

# **Oracle® Identity Manager**

Design Console Guide

Release 9.1.0.2

**E14762-01**

May 2009

Oracle Identity Manager Design Console Guide, Release 9.1.0.2

E14762-01

Copyright © 2009, Oracle and/or its affiliates. All rights reserved.

Primary Author: Lyju Vadassery

Contributing Author: Debapriya Datta

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This software and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

---

---

# Contents

<b>Preface</b> .....	xv
Audience .....	xv
Documentation Accessibility .....	xv
Related Documents .....	xvi
Documentation Updates .....	xvi
Conventions .....	xvi
Online Help .....	xvi
 <b>1 Oracle Identity Manager Architecture</b>	
1.1 Overview of Oracle Identity Manager Architecture .....	1-1
1.2 Benefits and Key Features of Oracle Identity Manager .....	1-1
1.3 Three Tiers of Oracle Identity Manager .....	1-2
1.3.1 Tier 1: Client .....	1-3
1.3.2 Tier 2: Application Server .....	1-3
1.3.3 Tier 3: Database .....	1-3
 <b>2 Design Console Main</b>	
2.1 Starting the Design Console .....	2-1
2.2 Overview of the Design Console .....	2-2
2.3 Design Console Menu Bar .....	2-2
2.3.1 File Menu .....	2-2
2.3.2 Edit Menu .....	2-3
2.3.3 Toolbar Menu .....	2-3
2.3.4 Help Menu .....	2-3
2.4 Design Console Toolbar .....	2-4
2.5 Design Console Shortcuts .....	2-4
2.6 Design Console Explorer .....	2-5
2.7 Design Console Workspace .....	2-6
 <b>3 Basic Functions in the Design Console</b>	
3.1 Special Field and Form Types .....	3-1
3.1.1 Data Fields .....	3-1
3.1.2 Lookup Fields .....	3-2
3.1.3 Date and Time Fields .....	3-2
3.1.4 List .....	3-3

3.1.5	Notes Window .....	3-3
3.1.6	Tabs on Forms .....	3-3
3.2	Assignment Windows .....	3-4
3.3	Performing a Search.....	3-5
3.4	Constructing a Search Filter .....	3-5
3.5	Results of a Search .....	3-6
3.6	Working with a Set of Query Results.....	3-6
3.7	Optimizing Query Performance .....	3-6
3.8	Exceeding the Limit for a Result Set .....	3-7

## 4 User Management

4.1	Overview of User Management.....	4-1
4.2	Organizational Defaults Form .....	4-1
4.3	Policy History Form .....	4-2
4.3.1	Policy History Tab .....	4-3
4.4	Assigning Group Entitlements .....	4-4
4.4.1	Pre-Existing Groups .....	4-5
4.4.1.1	System Administrators User Group .....	4-5
4.4.1.2	Operators User Group .....	4-6
4.4.1.3	All Users User Group.....	4-6
4.4.1.4	Self Operators Group .....	4-6
4.5	Administrative Queues Form .....	4-6
4.6	Reconciliation Manager Form .....	4-6
4.6.1	Viewing and Managing Reconciliation Events .....	4-10
4.6.2	Tabs on the Reconciliation Manager Form .....	4-11
4.6.2.1	Reconciliation Data Tab.....	4-11
4.6.2.1.1	Processed Data .....	4-11
4.6.2.1.2	Unprocessed Data .....	4-12
4.6.2.1.3	Mapping or Correcting Unprocessed Fields .....	4-13
4.6.2.2	Processes Matched Tree (for target resources only) .....	4-14
4.6.2.2.1	Linking a Provisioning Process Instance to the Reconciliation Event.....	4-15
4.6.2.3	Matched Users Tab.....	4-15
4.6.2.3.1	Linking a User Record to the Reconciliation Event.....	4-15
4.6.2.4	Matched Organizations Tab.....	4-16
4.6.2.4.1	Linking an Organization Record to the Reconciliation Event .....	4-16
4.6.2.5	Reconciliation Event History .....	4-17

## 5 Resource Management

5.1	Overview of Resource Management.....	5-1
5.2	IT Resources Type Definition Form .....	5-1
5.2.1	Defining a Template (a Resource Type) for IT Resources .....	5-2
5.2.2	Tabs on the IT Resource Type Definition Form .....	5-3
5.2.2.1	IT Resource Type Parameter Tab .....	5-3
5.2.2.2	IT Resource Tab .....	5-4
5.2.3	IT Resource Type Definition Table .....	5-4
5.3	IT Resources Form .....	5-4
5.3.1	Defining an IT Resource .....	5-4

5.3.2	Setting Access Permissions to an IT Resource Instance Parameter .....	5-5
5.4	Rule Designer Form .....	5-5
5.4.1	Creating a Rule.....	5-8
5.4.2	Tabs on the Rule Designer Form .....	5-9
5.4.2.1	Rule Elements Tab .....	5-9
5.4.2.2	Usage Tab .....	5-11
5.4.3	Rule Designer Table .....	5-12
5.5	Resource Objects Form.....	5-13
5.5.1	Creating a Resource Object .....	5-16
5.5.2	Tabs on the Resource Objects Form .....	5-18
5.5.2.1	Depends On Tab .....	5-18
5.5.2.2	Object Authorizers Tab .....	5-19
5.5.2.3	Process Determination Rules Tab .....	5-20
5.5.2.4	Event Handlers/Adapters Tab.....	5-21
5.5.2.5	Resource Audit Objectives .....	5-22
5.5.2.6	Status Definition Tab.....	5-22
5.5.2.7	Administrators Tab .....	5-24
5.5.2.8	Password Policies Rule Tab .....	5-25
5.5.2.9	User-Defined Fields Tab .....	5-26
5.5.2.10	Process Tab .....	5-26
5.5.2.11	Object Reconciliation Tab .....	5-26
5.5.3	Multiple Trusted Source Reconciliation .....	5-30
5.5.3.1	Multiple Trusted Source Reconciliation Using MTS-Compatible Connectors.	5-31
5.5.3.2	Multiple Trusted Source Reconciliation Using Connectors That Are Not MTS-Compatible	5-33
5.6	Service Account Management.....	5-38

## 6 Process Management

6.1	Overview of Process Management.....	6-1
6.2	Email Definition Form.....	6-1
6.2.1	Specifying the E-Mail Server .....	6-2
6.2.2	Email Definition Form .....	6-3
6.2.3	Creating an E-Mail Definition.....	6-4
6.3	Process Definition Form.....	6-6
6.3.1	Creating a Process Definition.....	6-8
6.3.2	Tabs on the Process Definition Form .....	6-9
6.3.2.1	Tasks Tab .....	6-9
6.3.2.1.1	Adding a Process Task.....	6-10
6.3.2.1.2	Editing a Process Task .....	6-10
6.3.2.1.3	Deleting a Process Task .....	6-10
6.3.2.2	Data Flow Tab .....	6-11
6.3.2.2.1	Mapping a Parent Resource Form Field to a Process Form Field .....	6-12
6.3.2.2.2	Mapping a Child Resource Form Field to Child Process Form Field .....	6-12
6.3.2.2.3	Breaking the Mapping Between Data Fields of a Resource Object and a Process	6-12
6.3.2.3	Reconciliation Field Mappings Tab .....	6-13
6.3.2.3.1	User Account Status Reconciliation.....	6-14

6.3.2.3.2	Mapping a Target Resource Field to Oracle Identity Manager .....	6-14
6.3.2.3.3	Deleting a Mapping .....	6-16
6.3.2.4	Administrators Tab .....	6-16
6.3.2.4.1	Assigning a User Group to a Process Definition .....	6-16
6.3.2.4.2	Removing a User Group From a Process Definition.....	6-17
6.3.3	Modifying Process Tasks .....	6-17
6.3.3.1	General Tab .....	6-17
6.3.3.1.1	Modifying a Process Task's General Information.....	6-19
6.3.3.2	Integration Tab.....	6-21
6.3.3.2.1	Assigning an Adapter or Event Handler to a Process Task.....	6-22
6.3.3.2.2	Mapping Adapter Variables .....	6-23
6.3.3.2.3	Removing an Adapter or Event Handler from a Process Task .....	6-23
6.3.3.3	Task Dependency Tab.....	6-23
6.3.3.3.1	Assigning a Preceding Task to a Process Task.....	6-24
6.3.3.3.2	Removing a Preceding Task from a Process Task .....	6-24
6.3.3.3.3	Assigning a Dependent Task to a Process Task.....	6-24
6.3.3.3.4	Removing a Dependent Task from a Process Task .....	6-24
6.3.3.4	Responses Tab.....	6-25
6.3.3.4.1	Adding a Response to a Process Task .....	6-25
6.3.3.4.2	Removing a Response from a Process Task.....	6-25
6.3.3.4.3	Assigning a Generated Task to a Process Task.....	6-26
6.3.3.4.4	Removing a Generated Task From a Process Task.....	6-26
6.3.3.5	Undo/Recovery Tab .....	6-26
6.3.3.5.1	Assigning an Undo Task to a Process Task .....	6-27
6.3.3.5.2	Removing an Undo Task From a Process Task.....	6-27
6.3.3.5.3	Assigning a Recovery Task to a Process Task.....	6-27
6.3.3.5.4	Removing a Recovery Task from a Process Task .....	6-28
6.3.3.6	Notification Tab .....	6-28
6.3.3.6.1	Assigning an E-Mail Notification to a Process Task .....	6-28
6.3.3.6.2	Removing an E-mail Notification from a Process Task .....	6-29
6.3.3.7	Task to Object Status Mapping Tab .....	6-29
6.3.3.7.1	Mapping a Process Task Status to a Provisioning Status .....	6-30
6.3.3.7.2	Unmapping a Process Task Status From a Provisioning Status.....	6-30
6.3.3.8	Assignment Tab of the Editing Task Window .....	6-30
6.3.3.8.1	Adding a Rule to a Process Task.....	6-32
6.3.3.8.2	Removing a Rule from a Process Task .....	6-33

## 7 Administering Oracle Identity Manager with the Design Console

7.1	Overview of Design Control Administration .....	7-1
7.2	Form Information Form .....	7-2
7.2.1	Adding an Oracle Identity Manager Form or Folder .....	7-3
7.2.2	Modifying the Design Console Explorer.....	7-4
7.3	Lookup Definition Form .....	7-4
7.3.1	Creating a Lookup Definition .....	7-6
7.3.2	Lookup Code Information Tab .....	7-6
7.3.2.1	Creating and Modifying a Lookup Value.....	7-6
7.3.2.2	Deleting a Lookup Value.....	7-7

7.4	User Defined Field Definition Form.....	7-7
7.4.1	Selecting the Target Form for a User-Defined Field .....	7-8
7.4.2	Tabs on the User Defined Field Definition Form .....	7-9
7.4.2.1	User Defined Columns Tab.....	7-9
7.4.2.2	Properties Tab .....	7-12
7.4.2.3	Administrators Tab .....	7-13
7.5	System Configuration Form .....	7-14
7.5.1	Creating and Editing an Instance of a Property Definition.....	7-15
7.5.2	Assigning a User or Group to an Instance of a Property Definition.....	7-16
7.5.3	Removing a User or Group from an Instance of a Property Definition.....	7-17
7.6	Remote Manager Form.....	7-17
7.7	Password Policies Form .....	7-18
7.7.1	Creating a Password Policy.....	7-19
7.7.2	Tabs on the Password Policies Form .....	7-19
7.7.2.1	Policy Rules Tab.....	7-19
7.7.2.2	Usage Tab .....	7-25
7.8	Task Scheduler Form.....	7-26
7.8.1	Predefined Scheduled Tasks .....	7-28
7.8.2	Creating a Scheduled Task.....	7-31
7.8.2.1	Adding a Task Attribute.....	7-32
7.8.2.2	Removing a Task Attribute .....	7-32
7.8.3	Deleting a Custom Scheduled Task .....	7-32

## 8 Development Tools

8.1	Overview of Developments Tools.....	8-1
8.2	Adapter Factory Form.....	8-2
8.3	Adapter Manager Form .....	8-2
8.4	Form Designer Form.....	8-2
8.4.1	Creating a Form .....	8-5
8.4.2	Tabs of the Form Designer Form.....	8-5
8.4.2.1	Additional Columns Tab.....	8-5
8.4.2.1.1	Adding a Data Field to a Form.....	8-8
8.4.2.1.2	Removing a Data Field From a Form .....	8-9
8.4.2.2	Child Table(s) Tab .....	8-10
8.4.2.2.1	Assigning a Child Table to a Form .....	8-11
8.4.2.2.2	Removing a Child Table from a Form.....	8-11
8.4.2.3	Object Permissions Tab.....	8-12
8.4.2.3.1	Assigning a User Group to a User-Created Form .....	8-12
8.4.2.3.2	Removing a User Group From a User-Created Form .....	8-13
8.4.2.4	Properties Tab .....	8-13
8.4.2.4.1	Adding a Property and Property Value to a Data Field.....	8-14
8.4.2.4.2	Adding a Property and Property Value for Customized Look up Query .	8-15
8.4.2.4.3	Removing a Property and Property Value From a Data Field .....	8-18
8.4.2.5	Administrators Tab .....	8-18
8.4.2.5.1	Assigning Privileges to a User Group for a Record of a User-Created Form.....	8-18
8.4.2.5.2	Removing User Group Privileges for a Record of a User-Created Form...	8-19

8.4.2.6	Usage Tab .....	8-19
8.4.2.7	Pre-Populate Tab .....	8-20
8.4.2.8	Default Columns Tab .....	8-20
8.4.2.9	User Defined Fields Tab .....	8-20
8.4.3	Creating an Additional Version of a Form .....	8-20
8.5	Error Message Definition Form .....	8-21
8.5.1	Creating an Error Message .....	8-22

## **9 Business Rule Definition**

9.1	Overview of Business Rule Definition.....	9-1
9.2	Event Handler Manager Form .....	9-1
9.3	Data Object Manager Form .....	9-3
9.3.1	Tabs of the Data Object Manager Form.....	9-5
9.3.1.1	Attach Handlers Tab .....	9-5
9.3.1.1.1	Assigning an Event Handler or Adapter to a Data Object .....	9-6
9.3.1.1.2	Organizing the Execution Schedule of Event Handlers or Adapters .....	9-6
9.3.1.1.3	Removing an Event Handler or Adapter from a Data Object .....	9-6
9.3.1.2	Map Adapters Tab.....	9-6
9.4	Reconciliation Rules Form.....	9-7
9.4.1	Defining a Reconciliation Rule .....	9-7
9.4.2	Adding a Rule Element.....	9-8
9.4.3	Nesting a Rule Within a Rule.....	9-10
9.4.4	Deleting a Rule Element or Rule .....	9-10

## **10 Oracle Identity Manager Logging Functions**

10.1	Overview of Oracle Identity Manager Logging Functions.....	10-1
10.2	Setting Log Levels.....	10-1

## **A Reference**

## **B Service Account Management**

## **C Form Version Control Utility**

C.1	FVC Utility Scope.....	C-1
C.2	FVC Utility Content.....	C-1
C.3	FVC Utility Description .....	C-2
C.4	FVC Utility Features .....	C-2

## **Index**





## List of Figures

1-1	Oracle Identity Manager Three-Tier Architecture .....	1-2
2-1	Design Console Main Screen .....	2-2
2-2	Design Console Toolbar .....	2-4
2-3	Design Console Explorer .....	2-6
2-4	Design Console Workspace .....	2-7
2-5	Table View .....	2-8
3-1	Lookup Dialog Box .....	3-2
3-2	Design Console - Tab on Forms .....	3-4
3-3	Displaying the Results of a Search Query .....	3-5
3-4	Multiple Records Returned .....	3-6
3-5	Query Size Exceeded Dialog Box.....	3-7
4-1	Organizational Defaults Form .....	4-2
4-2	Policy History Form.....	4-3
4-3	Reconciliation Manager Form .....	4-7
5-1	The IT Resources Type Definition Form.....	5-2
5-2	Rule Designer Form .....	5-6
5-3	Rule Elements Tab of the Rule Designer Form.....	5-9
5-4	Edit Rule Element Window .....	5-10
5-5	Usage Tab of the Rule Designer Form .....	5-11
5-6	Rule Designer Table.....	5-12
5-7	Trusted Source Reconciliation by User Type.....	5-36
5-8	Trusted Source Reconciliation for Specific OIM User Attributes .....	5-38
6-1	Email Definition Form.....	6-2
6-2	Process Definition Form.....	6-6
6-3	Tasks Tab of the Process Definition Form.....	6-10
6-4	Data Flow Tab of the Process Definition Form.....	6-11
6-5	Reconciliation Field Mappings Tab of the Process Definition Form .....	6-13
6-6	General Tab of the Editing Task Dialog Box.....	6-18
6-7	Handler Selection Dialog Box .....	6-22
7-1	Form Information Form .....	7-2
7-2	Lookup Definition Form .....	7-5
7-3	User Defined Field Definition Form.....	7-8
7-4	User Defined Columns Tab of the User Defined Field Definition Form .....	7-9
7-5	User Defined Fields Dialog Box.....	7-10
7-6	User Defined Fields Dialog Box - Filled .....	7-12
7-7	Properties Tab of the User Defined Field Definition Form.....	7-13
7-8	Administrators Tab of the User Defined Field Definition Form.....	7-13
7-9	System Configuration Form .....	7-14
7-10	Remote Manager Form.....	7-17
7-11	Password Policies Form .....	7-18
7-12	Usage Tab of the Password Policies Form .....	7-25
7-13	Task Scheduler Form.....	7-26
8-1	Adapter Factory Form.....	8-2
8-2	Adapter Manager Form .....	8-2
8-3	Form Designer Form.....	8-3
8-4	Additional Columns Tab of the Form Designer Form .....	8-6
8-5	Child Table(s) Tab of the Form Designer Form.....	8-11
8-6	Object Permissions Tab of the Form Designer Form .....	8-12
8-7	Properties Tab of the Form Designer Form.....	8-13
8-8	Add Property Dialog Box .....	8-14
8-9	Add Property Dialog Box - Filled.....	8-15
8-10	Add Property Dialog Box .....	8-16
8-11	Edit Property Dialog Box.....	8-17
8-12	Administrators Tab of the Form Designer Form.....	8-18

8-13	Usage Tab of the Form Designer Form.....	8-19
8-14	Error Message Definition Form .....	8-22
9-1	Event Handler Manager Form .....	9-2
9-2	Data Object Manager Form .....	9-4



## List of Tables

4-1	Fields of the Organizational Defaults Form.....	4-2
4-2	Fields of the Policy History Form.....	4-3
4-3	Fields of the Reconciliation Manager Form .....	4-8
5-1	Fields of the IT Resources Type Definition Form.....	5-2
5-2	Fields of the IT Resources Form.....	5-4
5-3	Fields of the Rule Designer Form .....	5-7
5-4	Fields of the Edit Rule Element Dialog Box .....	5-10
5-5	Information in the Rule Designer Table .....	5-12
5-6	Fields of the Resource Objects Form .....	5-13
5-7	Rule Conditions and Possible Rule Actions.....	5-29
6-1	Fields of the Email Definition Form.....	6-3
6-2	Fields of the Process Definition Form .....	6-7
6-3	Fields of the General Tab of the Editing Task Dialog Box .....	6-18
6-4	Fields of the Assignment Tab of the Editing Task Window .....	6-31
7-1	Fields in the Form Information Form .....	7-2
7-2	Fields of the Lookup Definition Form .....	7-5
7-3	Fields of the User Defined Field Definition Form.....	7-8
7-4	Fields of the User Defined Fields Dialog Box .....	7-10
7-5	Fields of the System Configuration Form .....	7-15
7-6	Fields of the Policy Rules Tab of the Password Policies Form.....	7-20
7-7	Fields of the Policy Rules Tab for Setting Custom Password Policy.....	7-21
7-8	Fields of the Task Scheduler Form .....	7-26
7-9	Predefined Scheduled Tasks .....	7-29
8-1	Fields of the Form Designer Form.....	8-4
8-2	Fields of the Additional Columns Tab.....	8-6
8-3	Fields of the Add Property Dialog Box for a Data Field .....	8-15
8-4	Fields of the Add Property Dialog Box for a Customized Look up Query .....	8-16
8-5	Fields of the Error Message Definition Form.....	8-22
9-1	Fields of the Event Handler Manager Form .....	9-2
9-2	Fields of the Data Object Manager Form.....	9-4
9-3	Transformation Properties.....	9-9



---

---

# Preface

This guide describes the procedures that you can perform by using the Oracle Identity Manager Design Console.

