4j.logger.XELLERATE.WEBAPP=DEBUG
log4j.logger.XELLERATE.SCHEDULER=DEBUG
log4j.logger.XELLERATE.SCHEDULER.Task=DEBUG
log4j.logger.XELLERATE.ADAPTERS=DEBUG
log4j.logger.XELLERATE.JAVACLIENT=DEBUG
log4j.logger.XELLERATE.POLICIES=DEBUG
log4j.logger.XELLERATE.RULES=DEBUG
log4j.logger.XELLERATE.DATABASE=DEBUG
log4j.logger.XELLERATE.APIS=DEBUG
log4j.logger.XELLERATE.OBJECTMANAGEMENT=DEBUG
log4j.logger.XELLERATE.JMS=DEBUG
log4j.logger.XELLERATE.REMOTEMANAGER=DEBUG
log4j.logger.XELLERATE.CACHEMANAGEMENT=DEBUG
log4j.logger.XELLERATE.ATTESTATION=DEBUG
log4j.logger.XELLERATE.AUDITOR=DEBUG
```

To set Design log levels, edit the <XL_DC_HOME>\xlclient\config\log.properties logging properties file as follows:

1. Open the <XL_DC_HOME>\xlclient\config\log.properties file in a text editor. This file contains a general setting for Oracle Identity Manager and specific settings for the components and modules that comprise Oracle Identity Manager.

   By default, Oracle Identity Manager is configured to output at the Warning level:

   ```
   log4j.logger.XELLERATE=WARN
   ```

   This is the general value for Oracle Identity Manager. Individual components and modules are listed following the general value in the properties file. You can set individual components and modules to different log levels. The log level for a specific component overrides the general setting.

2. Set the general value to the desired log level. The following is a list of the supported log levels, appearing in descending order of information logged (DEBUG logs the most information and FATAL logs the least information):

   - DEBUG
   - INFO
   - WARN
   - ERROR
   - FATAL

3. Individual components or modules can have different log levels. For example, the following values set the log level for Design Console to DEBUG:

   ```
   log4j.logger.XELLERATE=WARN
   log4j.logger.XELLERATE.ACCOUNTMANAGEMENT=INFO
   log4j.logger.XELLERATE.JAVACLIENT=DEBUG
   ```

4. Save your changes.

5. Restart Design Console so that the changes take effect.

A

Reference

This appendix describes the various tables in Design Console.

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

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	**Organization Provisioning; 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.

EMail Variables

The following table lists the variables that can be used to create email 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 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.
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 in 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 in 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 in 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 columns appears in the Lookup window.
		
		To correctly display the data returned from a query, you must add a `lookupfield.header` property to the xlWebAdmin_locale.properties file. For example, consider the following SQL query: select usr_status from usr. To view the data returned from the query, you must add the following entry to the xlWebAdmin_ locale.properties files:
		
		`lookupfield.header.users.status=User Status`
		
		If the xlWebAdmin_locale.properties file does not contain a `lookupfield.header` property for your specified query, then the Administrative and User Console displays a lookup window after you click the corresponding lookup icon.
		
		The syntax for a `lookupfield.header` property is as follows:
		
		`lookupfield.header.`*`column_code`*`=display value`
		
		The *column_code* portion of the entry must be lowercase and any spaces must be replaced by underscore characters (_).
		
		By default, the following entries for lookup field column headers are already available in the system resource bundle:
		
		`lookupfield.header.lookup_definition.lookup_ code_information .code_key=Value`
		`lookupfield.header.lookup_definition.lookup_code_information .decode=Description`
		`lookupfield.header.users.manager_login=User ID`
		`lookupfield.header.organizations.organization_ name=Name`
		`lookupfield.header.it_resources.key=Key`
		`lookupfield.header.it_resources.name=Instance Name`
		`lookupfield.header.users.user_id=User ID`
		`lookupfield.header.users.last_name=Last Name`
		`lookupfield.header.users.first_name=First Name`
		`lookupfield.header.groups.group_name=Group Name`
		`lookupfield.header.objects.name=Resource Name`
		`lookupfield.header.access_policies.name=Access Policy Name`

Data Type	Data Property	Description
Lookup Field	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 in the Lookup Code property supersedes any values set in 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.
	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	In 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 box appears in the **Property Value** text box. From this 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.

Data Type	Data Property	Description
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.
Text Area (Display Only)	Number of Rows	In 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**).
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.

Data Type	Data Property	Description
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 box, including box items and the text that appears with the 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 in the **Lookup Code** property supersedes any values set in 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 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.
	Visible Field	If you want this 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 in 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 in 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
Base Help URL	The location of the online Help files.	XL.BaseHelpUrl	//docs/thortech.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

Name	Description	Keyword	Value	S*	Run On
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
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\JA VA		C
JavaDoc Executable Location	Needs to be set for generating a form and indicates the location of the JavaDoc executable file.	SDK.JAVADO C_CMD	C:\JDK1.3\BI N\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\JA VA		C

Name	Description	Keyword	Value	S*	Run On
User Id reuse property	Determines whether a deleted user account can be reused. To reuse a deleted user account, assign this property a value of TRUE and drop the unique index for the `USR_LOGIN` column in the `USR` table and create a non-unique index. To prevent a user account from being reused, assign this property a value of FALSE.	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
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

Name	Description	Keyword	Value	S*	Run On
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
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

Name	Description	Keyword	Value	S*	Run On
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.MaxPasswordResetAttempts	3	v	
Self Registration Email From Address		XL.SelfRegistrationEmailFromAddress	selfreg@xlselfreg.com	v	
Profile Edit Email From Address		XL.ProfileEditEmailFromAddress	selfreg@xlselfreg.com	v	S
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 in the provisioning process, becoming active in the Tasks tab of the Process Definition. Any adapter that is associated with this provisioning process runs. 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 functions 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 systems. When running fvcutil.cmd, you must provide the Oracle Identity Manager database administrator password as a command-line argument.

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 utility prompts you for the Oracle Identity Manager database administrator password. 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.
- The utility can only be used to update custom process forms when a value of "Active Version" is assigned to the `ToVersion` property in the fvc.properties file.
- Default values for new fields must be defined in the property files.

Index

K

L

M

N

O

P

Q

R

S

T

U

W