## Audience

This guide is intended for users of the Oracle Identity Manager Design Console. This guide describes the basic functionality of the Design Console for both daily and administrative operations. For information about Oracle Identity Manager development tools, see *Oracle Identity Manager Tools Reference* and the Oracle Identity Manager SDK.

## Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. 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.

### Deaf/Hard of Hearing Access to Oracle Support Services

To reach Oracle Support Services, use a telecommunications relay service (TRS) to call Oracle Support at 1.800.223.1711. An Oracle Support Services engineer will handle technical issues and provide customer support according to the Oracle service request process. Information about TRS is available at

<http://www.fcc.gov/cgb/consumerfacts/trs.html>, and a list of phone numbers is available at <http://www.fcc.gov/cgb/dro/trsphonebk.html>.

## Related Documents

For more information, see the other documents in the Oracle Identity Manager documentation set for this release.

## Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager 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:

<i><b>Convention</b></i>	<b>Meaning</b>
<b>boldface</b>	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
<code>monospace</code>	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen (or text that you enter), and names of files, directories, attributes, and parameters.

## Online Help

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



---

# Oracle Identity Manager Architecture

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

- [Overview of Oracle Identity Manager Architecture](#)
- [Benefits and Key Features of Oracle Identity Manager](#)
- [Three Tiers of Oracle Identity Manager](#)

## 1.1 Overview of Oracle Identity Manager Architecture

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

## 1.2 Benefits and Key Features of Oracle Identity Manager

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 has 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 LDAP-enabled 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 online analytical processing (OLAP) capability of Oracle Identity Manager supports the most complex reports, analysis, and dynamic queries.

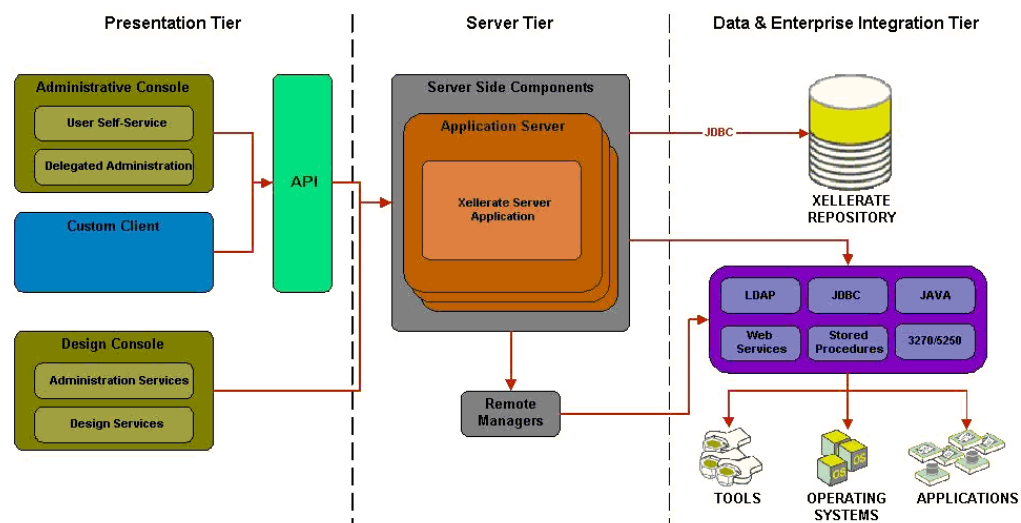
**Integration by using the Adapter Factory:** Attempting to support all systems with hand-coded adapters is impractical. Oracle developed an automated tool for adapter generation. This tool, the Adapter Factory, supports a wide range of interfaces and virtually any application or device. These adapters 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 by 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.

## 1.3 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**



### 1.3.1 Tier 1: Client

The first tier provides two interfaces, the Design Console (which is discussed in this guide) and the 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 describes the Oracle Identity Manager Design Console. For information about the Oracle Identity Manager Administrative and User Console, see *Oracle Identity Manager Administrative and User Console Guide*.

---

### 1.3.2 Tier 2: Application Server

The second tier implements the business logic in Java Data Objects. These objects are managed by the supported J2EE application server such as JBoss Application Server, Oracle WebLogic Server, IBM WebSphere Application Server, 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 other applications. To access the business functionality of Oracle Identity Manager, you can use the application programming interface (API) layer in the J2EE infrastructure, which provides the lookup and communication mechanism.

The J2EE-compliant application server that is supported by Oracle Identity Manager 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 information from the requests to the database. The server also delivers responses from the database to the client.
- **Scalability (connection pooling or sharing):** The application server supports single application or multiple 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 is displayed:  
  
"The security level for this data item indicates that it cannot be deleted or updated."

### 1.3.3 Tier 3: Database

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



---

## Design Console Main

This chapter describes how to start the Design Console and the Design Console main screen. It contains the following sections:

- [Starting the Design Console](#)
- [Overview of the Design Console](#)
- [Design Console Menu Bar](#)
- [Design Console Toolbar](#)
- [Design Console Shortcuts](#)
- [Design Console Explorer](#)
- [Design Console Workspace](#)

### 2.1 Starting the Design Console

To start the Design Console:

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

The Login window is displayed.

2. Enter your user ID and password.

Your password is displayed as asterisks (\*\*\*\*) for security purposes.

Your user ID and password cannot have special characters, for example, percent sign (%), plus sign (+), equals sign (=), comma (,), backslash (\), double quotation marks ("), less than symbol (<), greater than symbol (>), and slash (/).

3. Click **Login**.

The Design Console main screen is displayed.

After you log in to the Design Console, you can configure the system settings. These settings control the systemwide actions of Oracle Identity Manager. For information about these settings, see [Chapter 7, "System Configuration Form"](#).

---

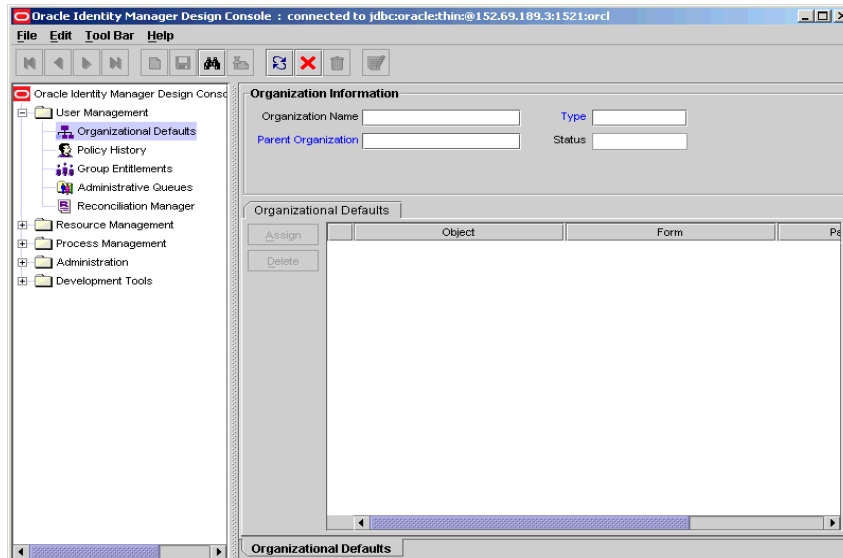
**Note:** You can also access the basic features of Oracle Identity Manager by using the Oracle Identity Manager Administrative and User Console. For information about the features of the Oracle Identity Manager Administrative and User Console, see *Oracle Identity Manager Administrative and User Console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

---

## 2.2 Overview of the Design Console

You can create, track, and analyze a business process by using the main screen in the Design Console, as shown in [Figure 2–1](#).

**Figure 2–1 Design Console Main Screen**



The Design Console main screen consists of four regions:

- [Design Console Menu Bar](#)
- [Design Console Toolbar](#)
- [Design Console Explorer](#)
- [Design Console Workspace](#)

## 2.3 Design Console Menu Bar

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

The Design Console menu bar provides the following menus:

- [File Menu](#)
- [Edit Menu](#)
- [Toolbar Menu](#)
- [Help Menu](#)

### 2.3.1 File Menu

The File menu provides the following options:

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

Menu Item	Action
Exit	Exits the Design Console

### 2.3.2 Edit Menu

The Edit menu provides the following options:

Menu Item	Action
Cut	Deletes selected text from editable fields and copies it to the system Clipboard
Copy	Copies the selected text to the system Clipboard
Paste	Pastes text from the system Clipboard to the selected field
Clear	Clears the selected text

### 2.3.3 Toolbar Menu

The **Toolbar** menu operations are described in the following table.

Menu Item	Action
New	Clears the contents of the active form
Save Changes	Saves all changes made to the active form
Query	Run a query on the active form
Notes	Displays any notes that are attached to the active form
Refresh	Refreshes the record of the active form
Close	Closes the active form
Delete	Deletes the current record
Next	Displays the next record when you query more than one record
Previous	Displays the previous record when you query more than one record
First	Displays the first record when you query more than one record
Last	Displays the last record when you query more than one record
Close All	Closes all open forms and clears the Design Console Workspace

### 2.3.4 Help Menu

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

Menu Item	Action
Administrator Guide	Displays the online Help equivalent of this guide.
About	Displays the copyright information about the Oracle Identity Manager Design Console.

## 2.4 Design Console Toolbar

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

Figure 2–2 shows the Design Console Toolbar.

**Figure 2–2 Design Console Toolbar**



When you hold the mouse over a toolbar button for a few seconds, a tool tip that describes the button is displayed.

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	Runs a query on the active form.
Notes	Displays any notes that are 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. <b>Note:</b> For information about prepopulate adapters, see <i>Oracle Identity Manager Tools Reference</i> .

## 2.5 Design Console Shortcuts

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

Shortcut Name	Keystroke Combination	Description
File menu	Alt+F	Activates the File menu
Edit menu	Alt+E	Activates the Edit menu
Toolbar menu	Alt+T	Activates the Toolbar menu
Help menu	Alt+H	Activates the Help menu

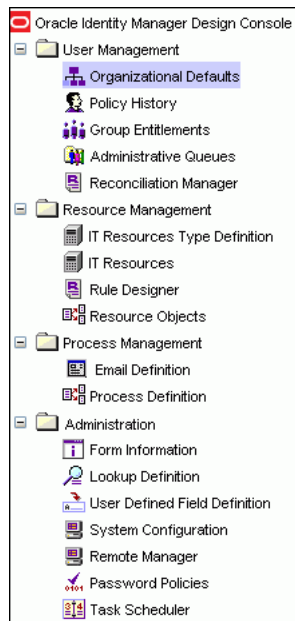


Shortcut Name	Keystroke Combination	Description
Print	Ctrl+P	Prints the active form
Cut	Ctrl+X	Deletes selected text from editable fields, and copies it to the system Clipboard
Copy	Ctrl+C	Copies the selected text to the system Clipboard
Paste	Ctrl+V	Pastes text from the system Clipboard to the selected field
Clear	Ctrl+Delete	Clears the selected text
New	Ctrl+N	Clears the active form
Save Changes	Ctrl+S	Saves all changes made to the active form
Query	Ctrl+Q	Runs a query on the active form
Notes	Ctrl+Shift+N	Displays notes that are attached to the active form
Refresh	Ctrl+R	Refreshes the active form
Close	Ctrl+W	Closes the active form
Delete	Ctrl+D	Deletes the current record
Next	Number pad + (plus)	Displays the next record, when you have queried more than one record
Previous	Number pad - (minus)	Displays 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	Displays the last record, when you have queried more than one record
Prepopulate	Ctrl+U	Populates designated fields of a customized form with data
Help	F1	Opens context-sensitive Help for the active form
Explorer	F3	Selects the Design Console icon, which is displayed at the top of the Design Console Explorer
Lookup	F4	Displays the Lookup window for the selected lookup field
Menu	F10	Activates the File menu

## 2.6 Design Console Explorer

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

[Figure 2–3](#) shows the Design Console Explorer. Your system administrator can customize the Explorer. Depending on the permissions assigned to you, you can see different icons in the Explorer. If you want to access a form icon that you do not have permissions for, contact your system administrator.

**Figure 2–3 Design Console Explorer**

**Tip:** If the system administrator changes your permissions, then you must refresh the Explorer window.

To start a form:

1. Expand the folder that contains the required form.
2. Double-click the form that you want to open.

The corresponding form is displayed in the Design Console Workspace.

**Tip:** You can adjust the size of the Design Console Explorer by moving the divider to the right or left.

To refresh the list of forms:

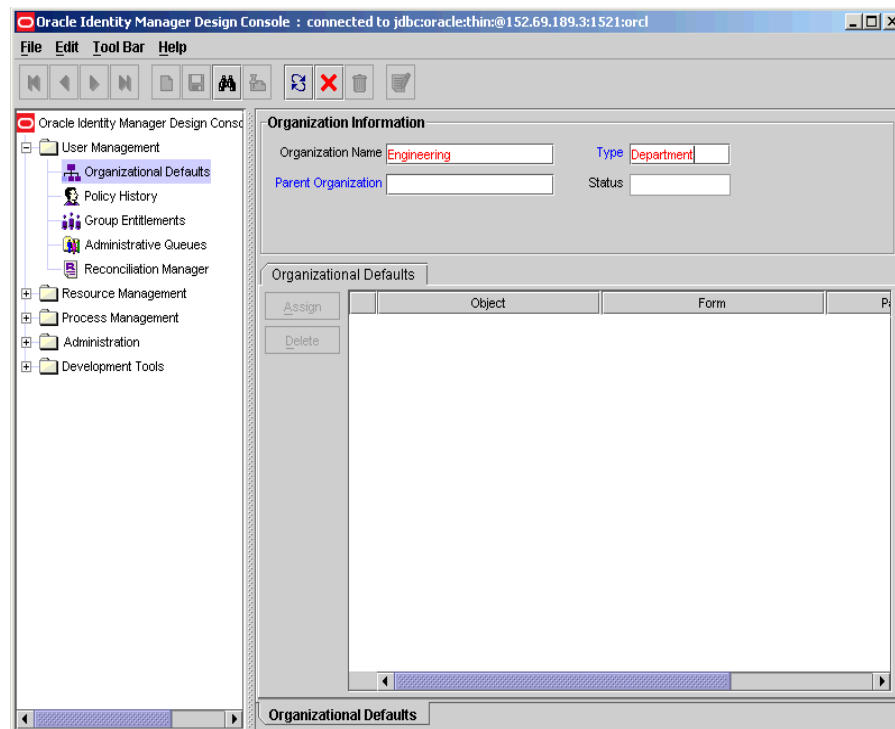
1. Right-click the Oracle Identity Manager logo at the top of the Oracle Identity Manager Explorer window. A menu is displayed.
2. Click **Refresh Explorer**.

The Design Console refreshes the Explorer with all forms that you can access, including any forms that a system administrator recently gave you permission to access.

## 2.7 Design Console Workspace

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

Figure 2–4 shows the Workspace.

**Figure 2–4 Design Console Workspace**

If you access multiple forms, the Design Console places the active form on top and layers the remaining forms on tabs along the bottom of the main screen. To switch between forms, click the desired form's tab.

The Design Console can display each form in two views: a form view and a table view.

### Form View

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

### Table View

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

For example, a query of the Organizations form can return several records. Both the form and table view tabs of the Organizations form can be displayed. [Figure 2–5](#) shows the table view of the Design Console.

**Figure 2–5 Table View**

	Organization Name	Parent Organization	Type	Status
1	Engineering		Department	Active
2	Human Resources		Department	Active
3	Marketing		Department	Active
4	Professional Service		Department	Active
5	Public Relations		Department	Active
6	Requests		System	Active
7	Research Developm		Department	Active
8	Sales		Department	Active
9	Shipping Recieving		Department	Active
10	Statewide - HR		Department	Active
11	Statewide - IT		Department	Active
12	Statewide - Investm		Company	Active
13	Statewide - Marketing		Department	Active
Organizational Defaults		Organizational Defaults Table		

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 headings, which are boxes with labels above each column.  
Column headings display the name of the column. If a column contains a Lookup dialog box, the column heading is displayed in blue.
- The Design Console forms contain row headings, which are boxes with numeric labels 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 is displayed 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 is displayed 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 are displayed in blue have Lookup dialog boxes.  
You can double-click these fields to access their Lookup dialog boxes, 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 the data in that field has changed and must be saved.
- To select consecutive record rows, press the Shift key.
- To select unconsecutive record rows, use the Ctrl key.
- To export a record, right-click the row heading.  
To select more than one record, press the Shift key before clicking the row heading.  
A dialog box is displayed.

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

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

- To save the records as a tab-delimited file, select **Copy to File**.
- You can control the order in which the records in a table view are displayed by using the sort feature.

To change the sort order of displayed records, click the heading of the column by which you want the records to be sorted. A triangle is displayed beside the column heading text. This indicates the direction, ascending or descending order, in which the records were sorted.



---

## Basic Functions in the Design Console

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

This chapter contains the following sections:

- [Special Field and Form Types](#)
- [Assignment Windows](#)
- [Performing a Search](#)

### 3.1 Special Field and Form Types

The actions of the basic features of the Design Console are standard for all forms. This section describes the standard actions of the Design Console and the field and window types in the Design Console main screen.

#### 3.1.1 Data Fields

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

The label of a field can 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 a standard field.
- A blue label indicates that the data in this field is derived from a predefined list of values supplied by using a Lookup or a Date & Time window.

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

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

- If the field value is displayed in black, then the data in this field is supplied by the user.  
You can query or edit the information in these types of fields.
- If the field value is displayed in red, then the data in this field is supplied by Oracle Identity Manager.

These values are read-only. This prevents you from overwriting critical information.

### 3.1.2 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:

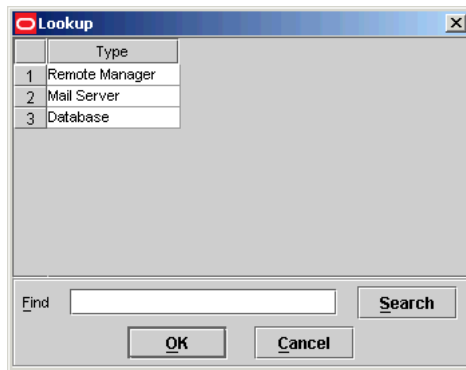
1. If the Lookup dialog box contains a short list of fields, click a field, then click **OK**.

Alternatively, you can select the field and press F4.

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

Figure 3–1 shows the Lookup dialog box.

**Figure 3–1 Lookup Dialog Box**



2. If the Lookup dialog box contains a long list of values, enter the first few characters of the value in the Find box, followed by an asterisk (\*), and then click **Search**.

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

### 3.1.3 Date and Time Fields

The Date & Time window enables you to select a month, year, day, and time. This window is displayed when you double-click a field that is equipped with a an option to open this window.

To select a date and time:

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

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

The Date & Time window is displayed.

2. From the menu, select the month.
3. From the **Date** scroll box, select the year.
4. Click the date on the calendar.
5. From the **Time** box, select the time.
6. Click **OK** to save your changes.

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

Click **Cancel** to exit without saving.



### 3.1.4 List

Lists have predefined values. When you click a list, its values are displayed. If the list contains more values that can be displayed at one time, a vertical scroll bar is displayed to the right of the list.

When you select a value, the list is replaced by a field in which the selected value is displayed.

### 3.1.5 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 the Design Console generated while compiling the adapter. For more information about adapters, see *Oracle Identity Manager Tools Reference*.

---

**Note:** In the following procedure, if the Notes button is red, then the current record 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. Select the required record.
2. Click **Notes**.

The Notes window is displayed.

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

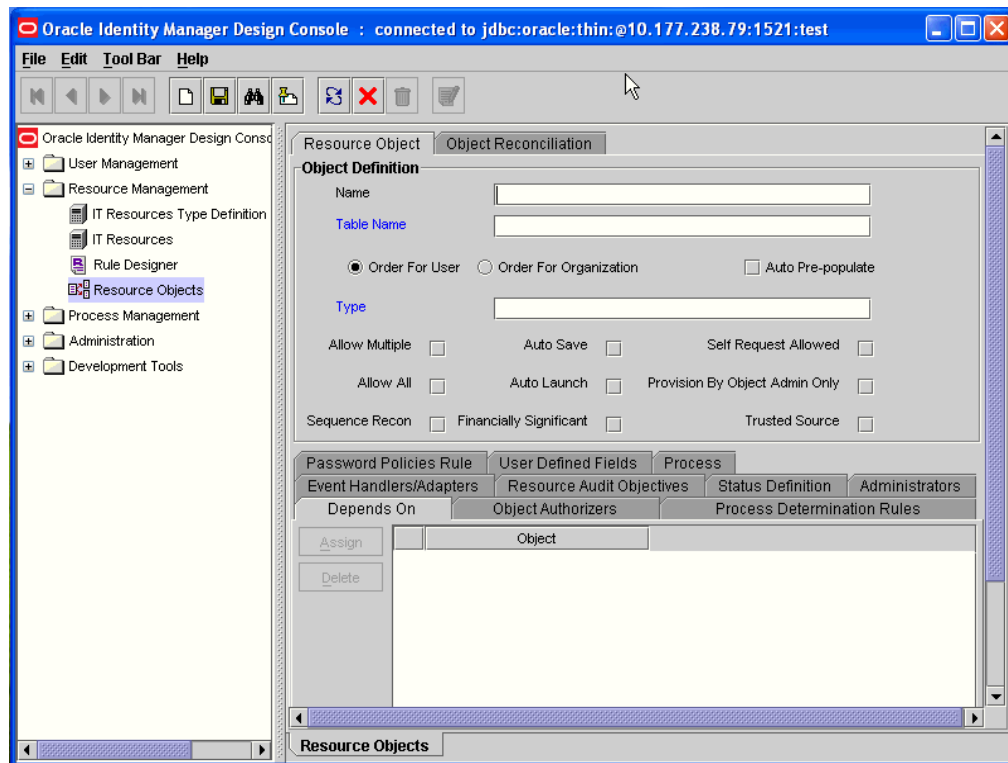
Or, click **Close** to close the Notes window without saving.

5. From the Toolbar, click **Save**.

The information you entered into the Notes window is saved.

### 3.1.6 Tabs on Forms

Most forms in the Design Console contain multiple tabs. The tabs are usually in the bottom 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 3–2](#).

**Figure 3–2 Design Console - Tab on Forms**

Each tab has its own tables and function buttons. Usually, the buttons on a tab are grayed out 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 heading.

## 3.2 Assignment Windows

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

The left pane lists items that you can assign to the record, for example, Organization. The right pane lists the items that have already been assigned to the record. Although the values available for selection in the left and right panes 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 nonconsecutive 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 the item and click the right arrow.

- To unassign one or more items, select them, and click the left arrow.

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

### 3.3 Performing a Search

The Design Console enables you to perform searches (queries) for records in the database. Every form in the 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.

### 3.4 Constructing a Search Filter

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

You can use a wildcard character in a search. The asterisk (\*) wildcard character represents unspecified portions of the search criteria. You can use a wildcard character 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 a 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 asterisk is placed in the middle of a search value, as in B\*on, you retrieve all records that begin with B and end with ON (for example, Brighton, Boston, and so on). If you place the asterisk 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 3-3](#), 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 3-3** *Displaying the Results of a Search Query*

The screenshot displays the 'Organization Information' form in the Design Console. The 'Organization Name' field contains the text 'Statew\*' in red, indicating a search filter. The 'Type' field is empty. The 'Parent Organization' and 'Status' fields are also empty. Below the form, the 'Organizational Defaults' section is visible, showing a table with columns 'Object' and 'Form'. The table is currently empty, and a scrollbar is visible at the bottom.

## 3.5 Results of a Search

After you enter the search criteria in the query fields, click the binoculars symbol or press Ctrl+Q.

One of the following occurs:

- **No records are returned.** No records in the database match your search criteria for this form. Either the record that you are searching for no longer exists in the database, or you must 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 is displayed, listing all records that meet your search criteria. The first record is displayed in the Form view, as shown in [Figure 3–4](#).





**Figure 3–4 Multiple Records Returned**

	Organization Name	Parent Organization	Type	Status
1	Statewide - HR		Department	Active
2	Statewide - IT		Department	Active
3	Statewide - Investm		Company	Active
4	Statewide - Marketir		Department	Active

Organizational Defaults    Organizational Defaults Table

## 3.6 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. The following table describes the VCR buttons:

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 is displayed 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.

## 3.7 Optimizing Query Performance

A query that returns a large result set can require significant time to run and can affect your computer's performance. To optimize performance, use 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.

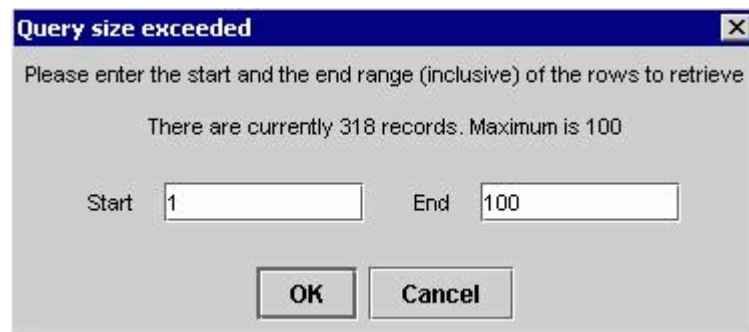
- Use the asterisk (\*) wildcard character where possible.

If you place the asterisk in front of an alphabetic character (for example, \*A), fewer records are returned as compared to when you leave a field blank.

## 3.8 Exceeding the Limit for a Result Set

If you have both read and write access to all forms and records in the Design Console in the System Configuration form (that is, if you are a system administrator), you can set the maximum number of records that are displayed in the result set for a search. If the number of records retrieved for a search exceeds this value, the Design Console displays the Query size exceeded dialog box, as shown in [Figure 3-5](#).

**Figure 3-5** Query Size Exceeded Dialog Box



You are prompted to enter a specific range or subset of the result set to be viewed. In [Figure 3-5](#), the maximum result set of 100 has been exceeded. Only records 1 through 100 will be displayed.

**See Also:** For more information about the System Configuration form, see "[System Configuration Form](#)" on page 7-14.



---

# User Management

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

- [Overview of User Management](#)
- [Organizational Defaults Form](#)
- [Policy History Form](#)
- [Assigning Group Entitlements](#)
- [Administrative Queues Form](#)
- [Reconciliation Manager Form](#)

## 4.1 Overview of User Management

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 can 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.

## 4.2 Organizational Defaults Form

The Organizational Defaults form is 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, for example, a company, department, or branch.

A suborganization is an organization that is a member of another organization, for example, a department in a company. The organization that the suborganization 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 option on the associated Resource Objects form selected.

The values that you provide on the Organizational Defaults tab become the default values for all users in the organization. Oracle recommends that you do not specify default values for passwords and encrypted parameters.

Figure 4–1 shows the Organizational Defaults form.

**Figure 4–1 Organizational Defaults Form**

Table 4–1 describes the fields of the Organizational Default form.

**Table 4–1 Fields of the Organizational Defaults 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 to which this organization belongs. If a parent organization is displayed in this field, this organization is displayed on the Sub Organizations tab for the parent organization. If this field is empty, this organization is a top-level organization.

## 4.3 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 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 user can access only the Administrative and User Console and generally has 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 by using the Administrative and User Console.

Figure 4–2 shows this form.

**Figure 4–2 Policy History Form**

Table 4–2 describes the fields of the Policy History form.

**Table 4–2 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 Address	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 the 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.

### 4.3.1 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 to which the user belongs
- Resource objects that are allowed by the organization to which the user belongs

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 to which the user is a member.

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 are displayed 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 are displayed in the Resources Not Allowed list.

To view the tracking system:

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

From the User Policy Profile History 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 a 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.

## 4.4 Assigning Group Entitlements

The Group Entitlements form is displayed 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 designate forms and folders to user groups by using the Group Entitlements form:

1. In the Explorer, double-click **Group Entitlements**.  
The User Group Information page is displayed.
2. In the **Group Name** field, enter the name of the user group.
3. Click **Assign**.

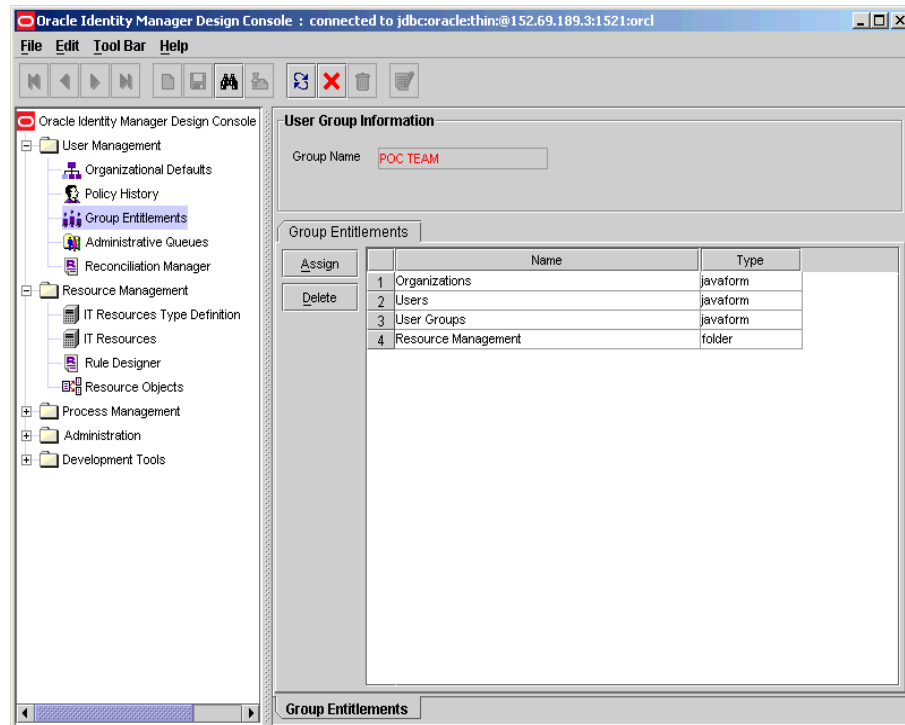
The User Form Assignment lookup table is displayed.

4. From the lookup table, select the user form for this user group.

Use the arrow buttons to either add or delete from the **Assigned Forms** list.

5. Click **OK**.

The User Group Information dialog box is displayed, as shown:



The newly added user forms are listed in a Group Entitlements table. The Group Entitlements Table displays all available user groups. This table shows the name of the user form and the type. In the Group Entitlements table, 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.

## 4.4.1 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.

### 4.4.1.1 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.

#### 4.4.1.2 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.

#### 4.4.1.3 All Users User Group

Members of the All Users user group have minimal permissions. These permissions include but are not limited to access to the user's own record. Each user automatically belongs to the All Users user group.

A user cannot be removed from the All Users group.

#### 4.4.1.4 Self Operators Group

The Self Operators user 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.

---

---

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

---

---

## 4.5 Administrative Queues Form

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

Administrative queues increase the efficiency and manageability of requests. 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 have different administrative privileges for the request. The first user group is allowed to read, modify, and delete the request. The second user group is allowed to read and modify the request. The third user group is allowed to read and delete the request.

---

---

**Note:** The Administrative Queues form in the Design Console is deprecated. Although the form can still be viewed in the Design Console, you must use the Oracle Identity Manager APIs to access administrative queue features.

See *Oracle Identity Manager API Usage Guide* for more information.

---

---

## 4.6 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 done automatically by Oracle Identity Manager based on action rules you define. These rules are based on whether or not 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 4–3 shows the Reconciliation Form.

**Figure 4–3 Reconciliation Manager Form**

**Note:** You can use the Design Console Task Scheduler form to define a schedule and set timing parameters to control 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.  
You can also review information that was automatically linked to the user or organization.
- If the event represents the 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.

You can also 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 the 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.

You can also use the form to review the information that was automatically linked to a organization.

- If the event represents the deletion of an account on a target system or trusted source, this form can be used to instruct Oracle Identity Manager to delete a particular account or to review an account that was automatically deleted.

For trusted sources, the deletion of an account on a target system or trusted source deletes the user's Oracle Identity Manager account and revokes all accounts with which that user have been provisioned on any target resource.

For target resources, Oracle Identity Manager is notified of revoked user accounts.

The upper portion of the Reconciliation Manager form contains the following fields, as shown in [Table 4-3](#).

**Table 4-3 Fields of the Reconciliation Manager Form**

Field Name	Description
Event ID	The numeric ID of the reconciliation event.
Delete Event (Yes or No flag)	<p>Indicates if the corresponding record was deleted from the target resource or the trusted source. Yes indicates a delete event.</p> <p>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.</p> <p><b>Note:</b> This field is set by Oracle Identity Manager.</p>
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	Indicates that the event for a resource object is associated with a user record or organization record.

**Table 4–3 (Cont.) Fields of the Reconciliation Manager Form**

Field Name	Description
Status	<p>The current status of the reconciliation event:</p> <ul style="list-style-type: none"> <li>■ <b>Event Received:</b> Indicates that changes were received from the target resource or trusted source, for example, the <code>CreateReconciliationEvent</code> method was called. The event has not received data from the target resource or trusted source.</li> <li>■ <b>Data Received:</b> The data that the information from the target resource or trusted source was received.</li> <li>■ <b>Users Matched:</b> The event matches one or more user records, based on reconciliation user-matching rules.  If you configure trusted source reconciliation of users, then you must ensure that the User ID field of the OIM User is used in the reconciliation matching rule.</li> <li>■ <b>Organizations Matched:</b> The event matches one or more organization records, based on reconciliation organization-matching rules.  If you configure trusted source reconciliation of organizations, then you must ensure that the Organization Name field of the OIM User is used in the reconciliation matching rule.</li> <li>■ <b>Processes Matched:</b> 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.</li> <li>■ <b>No Match Found:</b> 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 was not associated with a user or organization record.</li> <li>■ <b>Rules Reapplied:</b> The <b>Reapply Matching Rules</b> button was clicked (previous matches might be removed) and the logic of the latest edition of all matching rules that is associated with this resource was applied.</li> <li>■ <b>Event Linked:</b> The event was matched and linked to a particular user or organization record.</li> <li>■ <b>Event Closed:</b> A user manually closed the event by clicking the <b>Close Event</b> button, without its data being linked to a record in Oracle Identity Manager. Once closed, a reconciliation event cannot be reopened.</li> <li>■ <b>Required Data Missing:</b> At least one required data element is missing. If the data for any required field on the resource definition is not available in the event, then this message is displayed.</li> </ul>
Event Date	The date and time that this event was received.
Assigned to User	The user to whom this event is assigned.
Assigned to Group	The user group to which this event is assigned.
Linked To (region)	The fields in this section are User Login, Organization Name, Process Instance Key, and Process Descriptive Data.
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 to which the event is linked. If you are conducting organization discovery with a trusted source, then Oracle recommends that you do this before performing user discovery, because 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.

**Table 4–3 (Cont.) Fields of the Reconciliation Manager Form**

Field Name	Description
Process Descriptive Data	Instance-specific descriptive data for the provisioning process that is defined in the Map Descriptive Field window in the Process Definition form.
Close Event	Closes the reconciliation event. If the event is closed, no additional matching attempts or linking can be performed on it.
Re-apply Matching Rules	Reapplies the reconciliation matching rules. This includes both process data and user-matching or organization-matching rules that are associated with the resource object. If Oracle Identity Manager is not generating satisfactory matches, you can change and reapply the resource's reconciliation matching rules, or you can change the mappings for the provisioning process. Reapplying these rules after changing them can cause different records to be displayed 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 because the process matches should be more accurate.
Create Organization (Only available on events related to the trusted source)	Creates an organization record in Oracle Identity Manager based on the information in the reconciliation event. Click this button only 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)	Creates a user record in Oracle Identity Manager based on the information in the reconciliation event. Click this button only when you are certain that the reconciliation event represents the creation of a new user on the trusted source.

## 4.6.1 Viewing and Managing Reconciliation Events

To view and manage reconciliation events:

---

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

---

1. Go to the Reconciliation Manager form.
2. Use the query feature to locate a 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, **Delete Event** is set to **Yes**. Otherwise, it is set to **No**.

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

The information about each tab is described in the tabs on the Reconciliation Manager form section. When evaluating the matches that Oracle Identity Manager generates, you can do the following:



- **Link the reconciliation event to a particular provisioning process, user, or organization:** It is assumed that the event is associated with an existing user or organization record.

To do this, click **Link** on the applicable tab. You might 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 **Create User**. Or, you can 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 **Create Organization**. Or, you can 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. Re-apply the rule to generate more accurate matches.

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

---

**Note:** If you refine a reconciliation rule and reapply it or create or link a user or provisioning process or organization, then these actions are logged in the **Reconciliation Event History** tab. To view a log of the actions that were performed on the reconciliation event, click the **Reconciliation Event History** tab.

---

## 4.6.2 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

### 4.6.2.1 Reconciliation Data Tab

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

#### 4.6.2.1.1 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 were successfully processed, for example, they did not violate 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 might be one of several values that changed on the target resource or trusted source that initiated the reconciliation event.

The following is an example of a processed data field:

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

---

**Note:** If a field is of type multivalue (only allowed for target resources, not trusted sources), it will not have a value. Instead, its component fields (contained in its subbranch) will each have their own values.

---

#### 4.6.2.1.2 Unprocessed Data

The fields listed in the Unprocessed Data branch are reconciliation events 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 is displayed:

- Name of the field, for example, **user\_securityid**.
- Value of the field that was received in the reconciliation event, for example, capital. This might be one of several values that changed on the target resource or trusted source that 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 codes is displayed next to the unprocessed field:

Error code	Reason generated
NOT MULTI-VALUED ATTRIBUTE	The field value is a multivalued attribute. Only the component fields of a multivalue attribute, not the multivalue field itself, can accept values.
NOT NUMERIC	A numeric field value was nonnumeric.
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 was not defined on the resource.
PARENT DATA LINK MISSING	The parent data field (of type multivalue) 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 multivalue. One or more of the multivalue field's component (child) fields' data is not linked to reconciliation fields.
TABLE ATTRIBUTE LINKAGE MISSING	This applies only to fields of type multivalue. Some of the component (child) fields of type MultiValued Attribute are not linked to a reconciliation field of type MultiValued 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.

The following is an example of an unprocessed data field:

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

---

**Note:** Oracle Identity Manager does not match processes for target resources, or users or organizations for trusted sources, until all fields that are set on the Reconciliation Fields tab of the associated resource are successfully processed.

---

#### 4.6.2.1.3 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 multivalue field, you must map it to the appropriate child process form or select the individual component field.

For multivalue fields, double-click and correct the component fields.

The Edit Reconciliation Field Data dialog box is displayed.

---

**Note:** To map an unprocessed multivalued component field to one of the multivalue fields defined on the Reconciliation Fields tab of the associated resource, double-click the **Linked to** field, select the desired field, and click **OK**. 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 change 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 records 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 process instances match these values, Oracle Identity Manager evaluates the applicable user-matching 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. 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 record is found, an administrator must examine the records and decide to which Oracle Identity Manager account to link it. If no matches are found, then there might be a mismatch between the data in your trusted source and the target application. This event can be 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 with which user that account is associated.

#### 4.6.2.2 Processes Matched Tree (for target resources only)

After all required fields defined on the Reconciliation Fields tab of the associated resource are 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. Because 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 evaluates the user-matching 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 is similar to the following:

```
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, then Oracle Identity Manager applies any user-matching or organization-matching rules that are defined for the resource. If matches are found, then they are displayed on the **Matched Users** or **Matched Organizations** tab.

#### 4.6.2.2.1 Linking a Provisioning Process Instance to the Reconciliation Event

To link a provisioning process instance to the reconciliation event:

1. After you determine which provisioning process instance to link to the reconciliation event, select the process instance 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. This also inserts the **Reconciliation Update Received** task in that process.

#### 4.6.2.3 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 are generated on the **Processes Matched Tree** tab.

For each matching record, the 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 are displayed on the **Matched Users** tab. The process matches are more likely to be accurate.

---

#### 4.6.2.3.1 Linking a User Record to the Reconciliation Event

To link a user record to a reconciliation event:

---

**Note:** A record must exist for you to perform the following procedure. For trusted sources, if you determine that the reconciliation event represents the creation of a new user on the trusted source, click **Create User**. This creates a new user record by using the information in the reconciliation event.

---

1. Determine the user to link to the reconciliation event, select the user, 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, 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** in the instance of the user provisioning process for the user record to which the reconciliation event is linked.

#### 4.6.2.4 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 when 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 are 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 are displayed on the Matched Organizations tab because the process matches are and more likely to be accurate.

---

---

##### 4.6.2.4.1 Linking an Organization Record to the Reconciliation Event

To link an organization record to a reconciliation event:

---

---

**Note:** The following procedure assumes a record already exists. For trusted sources, if you determine that the reconciliation event is the creation of a new organization on the trusted source, click **Create Organization**. This creates a new organization record by using the information in the reconciliation event.

---

---

1. After you determine what organization to link to the reconciliation event, select the event 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, 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 to which the reconciliation event is linked.

#### 4.6.2.5 Reconciliation Event History

The Reconciliation Event History 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 shown. Oracle Identity Manager tracks and logs the following reconciliation events:

- **Event Received:** This action is logged when Oracle Identity Manager receives a reconciliation event.
- **Data Sorted:** This action is logged when the data in a reconciliation event is sorted into processed and unprocessed fields.
- **Rules Reapplied:** This action is logged when a user clicks the **Re-apply Matching Rules** button.
- **Processes Matched:** This action is logged when one or more process form instances and their associated provisioning process were matched to values of key fields in the reconciliation event.
- **Users Matched:** This action is logged when one or more user records are matched with data in the reconciliation event by using user-matching reconciliation rules.
- **Organization Matched:** This action is logged when one or more Oracle Identity Manager organization records are matched with data in the reconciliation event by using organization-matching reconciliation rules.
- **Linked to User:** This action is logged when the data in the reconciliation event is linked to a particular user.
- **Linked to Organization:** This action is logged when the data in the reconciliation event is linked to a particular organization.





---

## Resource Management

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

- [Overview of Resource Management](#)
- [IT Resources Type Definition Form](#)
- [IT Resources Form](#)
- [Rule Designer Form](#)
- [Resource Objects Form](#)
- [Service Account Management](#)

### 5.1 Overview of Resource Management

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

- **IT Resources Type Definition:** Use this form to create resource types that are displayed 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, automatic 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:** See *Oracle Identity Manager Tools Reference* for more information about adapters and adapter tasks

### 5.2 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, Microsoft Exchange, and 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 is available for selection when you define a resource. The type is displayed in the **Type** field on the IT Resources form.

IT resource types are 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 is 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.

Figure 5–1 shows the IT Resources Type Definition form.

Figure 5–1 The IT Resources Type Definition Form

Table 5–1 describes the fields of the IT Resources Type Definition form.

Table 5–1 Fields of the IT Resources Type Definition Form

Field Name	Description
Server Type	The name of the IT resource type
Insert Multiple	Specifies whether or not this IT resource type can be referenced by more than one IT resource

**Note:** If an IT resource must access an external resource but is not able to do so by using the network, then you must associate it with a remote manager. For more information, see *Oracle Identity Manager Tools Reference*.

5.2.1 Defining a Template (a Resource Type) for IT Resources

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, select **Insert Multiple**.
- 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.

## 5.2.2 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

### 5.2.2.1 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 5-1](#). Oracle recommends that you do not specify default values for passwords and encrypted fields. 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 an applicable resource definition, the new parameter is displayed 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

To add a parameter to an IT Resource Type:

1. Click **Add**.

A new row is displayed 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** option.

This check box determines if this parameter's value is masked, that is, represented with asterisk (\*) in a form field.

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

5. Click **Save**.

### Removing a Parameter from an IT Resource Type

To remove a parameter from an IT Resource Type:

1. Select 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.

#### 5.2.2.2 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.

### 5.2.3 IT Resource Type Definition Table

The IT Resource Type Definition Table displays the following information:

Field Name	Description
Server Type	The name of the resource asset type, as defined in the IT Resource Type Definition form
Insert Multiple	Indicates whether or not multiple instances of this IT Resource Definition can be created

## 5.3 IT Resources Form

The IT Resources form is 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 are located. 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 parameter for an IT resource. The parameters represent information about the hardware, for example, a server domain name or the ID of the user who accesses this IT resource.

**See Also:** *Oracle Identity Manager Tools Reference* for more information about adapters and their mappings

[Table 5–2](#) describes the fields of the IT Resources form.

**Table 5–2 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 by using a remote manager, then this field displays the name of the remote manager. Otherwise, this field is empty.

### 5.3.1 Defining 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 by using the IT Resource Type definition form.

3. Click **OK**.
4. To access the IT resource by using a remote manager, double-click the **Remote Manager** lookup field, and in the Lookup dialog box select a remote manager.

If the IT resource is not accessed by using a remote manager, then go to Step 6.

5. Click **OK**.
6. Click **Save**.

The saved IT resource is displayed 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 are displayed 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 change, enter the new value, and click **Save**.

### 5.3.2 Setting Access Permissions to an IT Resource Instance Parameter

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

To set access permissions:

1. Click the **Administrators** tab.

By default, the administrative 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. Select the appropriate check box for the permissions listed in the following table:

Permission	Description
Read	When selected, the administrative group indicated by the group name can read the current IT Resource Instance.
Write	When selected, the corresponding group name can read and modify the current IT Resource Instance parameter values.
Delete	When selected, the associated administrative group can delete the current IT Resource Instance.

4. Click **Save**.

## 5.4 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.

**See Also:** *Oracle Identity Manager Tools Reference* for more information about prepopulate adapters

The Rule Designer form shown in [Figure 5–2](#) is in the Resource Management folder. You use this form to create and manage rules that are used with resources.

**Figure 5–2 Rule Designer Form**

The screenshot shows the 'Rule Definition' form in the 'Rule Designer' tool. The 'Name' field is 'Rule for Solaris'. The 'Operator' is set to 'AND'. Under 'Type Information', the 'Type' is 'Process Determination', 'Sub-Type' is 'User Provisioning', 'Object' is 'Solaris 8', and 'Process' is 'Solaris 8'. The 'Description' is 'This rule will check to see if Solaris can be provisioned to an Xellerate user.' The 'Rule Elements' tab is active, showing a tree structure: 'Rule for Solaris' (parent) containing 'User Login == XELSYSADM' (child) and 'Rule to Prevent Solaris Access' (child). The 'Rule to Prevent Solaris Access' rule contains the element 'Object Name == Solaris'. Buttons for 'Add Element', 'Add Rule', and 'Delete' are visible on the left.

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 which 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 5–2](#), 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 5–2](#), 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 5–2](#), 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.

Table 5–3 describes the fields of the Rule Designer form.

**Table 5–3 Fields of the Rule Designer Form**

Field Name	Description
Name	The rule's name.
AND/OR	<p>These options specify the operation for the rule.</p> <p>To stipulate that a rule is successful only when all the outer rule elements and nested rules are true, select <b>AND</b>. To indicate that a rule is successful if any of its outer rule elements or nested rules are TRUE, select <b>OR</b>.</p> <p><b>Important:</b> These options do not reflect the operations for rule elements that are contained within nested rules. In Figure 5–2, the <b>AND</b> operation applies to the User Login == XELSYSADM rule element and the Rule to Prevent Solaris Access nested rule. However, this operation has no effect on the Object Name != Solaris rule element within the Rule to Prevent Solaris Access rule.</p>
Type	<p>The rule's classification status. A rule can belong to one of four types:</p> <ul style="list-style-type: none"> <li>■ <b>General:</b> 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.</li> <li>■ <b>Process Determination:</b> Determines the standard approval process that is associated with a request, and the approval and provisioning processes that are selected for a resource object.</li> <li>■ <b>Task Assignment:</b> Determines which user or user group is assigned to a process task.</li> <li>■ <b>Prepopulate:</b> Determines which prepopulate adapter is used for a form field.</li> </ul>
Sub-Type	<p>A rule of type Process Determination, Task Assignment, or Prepopulate can be categorized into one of four subtypes:</p> <ul style="list-style-type: none"> <li>■ <b>Organization Provisioning:</b> Classifies the rule as a provisioning rule. Determines the organization for which a process is provisioned, a task is assigned, or the prepopulate adapter is applied.</li> <li>■ <b>User Provisioning:</b> Classifies the rule as a provisioning rule. Determines the user for which a process is provisioned, a task is assigned, or a prepopulate adapter is applied.</li> <li>■ <b>Approval:</b> Classifies the rule as an approval rule. Approves the provisioning of resources to users or organizations.</li> <li>■ <b>Standard Approval:</b> Classifies the rule as a standard approval rule. Approves a request.</li> </ul> <p>For Task Assignment or Prepopulate rule types, the approval and standard approval items are not displayed in the Sub-Type box. The Sub-Type box is grayed out for the General rule type.</p>
Object	The resource object to which this rule is assigned.
All Objects	If selected, the rule can be assigned to all resource objects.
Process	The process to which this rule is assigned.
All Processes	If selected, the rule can be assigned to all processes.
Description	Explanatory information about the rule.

## 5.4.1 Creating a Rule

To create a rule:

---

---

**Note:** In the following procedure, note that the options do not apply to rule elements within nested rules. For example, in [Figure 5–2](#) 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 effect on the `Object Name != Solaris` rule element in the Rule to Prevent Solaris Access 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** option.

To indicate that a rule is successful if any of its rule elements or nested rules are true, select the **OR** option.

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, go 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 available to all resource objects, select the **All Objects** option.

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.

---

---

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

---

---

If you want the rule to be available to all processes, select the **All Processes** option.

---

---

**Note:** If you select a resource object in Step 5 by selecting the **All Processes** option, then this rule is available to every process that is associated with the selected resource object.

---

---

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



## 5.4.2 Tabs on the Rule Designer Form

The Rule Designer form contains the following tabs:

- Rule Elements tab
- Usage tab

Each of these tabs is discussed in the following sections.

### 5.4.2.1 Rule Elements Tab

From this tab, you can create and manage elements and nested rules for a rule. For example, in [Figure 5-3](#), the Rule for Solaris contains the User Login==XELSYSADM rule element. It also has a nested Rule to Prevent Solaris Access. [Figure 5-3](#) displays the Rule Elements tab of the Rule Designer form.

**Figure 5-3 Rule Elements Tab of the Rule Designer Form**

The rule in [Figure 5-3](#) 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 cannot access Solaris.

When a rule element or nested rule is no longer valid, 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

To add a rule element to a rule:

1. Click **Add Element**.

The Edit Rule Element dialog box is displayed.

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.

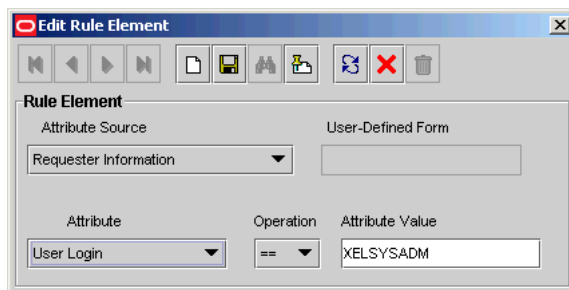
Table 5–4 describes the data fields in the Edit Rule Element dialog box.

**Table 5–4 Fields of 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 is displayed in the adjacent box. <b>Note:</b> If Object Data or Process Data are not displayed in the <b>Attribute Source</b> box, the <b>User-Defined Form</b> 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 field, enter the value for the attribute. <b>Note:</b> The attribute's value is case-sensitive.

- Set the parameters for the rule you are creating, as shown in Figure 5–4.

**Figure 5–4 Edit Rule Element Window**



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 about the parameters, see "[Rule Elements Tab](#)" on page 5-9.

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

The rule element is displayed in the **Rule Elements** tab of the Rule Designer form.

- From the main screen's toolbar, click **Save**.

The rule element is added to the rule.

### Adding a Nested Rule to a Rule

To nest a rule within a rule:

---

**Note:** In the following procedure, only rules of the same type and subtype as the parent rule are displayed in the Select Rule window.

---

1. Click **Add Rule**.

The Select Rule dialog box is displayed.

2. Select a nested rule and click **Save**.

3. Click **Close**.

The nested rule is displayed 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

To remove a rule element or a nested rule:

1. Select 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.

#### 5.4.2.2 Usage Tab

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

Figure 5–5 shows the Usage tab.

**Figure 5–5 Usage Tab of the Rule Designer Form**

**Rule Definition**

Name: Rule to Approve Solaris

Operator: ☐ AND ☒ OR

**Type Information**

Type: Process Determination

Sub-Type: Approval

Object: is Resource Object ☐ All Objects

Process: to Approve Solaris ☐ All Processes

Description: This rule will determine whether the target user can approve the provisioning of the Solaris resource object.

**Rule Elements Usage**

	Object	Process	Type	Priority
1	The Solaris Resource Object	Process to Approve Solaris	A	1

Rule Designer

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 prepopulate adapter associated with a rule.
- A one-letter code, signifying the rule's classification type: A=Approval and P=Provisioning.

This code is displayed for process determination rules only.

- The rule's priority number.

In [Figure 5-5](#), the Rule to Approve Solaris definition was assigned to the **Solaris Resource Object** and the **Process to Approve Solaris**. Because 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, after the corresponding resource object was assigned to the request.

### 5.4.3 Rule Designer Table

The Rule Designer Table, as shown in [Figure 5-6](#), displays all available rules defined in the Rule Designer form.

**Figure 5-6 Rule Designer Table**

	Rule Name	Rule Type	Rule Sub-Type	Task	Condition	Priority
1	UserSelfRegistration	Process Determination	General Approval	AND		001:004:3:00:004
2	UserSelfRegistration	Process Determination	General Approval	AND		001:004:3:00:004
3	SelfRegistration	Pre-Process	User Provisioning	AND	This rule is used	001:004:3:00:004
4	UserSelfRegistration	Process Determination	User Provisioning	AND	This rule is a single	001:004:3:00:004
5	Confirmation Rule	Process Determination	Standard Approval	AND	Confirmation Rule	001:004:3:00:004
6	UserSelfRegistration	Pre-Process	User Provisioning	AND	Request is approved	001:004:3:00:004
7	SelfRegistration	Task Assignment	User Provisioning	AND	This is a task	001:004:3:00:004

[Table 5-5](#) shows the information displayed in the Rule Designer Table.

**Table 5-5 Information in the Rule Designer Table**

Field Name	Description
Rule Name	The name of the rule.
Rule Type	<p>A rule can belong to one of four types:</p> <ul style="list-style-type: none"> <li>■ <b>General:</b> 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.</li> <li>■ <b>Process Determination:</b> Determines the standard approval process that is associated with a request, and the approval and provisioning processes that are selected for a resource object.</li> <li>■ <b>Task Assignment:</b> Determines which user, user group, or both are assigned to a process task.</li> <li>■ <b>Pre-Populate:</b> Determines which prepopulate adapter is executed for a given form field.</li> </ul>

**Table 5–5 (Cont.) Information in the Rule Designer Table**

Field Name	Description
Rule Sub-Type	<p>A rule of type Process Determination, Task Assignment, or Pre-Populate can be categorized into one of four sub-types:</p> <ul style="list-style-type: none"> <li> <b>Organization Provisioning:</b> Classifies the rule as a provisioning rule.  You use this subtype to determine the organization for which a process is provisioned, a task is assigned, or the prepopulate adapter is applied. </li> <li> <b>User Provisioning:</b> Classifies the rule as a provisioning rule.  You use this subtype to determine the user for which a process is provisioned, a task is assigned, or a pre-populate adapter is applied. </li> <li> <b>Approval:</b> Classifies the rule as an approval rule.  You use this subtype to approve the provisioning of resources to users or organizations. </li> <li> <b>Standard Approval:</b> Classifies the rule as a standard approval rule.  You use this subtype to approve a request. </li> </ul>
Rule Operator	The relationship between the attribute and the attribute value represented by the == or != operators.
Description	Explanatory information about the rule.
Last Updated	The date when the rule was last updated.

## 5.5 Resource Objects Form

The Resource Objects form is 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 are templates for provisioning the resource. However, the approval and provisioning of the resource depends on the design of the approval and provisioning processes that you link to the resource object.

---

**See Also:** ["Administrative Queues Form"](#) on page 4-6 for more information about requests and their relationship with resource objects

---

[Table 5–6](#) describes the data fields of the Resource Objects form.

**Table 5–6 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.)

**Table 5–6 (Cont.) Fields of the Resource Objects Form**

Field Name	Description
Order For User/Order For Organization	Options that determine whether or not the resource object can be requested for users or organizations.  To request the resource object for a user, select <b>Order For User</b> . To request the resource object for an organization, select <b>Order For Organization</b> .
Auto Pre-Populate	Option that determines whether or not a custom form will be populated by Oracle Identity Manager or a user. This applies to the following kinds of forms: <ul style="list-style-type: none"> <li>Forms that are associated with the resource object</li> <li>Forms with fields that have prepopulate adapters attached to them</li> </ul> <p>If the <b>Auto Pre-Populate</b> check box is selected, after the associated custom form is displayed, the fields with pre-populate adapters are populated with data.</p> <p>If this check box is deselected, a user must populate the fields by clicking the <b>Pre-Populate</b> button on the toolbar.</p> <p><b>Note:</b> This setting does not control the triggering of the pre-populate adapter. It determines if the contents resulting from the execution of the adapter are displayed in the associated field because of Oracle Identity Manager or a user.</p> <p>For more information about prepopulate adapters, see <i>Oracle Identity Manager Tools Reference</i>.</p> <p><b>Note:</b> This check box is only relevant if you have created a form that is to be associated with the resource object.</p>
Type	The resource object's classification status. A resource object can belong to one of three types: <ul style="list-style-type: none"> <li><b>Application:</b> Classifies this resource object as an application.</li> <li><b>Generic:</b> Contains business-related processes.</li> <li><b>System:</b> Oracle Identity Manager uses this type of resource object internally.</li> </ul> <p>Do not modify system resource objects without first consulting Oracle.</p>
Allow Multiple	Designates if the resource is provisioned more than once to a user or organization. If it is selected, the resource object can be provisioned more than once for each user or organization.
Auto Save	By selecting this check box, Oracle Identity Manager saves the data in any resource-specific form that was created by using the Form Designer form without first displaying the form.  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. The user will not have access to the form if you do not populate the form with the required data.  <b>Note:</b> This check box is only relevant if you have created a form for the provisioning of the resource object.
Self Request Allowed	By selecting this check box, users as well as the system administrator can request the resource object for themselves.  <b>Note:</b> This functionality only applies to the Oracle Identity Manager Design Console. It is not applicable to the Oracle Identity Manager Administrative and User Console.

**Table 5–6 (Cont.) Fields of the Resource Objects Form**

Field Name	Description
Allow All	By selecting this check box, the resource object can be requested for all Oracle users. This setting takes precedence over whether or not the organization to which a user belongs has allowed the resource that can be requested for its users.
Auto Launch	<p>By default, this check box is checked at the time of object creation. Oracle Identity Manager automatically initiates the provisioning process when the resource's approval process is in Completed status.</p> <p>Oracle Identity Manager automatically makes all resource objects set to Auto Launch, even though this check box is cleared.</p>
Provision by Object Admin Only	<p>This check box determines who can provision this resource, either by using direct provisioning or by manually initiating the provisioning process when the <b>Auto Launch</b> check box is deselected.</p> <p>If this check box is selected, only users who are members of the groups listed on the <b>Object Administrators</b> tab will be able to provision this resource object (either directly or by manually initiating the provisioning process from the request).</p> <p>If this check box is deselected, no restrictions are placed on who can directly provision this resource.</p>

**Table 5–6 (Cont.) Fields of the Resource Objects Form**

Field Name	Description
Sequence Recon	<p>If you select this check box, then reconciliation events are processed in the sequence in which they are created.</p> <p>The application of this feature can be illustrated by the following example:</p> <p>Suppose there are two reconciliation events for the OIM User resource object for user John Doe. The first reconciliation event (E1) data is as follows:</p> <ul style="list-style-type: none"> <li>■ Login: testuser1</li> <li>■ First Name: John</li> <li>■ Last Name: Doe</li> <li>■ Organization: Xellerate Users</li> <li>■ Type: End-User</li> <li>■ Role: Full-Time</li> </ul> <p>The second reconciliation event (E2) data is as follows:</p> <ul style="list-style-type: none"> <li>■ Login: testuser1</li> <li>■ First Name: John1</li> <li>■ Last Name: Doe1</li> <li>■ Organization: Xellerate Users</li> <li>■ Type: End-User</li> <li>■ Role: Full-Time</li> </ul> <p>Between the first and second events, the first name and last name of the user was changed.</p> <p>During trusted source reconciliation, if events are processed in the order in which they are created, then this change in first and last names is correctly reconciled into Oracle Identity Manager. However, if the second event is processed before the first one, then data in the target system does not match data in Oracle Identity Manager at the end of the reconciliation run. This inconsistency will be reflected in the auditing tables, and will remain until another event from the trusted source is created for this user.</p> <p>If you enable the Sequence Recon option, then you can ensure that events for the same entity (for example, same user or same process form) are processed in the order in which they were created.</p>
Trusted Source	<p>You can select this check box if you want to use the resource object for trusted user reconciliation.</p> <p>By default, this check box is not selected. It is selected by default only for the Xellerate User resource object.</p>

### 5.5.1 Creating 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. If required, you can attach a resource form to the resource object. To do this, 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 **Order For User**.



To request the resource object for an organization, select **Order For Organization**.

---

**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 prepopulate adapters attached to them, and you want these fields to be populated automatically by Oracle Identity Manager, select the **Auto Pre-Populate** option.

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** option.

---

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

---

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** option. Otherwise, go to Step 8.
8. When you want Oracle Identity Manager to save the data in any resource-specific form (created by using the Form Designer form) without first displaying the form, select the **Auto Save** option.

Otherwise, proceed to Step 9.

---

**Note:** 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 because the user will be unable to access the form.

Select this check box only if you have created a form for provisioning the resource object.

---

9. If you want to be able to request the resource object for yourself, select the **Self Request Allowed** option. Otherwise, go 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, go to Step 11.
11. If you want to use the resource object for trusted source user reconciliation, you must select the **Trusted Source** option. Otherwise, go to Step 12.

---

**Note:** You must deselect the Self Request Allowed and Allow All check boxes to ensure that the resource object is not available for provisioning requests and resource profiles.

---

12. 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** option. Otherwise, go to Step 13.

---

**Caution:** By default, Oracle Identity Manager sets all resource objects to Auto Launch, even though this check box is not selected.

---

13. To restrict the user groups that can provision this resource object to groups that are displayed in the **Object Authorizers** tab of the Resource Objects form, select the **Provision by Object Admin Only** option. This applies to resource objects that are provisioned directly or by assignment to a request. Otherwise, go to Step 14.

14. Click **Save**.

The resource object is created.

## 5.5.2 Tabs on the Resource Objects Form

When you start 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/Adapters Tab](#)
- [Resource Audit Objectives](#)
- [Status Definition Tab](#)
- [Administrators Tab](#)
- [Password Policies Rule Tab](#)
- [User-Defined Fields Tab](#)
- [Process Tab](#)
- [Object Reconciliation Tab](#)

### 5.5.2.1 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 is displayed on 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](#)
- [Removing the dependent resource object](#)

### Selecting a Dependent Resource Object

To select a dependent resource object:

1. Click **Assign**.

The Assignment dialog box is displayed.

2. Select the resource object, and assign it to the request.
3. Click **OK**.

The dependent resource object is selected.

### Removing a Dependent Resource Object

To remove a dependent resource object:

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

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

### 5.5.2.2 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 which 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 authorized to complete this process task is the user with the highest priority who belongs to the SYSTEM ADMINISTRATORS user group because 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 user group.

**See Also:** ["Rule Designer Form"](#) on page 5-5 and ["Assignment Tab of the Editing Task Window"](#) on page 6-30 for more information about task assignment rules and process tasks

### Assigning a User Group to a Resource Object

To assign a user group to a resource object:

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

The user group is selected.

### Removing a User Group from a Resource Object

To remove a user group from a resource object:

1. Select the desired user group.

2. Click **Delete**.

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

### Changing the Priority Number of a User Group

To change a user group's priority number:

1. Select the user group whose priority number you want to change.
2. To increase the selected user group's priority number by one, click **Increase**.

To decrease 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 increase 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.

#### 5.5.2.3 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 is a template for the resource that 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:

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

Each approval process and provisioning process 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, then Oracle Identity Manager evaluates the rule with the next highest priority. If a rule is true, then Oracle Identity Manager executes the process associated with 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, then 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, then Oracle Identity Manager evaluates the **Rule to Check Provisioning of Solaris for Developers** rule. If this rule is true, Oracle Identity Manager executes the **Provision Solaris for Devel** provisioning process associated with that rule.

### Adding 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 or 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, select a rule, and assign it to the resource object (only rules of *Process Determination* type are available for selection).
4. Click **OK**.
5. In the adjacent column, double-click the **Processes** lookup field.
6. From the Lookup dialog box, select a 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:

1. Select a rule and process combination.
2. Click **Delete**.  
The rule and process combination is removed from the resource object.

#### 5.5.2.4 Event Handlers/Adapters Tab

A resource object's provisioning process contains 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 Java code, which enables Oracle Identity Manager to communicate and interact with external resources.

When an event handler or adapter that is assigned to a resource object that is no longer valid, you must remove it from the resource object.

For this example, the **adpAUTOMATEPROVISIONINGPROCESS** adapter was 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

To assign an event handler to an adapter or a resource object:

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

### Remove an Event Handler or Adapter from a Resource Object

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

1. Select an event handler.
2. Click **Delete**.

The event handler is removed from the resource object.

#### 5.5.2.5 Resource Audit Objectives

The Resource Objects form in the Design Console is enhanced and now includes a new resource attribute named **Resource Audit Objectives**. This resource attribute helps you link resources to regulatory mandates.

A new lookup is defined for the values of the Resource Audit Objectives resource attribute. The predefined values in the Resource Audit Objectives list are:

- SOX (Hosts Financially Significant Information)
- HIPAA (Hosts Private Healthcare Information)
- GLB (Hosts Non-Public Information)
- Requires Quarterly Review
- Requires Annual Review

You can extend this list by editing the Lookups.Resource Audit Objective.Type lookup by using the Lookup Definition Form in the Design Console.

A new Resource Audit Objectives tab is now on the Resource Profile form in the Design console, which lets you select the value of this attribute.

#### 5.5.2.6 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 **Completed** status, 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 has the following predefined 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 deprovisioned 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 were 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 start 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 verifies that there are other resource objects upon which the **Exchange** resource object depends. If there are, Oracle Identity Manager starts the approval and provisioning processes of the dependent objects. Then, Oracle Identity Manager selects an approval and provisioning process for the **Exchange**.

You might 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 might want to set the corresponding provisioning status of the resource object to **Revoked**.

Similarly, when an existing provisioning status is no longer valid, you must 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

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, go 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:

1. Select a provisioning status.
2. Click **Delete**.

The provisioning status is removed from the resource object.

#### 5.5.2.7 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 deselected.

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

To assign a user group to a resource object:

1. Click **Assign**.

The Assignment dialog box is displayed.

2. Select the user group, and assign it to the resource object.
3. Click **OK**.

The user group is displayed 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, select the corresponding **Write** check box.

Otherwise, go to Step 5.

5. If you want this user group to be able to delete the current resource object, select the associated **Delete** check box.

Otherwise, go to Step 6.

6. Click **Save**.

The user group is assigned to the resource object.

### Removing 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.



### 5.5.2.8 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 might 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 by using the Password Policies form.

Because 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 might 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. This enables 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. This is done 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 (because 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 by 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.

The following sections discuss how to add and remove a password policy rule from a resource object.

### Adding 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 is displayed, double-click the **Rule** lookup field.
3. From the Lookup dialog box, 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, 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.

---

**Note:**

- If the resource type is Order for Organisation, then you cannot attach a password policy to the resource object. The exception to this rule is the Xellerate User resource object. Although this resource object is of Order for Organisation type, password policies can be attached to it.
  - If two or more rules evaluate to True, then the password policy attached to the rule with the highest priority is applied.
  - A Default rule is predefined in Oracle Identity Manager. This rule always evaluates to True. If no rules have been created through the Rule Designer, then a password policy can be attached to the Default rule.
- 

**Removing a Password Policy Rule from a Resource Object**

To remove a password policy from a resource object:

1. Select a password policy rule.
2. Click **Delete**.

The password policy rule is removed from the resource object.

**5.5.2.9 User-Defined Fields Tab**

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

**See Also:** See "[User Defined Field Definition Form](#)" on page 7-7 for instructions about how to create user-defined fields on existing Oracle Identity Manager forms

**5.5.2.10 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 by using the Process Definition form. Each process can then be linked to a process determination rule by 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.

**5.5.2.11 Object Reconciliation Tab**

The Object Initial Reconciliation Date field on the Object Reconciliation Tab displays the date when initial reconciliation was performed for the resource.

---

**Note:** The purpose of initial reconciliation is to bring all the user accounts from the target system into Oracle Identity Manager.

---

The date value stored in the Object Initial Reconciliation Date field is used to distinguish between initial reconciliation and subsequent reconciliations events. This date value is used by the two exception reports introduced in release 9.1.0. These exception reports display differences in the entitlements a user must have as compared to what the user actually has in the target system. The differences in entitlements are determined by using reconciliation data, along with other data items. The exception reports return data associated with only those reconciliation events that are created after the date stored in the Object Initial Reconciliation Date field. In addition, exception data is generated only if the Initial Object Reconciliation Date field displays a date value that is in the past. If required, you can enter a date value in this field so that the exception reports are generated.

The Object Reconciliation tab contains two subtabs, Reconciliation Fields and Reconciliation Action Rules.

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

- Name of the field on the target resource or 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 that designates whether or not this field is required in a reconciliation event

---

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

---

The following is an example of a target system field definition:

TargetField1 [String], Required

In the Reconciliation Fields tab, you can perform the following:

- Add a reconciliation field
- The following procedure adds 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 by 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 is displayed.

2. Enter the name of the field on the target resource or trusted source in the **Field Name** field.

This is the name that will reference the target resource or trusted source field in Oracle Identity Manager.

3. Select one of the following values from the menu in the **Field Type** field:

- Multi-Valued

This is meant for use with fields that contain one or more component fields.

- String

- String

- Date

- IT resource

During reconciliation event creation, the value this field receives must be the same as the name of an IT resource defined in Oracle Identity Manager.

4. Select the **Required** check box.

If selected, the reconciliation field must be processed on the **Reconciliation Data** tab of the Reconciliation Manager form before Oracle Identity Manager will begin matching a provisioning process, user, or organization to the reconciliation event. If this check box is not selected, 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.

■ Delete 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 reconciles data on the target system (this will have no effect on the data in the target system itself).

By using this tab, you can specify the actions that Oracle Identity Manager will perform when some matches within reconciliation event records are encountered. Each record in this tab is a combination of:

- The conditions and actions from which you can select are predefined. Depending on the matching conditions, certain actions might not be applicable. A complete list of the available options is provided in [Table 5-7](#).

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

**Table 5–7 (Cont.) Rule Conditions and Possible Rule Actions**

Rule Condition	Possible Rule Actions
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 6-30 for a description of the classification types for the users and groups listed in the preceding table

### Adding a Reconciliation Action Rule

To add a reconciliation action rule:

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

### Deleting a Reconciliation Action Rule

To delete a reconciliation action rule:

1. Select the matching action combination to delete.
2. Click **Delete**.

The reconciliation action rule will be removed and the action associated with its condition will not be executed automatically.

## 5.5.3 Multiple Trusted Source Reconciliation

In earlier releases, you could set up only the Xellerate User resource object as a trusted source to reconcile identities. Now, you can do this by creating the reconciliation fields, reconciliation action rules, field mappings, and matching roles for the Xellerate User resource object and the process definition.

If there are two trusted sources from which you want to reconcile identities to create OIM Users, then you are not able to configure a single resource object (Xellerate User) for both the trusted sources. Even if you create reconciliation fields for both the trusted sources in the Xellerate User resource object, you cannot create the corresponding reconciliation field mappings in the Xellerate User process definition.

From release 9.1.0 onward, you can configure resource objects other than Xellerate User as trusted sources for identity reconciliation. You can do this by selecting the **Trusted Source** check box in the Resource Objects form while creating a resource object.

For a resource object to which the Trusted Source flag is attached, you can create multiple reconciliation fields to denote the target system fields. You can also configure the reconciliation action rule in which if there are no process matches found, then either a user is created or the data is sent to the administrator or authorizer for identity creation. If a process match is found, then the link is established.

When defining provisioning process for trusted source resources, do not attach user-defined forms. For these provisioning processes, reconciliation field mappings can be created between reconciliation fields defined on the resource and OIM User attributes.

---

---

**Note:** If the resource object is for target resource reconciliation, then the mapping is between the reconciliation fields and process data fields.

Do not use any resource objects that are defined as a trusted source for provisioning activities. These resources are meant to be used only for OIM Users' reconciliation.

---

---

Another addition in this release is the attribute authoritative sources feature. This means sources are trusted for only attributes of the identities and not the identities themselves. You can configure attribute authoritative source reconciliation by creating appropriate reconciliation action rules. If no process match is found, then it is assigned to the administrator. This ensures that a user is not created by mistake even if there are no matches found. If a process match is found, then the reconciliation action rule will establish a link.

The following sections discuss two use cases in which you can implement multiple trusted source reconciliation.

---

---

**Note:** At some places in this document:

- Multiple trusted source reconciliation has been referred to as MTS.
  - The terms fields and attributes have been used interchangeably.
- 
- 

### 5.5.3.1 Multiple Trusted Source Reconciliation Using MTS-Compatible Connectors

---

---

**Note:** To determine whether or not your connector is MTS-compatible, see connector-specific documentation.

---

---

The following sections discuss scenarios in which you can implement multiple trusted source reconciliation by using MTS-compatible connectors:

- [Configuring MTS-Compatible Connectors for Trusted Source Reconciliation by User Type](#)
- [Configuring MTS-Compatible Connectors for Trusted Source Reconciliation of Specific OIM User Attributes](#)

#### Configuring MTS-Compatible Connectors for Trusted Source Reconciliation by User Type

In this context, user type refers to the type of users whose records you want to reconcile. Examples of user types are `Employee` and `Customer`.

To implement trusted source reconciliation by user type, perform the procedure to implement trusted source reconciliation while deploying the connectors of each target system that you want to configure as a trusted source.

During reconciliation, all the target system records of the specified user types are reconciled. If the target systems contain multiple user types, then you can use the Limited Reconciliation feature to specify the user type for which records must be reconciled from each target system.

### **Configuring MTS-Compatible Connectors for Trusted Source Reconciliation of Specific OIM User Attributes**

You might want to configure trusted source reconciliation for specific OIM User attributes from multiple target systems. The procedure to implement this is described with the help of the following sample scenario:

You want to reconcile identities from one target system, for example TS1, and specific attributes of these identities (for example `attr1`, `attr2`, and `attr3`) from another target system, for example TS2. This means that TS1 is the trusted source for the identities, and TS2 is the trusted source for specific attributes of those identities and not the identities themselves. TS1 must provide all the mandatory OIM User attributes for the successful creation of an OIM User. TS2 will provide only those OIM User attributes (either a mandatory OIM User attribute or a non-mandatory one) for which TS2 is the trusted source. If you reconcile a mandatory OIM User attribute from TS2, then the value of this attribute overwrites the value contained in this attribute after the OIM User is created from TS1. If you want to reconcile only non-mandatory OIM User attributes from TS2, then you can choose not to reconcile these attributes from TS1 during OIM User creation.

For the TS1 connector:

1. Perform all the steps required to deploy the TS1 connector and configure it for trusted source reconciliation.

**See Also:** The documentation for the connector you are deploying for information about the procedure to configure trusted source reconciliation

2. In the Reconciliation Fields tab on the Object Reconciliation page, delete all the TS1 attributes that you want to reconcile from TS2 (in this case `attr1`, `attr2`, and `attr3`).
3. In the Reconciliation Field Mappings tab on the Process Definition page, delete all the mappings other than the ones you want to retain.

Instead of deleting reconciliation fields, you can remove the reconciliation field mappings of those fields for which you do not want to reconcile the values into the OIM User created through reconciliation.

4. In the Reconciliation Action Rules tab on the Object Reconciliation page, ensure that the following rule condition and action mappings exist:

Rule Condition: No Matches Found

Action: Create User

For the TS2 connector:

1. Perform all the steps required to deploy the TS2 connector and configure it for trusted source reconciliation.



**See Also:** The documentation for the connector you are deploying for information about the procedure to configure trusted source reconciliation

2. In the Reconciliation Fields tab on the Object Reconciliation page, delete all the TS2 attributes other than `attr1`, `attr2`, and `attr3`. In addition, retain the attributes that you want to use to match OIM Users with existing TS2 accounts. This means that you retain only those attributes that will be used for reconciliation rule evaluation. For example, you might want to use the `username` attribute in Oracle Identity Manager to match the value of the `first name` attribute in TS1.
3. In the Reconciliation Field Mappings tab on the Process Definition page, delete all the mappings other than the ones you want to retain.

Instead of deleting reconciliation fields, you can also choose to just remove the reconciliation field mappings of those fields for which you do not want to reconcile the values into the OIM User created through reconciliation.

4. In the Reconciliation Action Rules tab on the Object Reconciliation page, create rule conditions and action mappings. One of these rule condition-action mappings must be the following:

Rule Condition: `No Matches Found`

Action: `Anything other than Create User`

### 5.5.3.2 Multiple Trusted Source Reconciliation Using Connectors That Are Not MTS-Compatible

---

**Note:** To determine whether or not your connector is MTS-compatible, see connector-specific documentation.

---

For a connector that is not MTS-compatible, the following prerequisites must be addressed before you can use the connector in a multiple trusted source reconciliation setup:

- i. Only one of the trusted source resource objects can be `Xellerate User`. In your operating environment, if the `Xellerate User` resource object is already in use by a connector for trusted source reconciliation, then for the trusted source connector that you want to configure, you must create a new resource object and process definition.
- ii. The scheduled task of the connector must have an attribute that accepts the name of the resource object used for trusted source user reconciliation as its value.

The following sections discuss scenarios in which you can implement multiple trusted source reconciliation by using non-MTS-compatible connectors:

- [Configuring Non-MTS-Compatible Connectors for Trusted Source Reconciliation by User Type](#)
- [Configuring Non-MTS-Connectors for Trusted Source Reconciliation of Specific OIM User Attributes](#)

### Configuring Non-MTS-Compatible Connectors for Trusted Source Reconciliation by User Type

In this context, user type refers to the type of users whose records you want to reconcile. Examples of user types are Contractor, Employee, and Customer.

You use Microsoft Active Directory and Oracle e-Business Suite as trusted sources in your operating environment. Active Directory is used to store information about identities that belong to the Contractor user type. Oracle e-Business Suite is used to store information about identities that belong to the Customer and Employee user type. You want to reconcile Contractor records from Active Directory and Employee records from Oracle e-Business Suite. To do this, perform the following:

For Active Directory:

1. Perform all the steps required to deploy the Active Directory connector and configure it for trusted source reconciliation.

**See Also:** The documentation for the connector you are deploying for information about the procedure to configure trusted source reconciliation

When you import the connector XML file for trusted source reconciliation, information specific to Active Directory is added in the `Xellerate User` resource object and process definition.

2. On the Resource Object tab, create the `ActDir` resource object for trusted source reconciliation with Active Directory.

---

**Note:** You can assign any name to the resource object. This procedure is based on the use of `ActDir` as the name assigned to the resource object.

For detailed information about the procedure to create a resource object, see "[Resource Objects Form](#)" on page 5-13.

---

While creating the resource object:

- a. Select the **Trusted Source** check box on the Resource Object tab.
  - b. On the Object Reconciliation>>Reconciliation Fields tab, see `Xellerate User` resource object and add the Active Directory-specific fields that you want to reconcile in `ActDir`. All the mandatory OIM User fields must be covered by the fields that you add on this tab.
3. On the Object Reconciliation>>Reconciliation Action Rules tab, create rule conditions and action mappings. One of these rule condition-action mappings must be the following:

Rule Condition: No Matches Found

Action: Create User

4. Delete the fields specific to Active Directory and the corresponding rules from the `Xellerate User` resource object.
5. Create the `ActDir` process definition in the Process Definition form.

For detailed information about the procedure to create a process definition, see "[Process Definition Form](#)" on page 6-6. Based on the reconciliation field mappings in the `Xellerate User` process definition, on the Reconciliation Field Mappings tab, add the reconciliation field mappings for the `ActDir` process definition.

6. Delete the Active Directory-specific field mappings in the `Xellerate User` resource object.

7. In the Reconciliation Rule Builder form on the Reconciliation Rules page, query and open the reconciliation rule for this connector and change the value of the Object field to map to the resource object that you have created. By default, the value of this field is mapped to that of the `Xellerate User` resource object.

For Oracle e-Business Suite, repeat all the steps you performed for Active Directory. Perform the following steps of that procedure differently for the Oracle e-Business Employee Reconciliation connector:

1. On the Resource Object tab, create the `EmpRecon` resource object for trusted source reconciliation with Oracle e-Business Suite.

---

**Note:** You can assign a name to the resource object. This procedure is based on the use of `EmpRecon` as the name assigned to the resource object.

---

2. On the Object Reconciliation>>Reconciliation Action Rules tab, create rule conditions and action mappings. One of these rule condition-action mappings must be the following:

Rule Condition: No Matches Found

Action: Create User

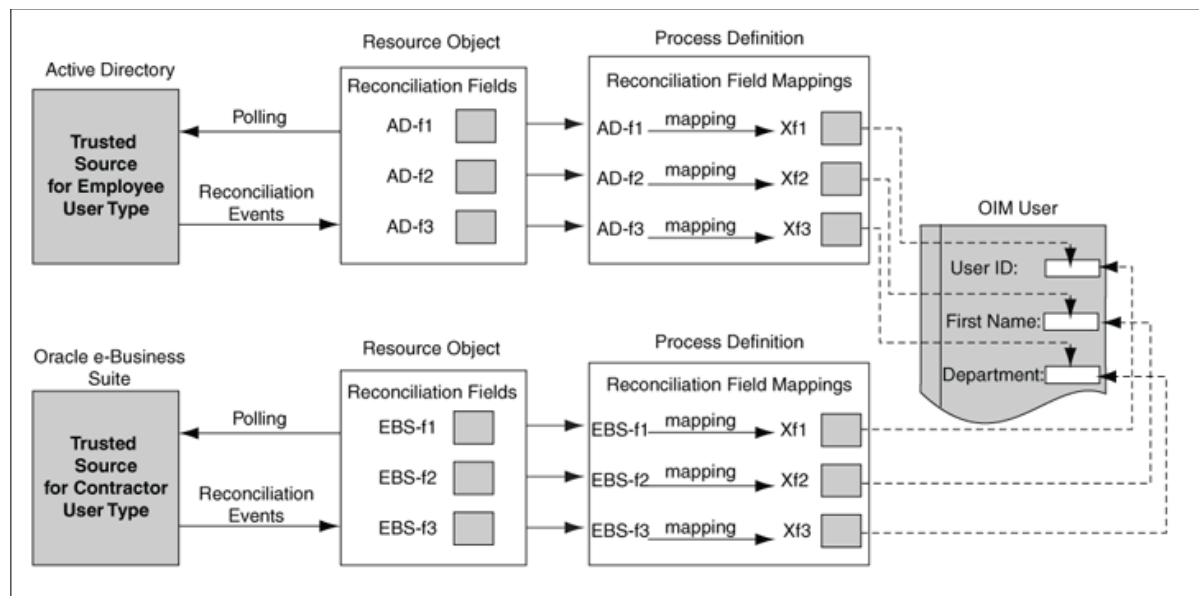
Use the Limited Reconciliation feature to specify that only identities that belongs to the Employee user type must be reconciled.

3. After you add the fields and the reconciliation rules, delete the Oracle e-Business Suite-specific fields and the corresponding rules created in the `Xellerate User` resource object.
4. Create the `EmpRecon` process definition in the Process Definition form. For detailed information about the procedure to create a process definition, see "[Process Definition Form](#)" on page 6-6. Based on the `Xellerate User` reconciliation field mappings, on the Reconciliation Field Mappings tab, add the field mappings for the `EmpRecon` process definition.
5. Delete the Oracle e-Business Suite-specific field mappings in the `Xellerate User` resource object.
6. On the Reconciliation Rules>>Reconciliation Rule Builder form, query and open the reconciliation rule for this connector and change the value of the Object field to map to the resource object that you have created. By default, the value of this field is mapped to that of the `Xellerate User` resource object.

For both Active Directory and Oracle e-Business Suite, perform the rest of the steps required to configure trusted source reconciliation. For example, while configuring the reconciliation scheduled task for each connector, specify the name of the trusted source resource object that must be used during trusted source user reconciliation.

The current value of the scheduled task attribute would be `Xellerate User` and it must be updated with the name of the new resource object configured for trusted source user reconciliation for this connector.

[Figure 5-7](#) shows the design time implementation of trusted source reconciliation based on the user type.

**Figure 5–7 Trusted Source Reconciliation by User Type**

### Configuring Non-MTS-Connectors for Trusted Source Reconciliation of Specific OIM User Attributes

You might want to configure trusted source reconciliation for specific OIM User attributes from multiple target systems. The procedure to implement this is described with the help of the following sample scenario:

You use Microsoft Active Directory and IBM Lotus Notes as your target systems. You want to reconcile identities from Active Directory and only the value of the e-mail address attribute of each identity (reconciled into Oracle Identity Manager from Active Directory) from Lotus Notes. To achieve this:

For the Active Directory connector:

1. Perform all the steps required to deploy the Active Directory connector and configure it for trusted source reconciliation.

**See Also:** The documentation for the connector you are deploying for information about the procedure to configure trusted source reconciliation

When you import the connector XML file for trusted source reconciliation, Active Directory-specific information is added in the Xellerate User resource object and process definition.

2. On the Resource Object tab, create the ActDir resource object for trusted source reconciliation with Active Directory.

---

#### Note:

You can assign any name to the resource object. This procedure is based on the use of ActDir as the name assigned to the resource object.

For detailed information about the procedure to create a resource object, see "[Resource Objects Form](#)" on page 5-13.

---

While creating the resource object:

- i. Select the **Trusted Source** check box on the Resource Object tab.
- ii. On the Object Reconciliation>>Reconciliation Fields tab, see `Xellerate User` resource object and add the Active Directory-specific fields that you want to reconcile in `ActDir`. All the mandatory OIM User fields must be covered by the fields that you add on this tab.
3. On the Object Reconciliation>>Reconciliation Action Rules tab, create rule conditions and action mappings. One of these rule condition-action mapping must be the following:
 

Rule Condition: No Matches Found

Action: Create User
4. Delete the Active Directory-specific fields and the corresponding rules from the `Xellerate User` resource object.
5. Create the `ActDir` process definition in the Process Definition form. For detailed information about the procedure to create a process definition, see "[Process Definition Form](#)" on page 6-6. Based on the reconciliation field mappings in the `Xellerate User` process definition, on the Reconciliation Field Mappings tab, create the field mappings for the `ActDir` process definition.
6. Delete the Active Directory-specific field mappings in the `Xellerate User` resource object.
7. On the Reconciliation Rules>>Reconciliation Rule Builder form, query and open the reconciliation rule for this connector and change the value of the Object field to map to the resource object that you have created. By default, the value of this field is mapped to that of the `Xellerate User` resource object.

For IBM Lotus Notes, repeat all the steps you performed for Active Directory. Perform the following steps of that procedure differently for the Lotus Notes connector:

1. On the Resource Object tab, create the `LotNotes` resource object for trusted source reconciliation with Lotus Notes.

---

**Note:** You can assign a name to the resource object. This procedure is based on the use of `LotNotes` as the name assigned to the resource object.

---

2. When you create the resource object, add only the `e-mail address` attribute.
3. On the Object Reconciliation>>Reconciliation Action Rules tab, create rule conditions and action mappings. Create any rule condition other than user creation if no matches are found. If a match is found, then the link is established.
4. After you have added the fields and the reconciliation rules, delete the Lotus Notes-specific fields and the corresponding rules created in the `Xellerate User` resource object.
5. Create the `LotNotes` process definition in the Process Definition form. For detailed information about the procedure to create a process definition, see "[Process Definition Form](#)" on page 6-6. Based on the `Xellerate User` reconciliation field mappings, on the Reconciliation Field Mappings tab, add the field mappings for the `LotNotes` process definition.

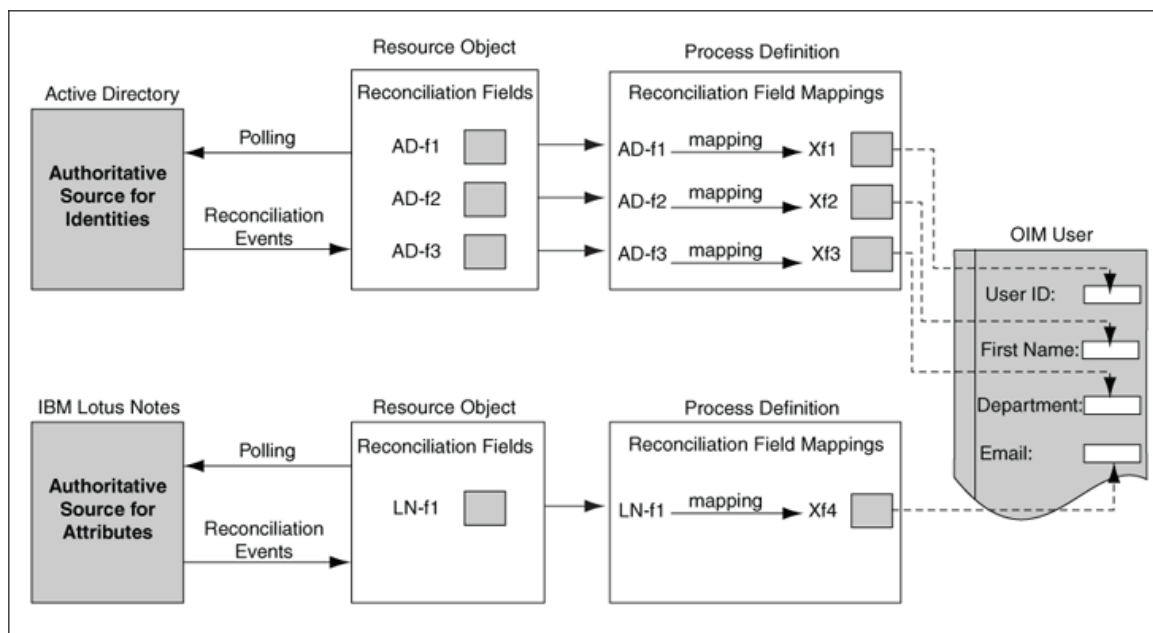
6. Delete the Lotus Notes-specific field mappings in the `Xellerate User` resource object.

For both Active Directory and Lotus Notes, perform the rest of the steps required to configure trusted source reconciliation. For example, while configuring the reconciliation scheduled task for each connector, specify the name of the trusted source resource object that must be used during reconciliation.

The current value of the scheduled task attribute would be `Xellerate User` and it must be updated with the name of the new resource object configured for trusted source user reconciliation for this connector.

Figure 5–8 shows the design time implementation of trusted source reconciliation of specific OIM User attributes.

**Figure 5–8 Trusted Source Reconciliation for Specific OIM User Attributes**



## 5.6 Service Account Management

Oracle Identity Manager supports service accounts. Service accounts are general administrator accounts (for example, `admin1`, `admin2`, `admin3`, and so on) 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 canceled (which would cause the undo tasks to start). 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 available through APIs.





---

# Process Management

This chapter describes process management with the Design Console. It contains the following topics:

- [Overview of Process Management](#)
- [Email Definition Form](#)
- [Process Definition Form](#)

## 6.1 Overview of Process Management

The Process Management folder provides you 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 you to create templates for e-mail notifications.
- **Process Definition:** This form is used to create and manage approval and provisioning processes. It also lets you start the Workflow Definition Renderer that displays your workflow definition in a graphical presentation.

## 6.2 Email Definition Form

The Email Definition form, as shown in [Figure 6–1](#), 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 6–1 Email Definition Form**

**Email Definition**

Name: Self Registration

**Type**

☐ Provisioning Related

☒ Request Related

☐ General

**Variables**

Targets: [Dropdown]

Variables: [Dropdown]

Object Name: [Text Box]

Language: en

Process Name: [Text Box]

Region: US

From: Requester [Dropdown] User Login: XE\_SYSDM

Subject: Self-registration request received

Body: Thank you for registering yourself with Oracle Corporation. Your request number is <Request Information.Request ID>. Please use this to track your request.

Email Definition | Email Definition Table

You apply e-mail definitions through the **Assignment** tab of the Process Definition form.

In [Figure 6–1](#), an e-mail definition was created. After the request represented by the Request ID e-mail variable is approved, an e-mail notification is sent from user SOLO to the user who created the request or to the requester.

### 6.2.1 Specifying the E-Mail Server

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

**See Also:** ["System Configuration Form"](#) on page 7-14 and ["IT Resources Form"](#) on page 5-4

To specify the e-mail server:

1. Open 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 e-mail server.
4. Once this IT resource is displayed, specify the IP address of the e-mail server and the name and password of the user who validates the usage of this server.

## 6.2.2 Email Definition Form

Table 6–1 describes the fields of the Email Definition form.

**Table 6–1 Fields of the Email Definition Form**

Field Name	Description
Name	The name of the e-mail definition.
Type	<p>This region contains three options for the following:</p> <ul style="list-style-type: none"> <li>Whether or not to categorize the e-mail definition as related to a request or a provisioning process</li> <li>Whether or not to associate a variable for the e-mail definition with a request or a provisioning process</li> <li>Whether or not to associate a variable for the e-mail definition with a general process</li> </ul> <p>To classify the e-mail definition as a provisioning definition or to associate the e-mail variable with a provisioning process, select the <b>Provisioning Related</b> option.</p> <p>To categorize the e-mail definition as a request definition or to associate the e-mail variable with a request, select the <b>Request Related</b> option.</p> <p>To categorize the e-mail definition as a general announcement, select the <b>General</b> option.</p>
Object Name	<p>From this lookup field, select the resource object that is associated with the provisioning process to which the e-mail definition is related.</p> <p><b>Note:</b> Leave this lookup field empty to make the e-mail definition available for use with all resource objects.</p>
Process Name	<p>From this lookup field, select a provisioning process that was assigned to the selected resource object. This is the provisioning process to which the e-mail definition is to be related.</p> <p><b>Note:</b> If the <b>Provisioning Related</b> option is not selected, both the <b>Object Name</b> and <b>Process Name</b> lookup fields are grayed out.</p>
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	<p>Select the source of the variable for the e-mail definition. For example, if the variable you want to select were Request Name, the source to select will be Request Information.</p> <p><b>Note:</b> The items that are displayed in this box reflect the options you selected from the Type region.</p>
Variables	<p>From this box, select the variable for the e-mail definition (for example, Request Name). The variables, which are displayed in this box, reflect the items you selected from the Targets box.</p> <p><b>Note:</b> For more information about e-mail variables and their parameters, see <i>Oracle Identity Manager Reference</i></p>
From	<p>Currently, two types of users can be selected from this box:</p> <ul style="list-style-type: none"> <li><b>Requester:</b> The user who created the request.</li> <li><b>User:</b> Any Oracle User with an e-mail address, which is displayed in the <b>Contact Information</b> tab of their Users form.</li> </ul>

**Table 6–1 (Cont.) Fields of the Email Definition Form**

Field Name	Description
User Login	The ID of the user in the From region of the e-mail notification. <b>Note:</b> If the User item is not displayed in the From box, the <b>User Login</b> field is grayed out.
Subject	The title of the e-mail definition.
Body	The content of the e-mail definition.

### 6.2.3 Creating an E-Mail Definition

To create an e-mail definition:

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

---

**Note:** If the **Request Related** option is selected, ensure that the name of the e-mail server is displayed 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 e-mail definition with a particular resource object, double-click the **Object Name** lookup field in the Lookup dialog box. Then, 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 e-mail 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 option is not selected, both the Object Name and Process Name lookup fields are grayed out.

---

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**) that is displayed in the From region of the e-mail notification.

---

---

**Note:** If the **Provisioning Related** option is not selected in Step 3, the **Manager of Provisioned User** item will not be displayed in the **From** box.

---

---

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

From the Lookup dialog box, select the user ID that is displayed in the From region of the e-mail notification.

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

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

This field contains the title of the e-mail definition.

12. Add information in the Body text area.

This text area contains the contents of the e-mail definition.

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

The following table describes the e-mail variables that you can customize for the e-mail definition.

Name	Description
Type	<p>These options specify whether or not a variable for the e-mail definition will be related to a provisioning process or a request.</p> <p>To associate the e-mail variable with a provisioning process, select the <b>Provisioning Related</b> option. To relate the variable to a request, select the <b>Request Related</b> option.</p>
Targets	<p>From this box, select the source of the variable for the e-mail definition. For example, if you want to use the <b>Request Name</b> variable, the source to select will be <b>Request Information</b>.</p>
Variables	<p>From this box, select the variable for the e-mail definition, for example, <b>Request Name</b>.</p>

---

---

**Note:** The items that are displayed 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 are displayed in the **Targets**, **Location Types**, and **Contact Types** boxes.

---

---

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

Subject	<Request Information Request ID> has been approved
Body	Hello, Nikita! <Request Information Request ID> has been approved.

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

**15. Click Save.**

The e-mail definition is created.

## 6.3 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 to 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 6–2](#) is 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 6–2 Process Definition Form**

The screenshot shows the Oracle Identity Manager Design Console interface. The left pane displays a tree view of the system configuration, with 'Process Definition' selected under 'Process Management'. The main pane shows the 'Process Definition' form for 'Solaris 8'. The form includes fields for Name, Type (Provisioning), Object Name, and Form Assignment (Table Name: UD\_SOLARIS). Below these fields are tabs for Tasks, Data Flow, Reconciliation Field Mappings, and Administrators. The 'Tasks' tab is active, showing a list of tasks with checkboxes for 'Default Assign...', 'Event Handler/A...', 'Conditional', and 'Required for Co...'. The tasks listed are:

Task	Default Assign...	Event Handler/A...	Conditional	Required for Co...
1 Reconciliation Insert Receive			<input checked="" type="checkbox"/>	<input type="checkbox"/>
2 Reconciliation Update Receive			<input checked="" type="checkbox"/>	<input type="checkbox"/>
3 Reconciliation Delete Receive			<input checked="" type="checkbox"/>	<input type="checkbox"/>
4 Service Account Alert			<input checked="" type="checkbox"/>	<input type="checkbox"/>
5 Service Account Moved			<input checked="" type="checkbox"/>	<input type="checkbox"/>
6 Service Account Changed			<input checked="" type="checkbox"/>	<input type="checkbox"/>
7 User Attestation Event Occu			<input checked="" type="checkbox"/>	<input type="checkbox"/>
8 Resource Attestation Event			<input checked="" type="checkbox"/>	<input type="checkbox"/>
9 System Validation			<input type="checkbox"/>	<input checked="" type="checkbox"/>

In [Figure 6–2](#), the **Solaris 8** provisioning process is created and assigned to the **Solaris 8** resource object.

[Table 6–2](#) describes the fields of the Process Definition form.

**Table 6–2 Fields of the Process Definition Form**

Field Name	Description
Name	The name of the process.
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 start a Web browser and display the current workflow definition by using the Workflow Renderer tool.
Default Process	<p>This check box determines if the current process is the default approval or provisioning process for the resource object with which it is associated.</p> <p>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 deselect 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.</p>
Auto Save Form	<p>This check box designates whether Oracle Identity Manager suppresses the 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.</p> <p>Select this check box to automatically save the data in the custom process form without displaying the form. If you select this check box, then you must supply either system-defined data or ensure that an adapter is configured to populate the form with the required data because the user will not be able to access the form. Deselect this check box to display the custom process form and allow users to enter data into its fields.</p>
Auto Pre-Populate	<p>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:</p> <ul style="list-style-type: none"> <li>Forms that are associated with the process</li> <li>Forms that contain fields with prepopulated adapters attached to them</li> </ul> <p>If the <b>Auto Pre-Populate</b> check box is selected, when the associated custom form is displayed, the fields that have prepopulate adapters attached to them will be populated by Oracle Identity Manager.</p> <p>When this check box is deselected, a user must populate these fields by clicking the <b>Pre-Populate</b> button on the toolbar or by manually entering the data.</p> <p><b>Note:</b> This setting does not control the triggering of the prepopulate adapter. It only determines if the contents resulting from the execution of the adapter are displayed in the associated form field(s) because of Oracle Identity Manager or a user.</p> <p>For more information about prepopulate adapters, see <i>Oracle Identity Manager Tools Reference</i>.</p> <p><b>Note:</b> This check box is only relevant if you have created a process form that is to be associated with the process and prepopulate adapters are used with that form.</p>
Table Name	The name of the table that represents the form that is associated with the process definition.

### 6.3.1 Creating 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, go 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, deselect this check box.

---

---

**Note:** If you select the **Auto Save Form** check box, ensure 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 about adapters and their relationship with fields of custom forms, see *Oracle Identity Manager Tools Reference*.

---

---

7. If a custom form is to be associated with the process definition, this form contains fields that have prepopulate 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), deselect 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, deselect the **Auto Pre-Populate** check box. For more information about prepopulate adapters, see *Oracle Identity Manager Tools Reference*.

---

---

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

From the Lookup window that is displayed, 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 is displayed.



From this window, you can select the field (for example, the Organization Name field) that will be used as an identifier of the process definition when an instance of the process is assigned to a resource object. This field and its value will then be displayed in the Reconciliation Manger form.

---

---

**See Also:** If a process has a custom process form attached to it, the fields on that form will also be displayed 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:** See *Oracle Identity Manager Administrative and User Console Guide* for detailed information about how to use the Workflow Definition Renderer

---

---

## 6.3.2 Tabs on the Process Definition Form

After you start 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.

### 6.3.2.1 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 6–3](#) displays the Tasks tab of the Process Definition form.

**Figure 6–3 Tasks Tab of the Process Definition Form**

Oracle Identity Manager Design Console : connected to jdbc:oracle:thin:@152.69.189.3:1521:orcl

File Edit Tool Bar Help

Oracle Identity Manager Design Console

- User Management
- Resource Management
- Process Management
  - Email Definition
  - Process Definition
- Administration
- Development Tools

Process Definition

Name: User Profile Edit

Type: Approval

Object Name: Request

Form Assignment: Table Name

Map Descriptive Field

Render Workflow

Default Process

Auto Pre-populate

Auto Save Form

Tasks

	Task	Default Assign...	Event Handler/Ad...	Conditional	Required for Com...
1	System Validation			<input type="checkbox"/>	<input checked="" type="checkbox"/>
2	Provide Information			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	Awaiting Approval Data			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Process Definition

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

---

**See Also:** See ["Modifying Process Tasks"](#) on page 6-17 for information about editing process tasks

---

#### 6.3.2.1.1 Adding a Process Task

Process tasks represent the steps that you must complete in a process.

To add a process task:

1. Click **Add**.

The Creating New Task dialog box is displayed.

2. In the **Task Name** field, enter the name of the process task.
3. From the Toolbar of the Creating New Task window, click **Save**. Then, click **Close**.

The process task is added to the process definition.

#### 6.3.2.1.2 Editing a Process Task

For instructions about how to edit and set process tasks, see ["Modifying Process Tasks"](#) on page 6-17.

#### 6.3.2.1.3 Deleting a Process Task

To delete a process task:

1. Select the process task that you want to delete.
2. Click **Delete**.

The process task is removed from the process definition.

### 6.3.2.2 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 6–4 shows the data flow tab of the Process Definition form.

**Figure 6–4 Data Flow Tab of the Process Definition Form**

	Source Object	Source Field	Sink Process	Sink Field
1	Solaris	Home Directory	Solaris	User's Home Directory
2		Child Form for Solaris Resource Object (Solaris)		Child Form for Solaris Process (Solaris)

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:** See ["Form Designer Form"](#) on page 8-2 for more information about editing process tasks

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 6–4, 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.

#### **6.3.2.2.1 Mapping a Parent Resource Form Field to a Process Form Field**

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 is displayed.

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

#### **6.3.2.2.2 Mapping a Child Resource Form Field to Child Process Form Field**

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 is displayed.

2. From the **Resource Object Child Table** box, select the table names of the child resource form.
3. From the **Process Child Table** box, select the target table names of the child process form.
4. From the window's Toolbar, click **Save**, and then click **Close**.

The selected table names of the child resource form is now mapped to the target table names of the child process form.

5. Click **Add Field Map**.

The Define Data Flow dialog box is displayed.

6. From the **Table Mapping** 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.

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

To break a mapping:

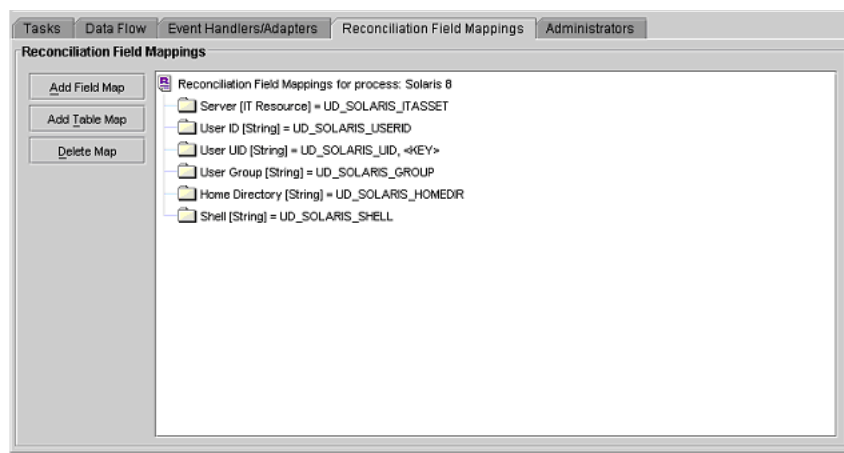
1. Select the data fields, which contain a mapping you want to break.
2. Click **Delete Map**.

The selected data field of the resource object form is no longer mapped to the selected data field of the process form.

### 6.3.2.3 Reconciliation Field Mappings Tab

You use the Reconciliation Field Mappings tab shown in [Figure 6–5](#) to define a relationship between data elements in a target system or trusted source and fields in Oracle Identity Manager.

**Figure 6–5 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 which 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 which fields are key fields. Key fields determine the values that must be same on the process form and the reconciliation event to generate a match on the **Processes Matched Tree** tab of the Reconciliation Manager form.

For each mapping, the following information is displayed:

- Name of the field, as defined on the **Reconciliation Fields** tab of the associated resource, on the target system 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.

---

**See Also:** See ["Multiple Trusted Source Reconciliation"](#) on page 5-30 for information about how fields are mapped for multiple trusted source reconciliation

---

- **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.

#### 6.3.2.3.1 User Account Status Reconciliation

If you want to configure user account status reconciliation, then you must perform the following:

- **For trusted sources:** You must create a reconciliation field, for example, *Status*, in the corresponding trusted resource object, which denotes the status of the user in the target. The value of this field must be either *Active* or *Disabled*. This reconciliation field must be mapped to the user attribute *status* in the corresponding process definition.
- **For target resources:** You must create a reconciliation field, for example, *Status*, in the corresponding resource object, which denotes the status of the resource in the target. The value of this field must be either *Enabled* or *Disabled*. This reconciliation field must be mapped to the process attribute *OIM\_OBJECT\_STATUS* in the corresponding process definition.

#### 6.3.2.3.2 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 mappings determine the fields that must be updated in Oracle Identity Manager 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 described in the following sections.

#### Mapping a Single Value Field

To map a single value field:

1. Click **Add Field Map**.

The Add Reconciliation Field Mappings dialog box is displayed.

2. Select the field on the target system that you want 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**. Go 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, go to step 5.

Set the **Key Field for Reconciliation Matching** check box for target resources only. If this check box 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 are displayed on the **Processes Matched Tree** tab of the Reconciliation Manager form. If this check box is deselected, 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 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:

1. Click **Add Table Map**.

The Add Reconciliation Table Mappings dialog box is displayed.

2. Select the multi-value field on the target system that you want 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.

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 is displayed.

7. Select the component (child) field you want 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** check box.

If this check box 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 are displayed on the **Processes Matched Tree** tab of the Reconciliation Manager form. If you deselect this check box, 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 improves 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 through 9 for each component (child) field defined on the multi-value field.
11. Click **Save**.

The mapping for the selected fields will be applied the next time a reconciliation event is received from the target resource.

#### 6.3.2.3 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. Go to the provisioning process definition for the associated resource.
2. Select the **Reconciliation Field Mappings** tab.
3. Select the field mapping you want to delete.
4. Click **Delete Map**.

The mapping for the selected field is deleted.

#### 6.3.2.4 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.

##### 6.3.2.4.1 Assigning a User Group to a Process Definition

To assign a user group:

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

The user group is displayed 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, go to Step 5.
5. To enable this user group to delete the current process definition, double-click the associated **Delete** check box. Otherwise, go to Step 6.
6. Click **Save**.

The user group is assigned to the process definition.

#### 6.3.2.4.2 Removing a User Group From a Process Definition

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.

### 6.3.3 Modifying Process Tasks

To modify a process task for a process definition, double-click its row heading. The Editing Task window is displayed, 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](#)

#### 6.3.3.1 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 6–6](#) shows the General tab of the Editing Task dialog box.

**Figure 6–6 General Tab of the Editing Task Dialog Box**

The screenshot shows the 'Editing Task: Create User' dialog box with the 'General' tab selected. The 'Task Name' field contains 'Create User'. The 'Task Description' field contains 'This task is used to create a user within Solaris'. The 'Duration' section shows 'Days' set to 1, 'Hours' set to 6, and 'Minutes' set to 30. The 'Task Properties' section includes checkboxes for 'Conditional', 'Required for Completion', and 'Constant Duration'. The 'Task Effect' dropdown is set to 'Enables Process Or Access To Application'. The 'Child Table' dropdown is set to 'None'.

Table 6–3 describes the fields of the General tab.

**Table 6–3 Fields of the General Tab of the Editing Task Dialog Box**

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	<p>This check box determines if a condition is met to add the current process task to the process.</p> <p>Select this check box to prevent the process task from being added to the process unless a condition has been met.</p> <p>Clear this check box to not require the condition to be met for the process task to be added to the process.</p>
Required for Completion	<p>This check box determines if the current process task must be completed for the process to be completed.</p> <p>Select this check box to require the process task to have a status of Completed before the process can be completed.</p> <p>Deselect this check box to ensure that the status of the process task does not affect the completion status of the process.</p>
Constant Duration	Not applicable
Task Effect	<p>From this box, select the process action you want to associate with the task, for example, disable or 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.</p> <p><b>Note:</b> If you do not want the process task to be associated with a particular process action, select <b>NONE</b> from the box.</p>

**Table 6–3 (Cont.) Fields of the General Tab of the Editing Task Dialog Box**

Field Name	Description
Disable Manual Insert	<p>This check box determines if a user can manually add the current process task to the process.</p> <p>Select this check box to prevent the process task from being added to the process manually.</p> <p>Deselect this check box to enable a user to add the process task to the process.</p>
Allow Cancellation while Pending	<p>This check box determines if the process task can be canceled if its status is Pending.</p> <p>Select this check box to allow the process task to be canceled if it has a Pending status.</p> <p>Deselecting this check box to prevent the process task from being canceled if its status is Pending.</p>
Allow Multiple Instances	<p>This check box determines if the process task can be inserted into the current process more than once.</p> <p>Select this check box to enable multiple instances of the process task to be added to the process.</p> <p>Deselect this check box to enable the process task to be added to the current process only once.</p>
Retry Period in Minutes	<p>If a process task is rejected, this field determines the interval before Oracle Identity Manager inserts a new instance of that task with the status of Pending.</p> <p>In <a href="#">Figure 6–6</a>, 30 is displayed in the Retry Period in Minutes field. 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.</p>
Retry Count	<p>Determines how many times Oracle Identity Manager retries a rejected task. In <a href="#">Figure 6–6</a>, 5 is displayed in the Retry Count field. If the Create User process task is rejected, Oracle Identity Manager adds a new instance of this task, and assigns 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.</p>
Child Table/ Trigger Type	<p>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 <b>Table Name</b> field of the <b>Process Definition</b> form.</p> <p>From the <b>Child Table</b> box, select the child table of the custom form where Oracle Identity Manager will perform an action.</p> <p>From the Trigger Type box, specify the action that Oracle Identity Manager is to perform in the child table. These actions include:</p> <ul style="list-style-type: none"> <li>■ <b>Insert.</b> Adds a new value to the designated column of the child table</li> <li>■ <b>Update.</b> Modifies an existing value from the corresponding column of the child table</li> <li>■ <b>Delete.</b> Removes a value from the designated column of the child table</li> </ul> <p><b>Note:</b> If the custom process form does not have any child tables associated with it, the <b>Child Table</b> box will be empty. In addition, the Trigger Type box will be grayed out.</p>

### 6.3.3.1.1 Modifying a Process Task's General Information

To modify the general information for a process task:

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

---

**Note:** 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, go 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, go 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, go 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, go to Step 10.
10. Click the **Task Effect** box.

From the custom menu that is displayed, select one of the following:

- **Enable Process or Access to Application.** If a resource is reactivated by using the enable function, then all tasks with this effect are inserted into the process. If you select this option, you must also select the **Allow Multiple Instances** check box.
  - **Disable Process or Access to Application.** If a resource is deactivated by using the disable function, all tasks with this effect are inserted into the process. If you select this option, you must also select 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 might 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** field, enter the number of times Oracle Identity Manager will retry a rejected task. For example, suppose **3** is displayed in the **Retry Count** field.

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 because 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:** Adds a new value to the designated column of the child table
- **Update:** Modifies an existing value from the corresponding column of the child table
- **Delete:** Removes 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 grayed out.

---

13. Click **Save**.

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

### 6.3.3.2 Integration Tab

By using 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 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, 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:** See ["Adapter Factory Form"](#) on page 8-2 and ["Event Handler Manager Form"](#) on page 9-1 for more information about adapters and event handlers

### 6.3.3.2.1 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 6-23 for details.

---

To assign an adapter or event handler to a process task:

1. Double-click the row heading of the process task to which you want to assign an event handler or adapter.

The Editing Task window is displayed.

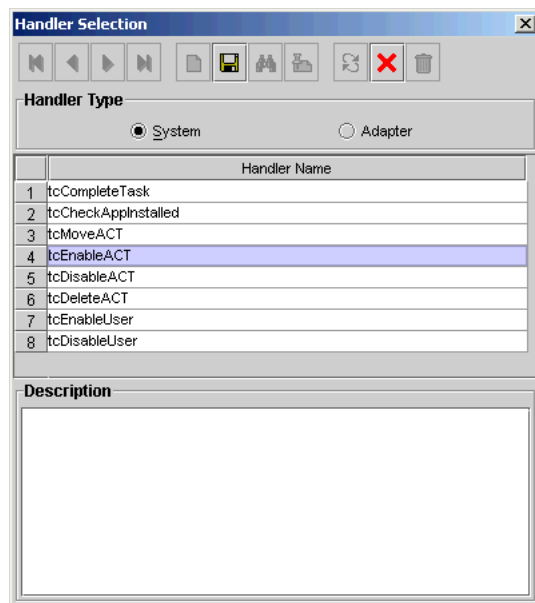
2. Click the **Integration** tab.
3. Click **Add**.

The **Handler Selection** dialog box is displayed, as shown in [Figure 6-7](#).

4. To assign an event handler to the process task, select the **System** option.

To add an adapter to the process task, select the **Adapter** option. A list of event handlers or adapters, which you can assign to the process task, is displayed in the **Handler Name** region.

**Figure 6-7 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 is displayed.
7. Click **OK**.

The event handler or adapter is assigned to the process task.

### 6.3.3.2.2 Mapping Adapter Variables

**See Also:** *Oracle Identity Manager Tools Reference* for more information about the items to select in this procedure

---

---

**Note:** 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 is displayed.
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.

### 6.3.3.2.3 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 is displayed.
2. Click **OK**.  
The event handler or adapter is removed from the process task.

### 6.3.3.3 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 effect 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. Before 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.

#### 6.3.3.3.1 Assigning a Preceding Task to a Process Task

To assign a preceding task to a process task:

1. Double-click the row heading of the process task to which you want to assign a preceding task.

The **Editing Task** window is displayed.

2. Click the **Task Dependency** tab.
3. From the Preceding Tasks region, click **Assign**.

The **Assignment** window is displayed.

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.

#### 6.3.3.3.2 Removing a Preceding Task from a Process Task

To remove a preceding task from a process task:

1. Select 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.

#### 6.3.3.3.3 Assigning a Dependent Task to a Process Task

To assign a dependent task to a process task:

1. Double-click the row heading of the process task to which you want to assign a dependent task.

The **Editing Task** window is displayed.

2. Click the **Task Dependency** tab.
3. From the **Dependent Tasks** region, click **Assign**.

The **Assignment** window is displayed.

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.

#### 6.3.3.3.4 Removing a Dependent Task from a Process Task

To remove a dependent task from a process task:

1. Select 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.

#### 6.3.3.4 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 started 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 in the form of an error message in a dialog box.

---

##### 6.3.3.4.1 Adding a Response to a Process Task

To add a response to a process task:

1. Double-click the row heading of the process task to which you want to add a response.

The Editing Task window is displayed.

2. Click the **Responses** tab.
3. In the **Responses** region, click **Add**.

A blank row is displayed in the Responses region.

4. Enter information in the **Response** field.

This field contains the response code value. This field is case-sensitive.

5. Enter information in the **Description** field. This field contains explanatory information about the response.

If the process task triggers the response, this information is displayed in the task information dialog box.

6. Double-click the **Status** lookup field.

From the Lookup window that is displayed, 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.

##### 6.3.3.4.2 Removing a Response from a Process Task

To remove a response from a process task:

1. Select the response that you want to delete.
2. From the **Responses** region, click **Delete**.

The response is removed from the process task.

---

**Note:** You will not be able to delete a response from a process task that is invoked for any provisioning instance, even if the response is existing or is newly added. However, if the process task is not invoked for any provisioning instance, you will be able to delete the response.

---

#### 6.3.3.4.3 Assigning a Generated Task to a Process Task

To assign a generated task to a process task:

1. Double-click the row heading of the process task to which you want to assign a generated task.

The Editing Task window is displayed.

2. Click the **Responses** tab.
3. Select the response code for which you want to assign generated tasks.
4. From the **Tasks to Generate** region, click **Assign**.

The Assignment window is displayed.

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.

#### 6.3.3.4.4 Removing a Generated Task From a Process Task

To remove a generated task from a process task:

1. Select a response code.
2. Select 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.

#### 6.3.3.5 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 canceled. 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 has a **Cancelled** status, then 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 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.

#### 6.3.3.5.1 Assigning an Undo Task to a Process Task

To assign an undo task to a process task:

1. Double-click the row heading of the process task to which you want to assign an undo task.

The Editing Task window is displayed.

2. Click the **Undo/Recovery** tab.
3. In the **Undo Tasks** region, click **Assign**.

The Assignment window is displayed.

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.

#### 6.3.3.5.2 Removing an Undo Task From a Process Task

To remove an undo task from a process task:

1. Select 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.

#### 6.3.3.5.3 Assigning a Recovery Task to a Process Task

To assign a recovery task to a process task:

1. Double-click the row heading of the process task to which you want to assign a recovery task.

The Editing Task window is displayed.

2. Click the **Undo/Recovery** tab.
3. From the **Recovery Tasks** region, click **Assign**.

The Assignment window is displayed.

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, do not select this check box.

#### 6.3.3.5.4 Removing a Recovery Task from a Process Task

To remove an recovery task from a process task:

1. Select 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.

#### 6.3.3.6 Notification Tab

You use this tab to designate the e-mail notification to be generated when the current process task achieves a particular status. A separate e-mail notification can be generated for each status a task can achieve. If an e-mail 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 e-mail notification to the user who is to be provisioned with the resource. If the Create User process task is rejected, the Process Task Completed e-mail notification is sent to the user and the user's manager.

---

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

See "[Email Definition Form](#)" on page 6-1 for details.

---

The following sections describe how to assign e-mail notifications to a process task, and remove e-mail notifications from a process task.

##### 6.3.3.6.1 Assigning an E-Mail Notification to a Process Task

To assign an e-mail notification to a process task:

1. Double-click the row heading of the process task to which you want to assign an e-mail notification.

The Editing Task dialog box is displayed.

2. Click the **Notification** tab.
3. Click **Assign**.

The Assignment dialog box is displayed.

4. From this window, select the e-mail template definition to use, and assign it to the process task.
5. Click **OK**.

The name of the e-mail notification is displayed in the Notification tab.

6. Double-click the **Status** lookup field.

From the Lookup window that is displayed, select a completion status level. When the process task achieves this status level, Oracle Identity Manager will send the associated e-mail notification.

7. Select the check boxes that represent the users who will receive the e-mail notification.

Currently, an e-mail notification can be sent to the following users:

- **Assignee.** This user is responsible for completing the associated process task.
- **Requester.** This user requested the process that contains the corresponding process task.
- **User.** This user will be provisioned with the resource once the associated process task is Completed.
- **User's Manager.** This user is the supervisor of the user, who will be provisioned with the resource once the corresponding process task is Completed.

8. Click **Save**.

The e-mail notification is assigned to the process task.

#### 6.3.3.6.2 Removing an E-mail Notification from a Process Task

The following procedure describes how to remove an e-mail notification from a process task.

To remove an e-mail notification from a process task:

1. Select the e-mail notification that you want to delete.
2. Click **Delete**.

The e-mail notification is removed from the process task.

#### 6.3.3.7 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 predefined provisioning statuses, which represent the various statuses of the resource object throughout its life cycle 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, and 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 required, or you want to associate a process task status with a different provisioning status for the resource object, you must break the link that currently exists.

For this example, there are five mappings among 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 canceled, the provisioning status for the resource object will be `Revoked`. `None` indicates that this status has no effect 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.

#### 6.3.3.7.1 Mapping a Process Task Status to a Provisioning Status

To map an process task status to a provisioning status:

1. Double-click the row heading 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 is displayed.

2. Click the **Task to Object Status Mapping** tab.
3. Select the desired process task status.
4. Double-click the **Object Status** lookup field.

From the Lookup window that is displayed, 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 is displayed in the Task to Object Status Mapping tab.

6. Click **Save**.

The process task status is mapped to the provisioning status.

#### 6.3.3.7.2 Unmapping a Process Task Status From a Provisioning Status

To unmap an process task status from a provisioning status:

1. Select the desired process task status.
2. Double-click the **Object Status** lookup field.

From the Lookup window that is displayed, select `None`. `None` indicates that this status has no effect on the provisioning status of the resource object.

3. Click **OK**.

The provisioning status of `None` is displayed 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.

#### 6.3.3.8 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 because these tasks are usually completed manually. On the other hand, tasks that belong 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, then the Solaris Process Tasks - User rule will be evaluated because 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 met, 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 about specifying the classification type of a rule, see ["Rule Designer Form"](#) on page 5-5. In addition, a Default rule is predefined in Oracle Identity Manager. This rule always evaluates to True. Therefore, it can be used as a safeguard mechanism to ensure that at least one predefined task assignment occurs if all the other rules fail.

---

[Table 6-4](#) describes the fields of the Assignment tab.

**Table 6-4 Fields of the Assignment Tab of the Editing Task Window**

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

**Table 6–4 (Cont.) Fields of the Assignment Tab of the Editing Task Window**

Field Name	Description
Target Type	<p>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:</p> <ul style="list-style-type: none"> <li>■ <b>User.</b> An Oracle Identity Manager user.</li> <li>■ <b>Group.</b> A user group.</li> <li>■ <b>Group User with Highest Priority.</b> The member of the specified user group with the highest priority number.</li> <li>■ <b>Group User with Least Load.</b> The member of the specified user group with the fewest process tasks assigned.</li> <li>■ <b>Request Target User's Manager.</b> The supervisor of the user who is being provisioned with the resource.</li> <li>■ <b>Object Authorizer User with Highest Priority.</b> The member of the user group (designated as an Object Authorizer user group for the resource) with the highest priority number.</li> <li>■ <b>Object Authorizer User with Least Load.</b> The member of the user group (designated as an Object Authorizer user group for the resource) with the fewest process tasks assigned.</li> <li>■ <b>Object Administrator.</b> A user group that is defined as an administrator of the associated resource object.</li> <li>■ <b>Object Administrator User with Least Load.</b> The member of the user group (designated as an Object Administrator user group) with the fewest process tasks assigned.</li> </ul> <p><b>Note:</b> Object Authorizer and Object Administrator user groups are defined in the <b>Object Authorizers</b> and <b>Administrators</b> tabs, respectively, of the Resource Objects form.</p>
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 <b>Email Name</b> lookup field, and selecting the <b>Send Email</b> 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.

#### 6.3.3.8.1 Adding a Rule to a Process Task

To add a rule to a process task:

1. Double-click the row heading of the task to which you want to add a rule.



The Editing Task window is displayed.

2. Click the **Assignment** tab.

3. Click **Add**.

A blank row is displayed in the Assignment tab.

4. Double-click the **Rule** lookup field.

From the Lookup window that is displayed, select the rule that you want to add to the process task. Then, click **OK**.

5. Double-click the **Target Type** lookup field.

From the Lookup window that is displayed, 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 is displayed, 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 is displayed, 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 is displayed, 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 e-mail notification when the task is assigned, go 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.

#### 6.3.3.8.2 Removing a Rule from a Process Task

To remove a rule from a process task:

1. Select the rule that you want to delete.

2. Click **Delete**.

The rule is removed from the process task.



---

# Administering Oracle Identity Manager with the Design Console

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

- [Overview of Design Control Administration](#)
- [Form Information Form](#)
- [Lookup Definition Form](#)
- [User Defined Field Definition Form](#)
- [System Configuration Form](#)
- [Remote Manager Form](#)
- [Password Policies Form](#)
- [Task Scheduler Form](#)

## 7.1 Overview of Design Control Administration

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 are displayed 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 the 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 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.
- **Password Policies:** You use this form to set password restrictions for the users and view the rules and resource objects that are associated with a password policy.
- **Task Scheduler:** You use this form to set up the schedules that determine when scheduled tasks are to be run.

## 7.2 Form Information Form

The Form Information form, shown in [Figure 7-1](#), is in the Design Console Administration folder. You use this form to specify the class name, the label that is displayed 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 are displayed in the Design Console Explorer.

**Figure 7-1** *Form Information Form*

The screenshot shows the 'Form Information' form in the Design Console. The form is titled 'Form Designer' and has several tabs: 'Table Information', 'Version Information', 'Operations', 'Properties', 'Administrators', 'Usage', 'Pre-Populate', 'Default Columns', 'User Defined Fields', and 'Object Permissions'. The 'Table Information' tab is active, showing fields for 'Table Name', 'Description', 'Form Type' (with radio buttons for 'Process' and 'Object'), and 'Object Name'. There is a 'Preview Form' button. The 'Version Information' section has 'Latest Version' and 'Active Version' fields. The 'Operations' section has a 'Current Version' dropdown, 'Create New Version', and 'Make Version Active' buttons. Below these sections is a table with columns: 'Name', 'Variant Type', 'Length', 'Field Label', 'Field Type', 'Default Value', 'Order', 'Application Profile', and 'Encrypted'. The table is currently empty, and there are 'Add' and 'Delete' buttons on the left side.

[Table 7-1](#) describes the data fields of this form.

**Table 7-1** *Fields in the Form Information Form*

Field Name	Description
Key	The system-generated ID for the form or folder.

**Table 7–1 (Cont.) Fields in the Form Information Form**

Field Name	Description
Class Name	The name of the class associated with the form or folder. For the forms and folders that are preinstalled with Oracle Identity Manager, this will be a <code>tc</code> class.
Description	The label that is displayed for this form or folder in the Oracle Identity Manager Explorer. For forms of the <b>childform</b> type, this value must include the name of the parent form and adhere to the following naming convention: <i>parent_form_name.child_form_name</i> .
Type	The form type associated with the form or folder. For folders, this must be <b>folder</b> . Valid selections are <b>folder</b> , <b>export</b> , <b>processform</b> , <b>childform</b> , <b>javaform</b> , <b>import</b> , and <b>menuitem</b> .
Graphic Filename	The name of the graphic file that is displayed 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 is displayed if the user presses <b>F1</b> when this form is active.

## 7.2.1 Adding an Oracle Identity Manager Form or Folder

To add an Oracle Identity Manager form or folder:

1. Go to 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 want 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 items 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 are displayed 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**.

**See Also:** See *Oracle Identity Manager Administrative and User Console Guide* for more information about Oracle Identity Manager Administrative and User Console

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 is displayed in the **Key** field.

## 7.2.2 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.

## 7.3 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 by using the Form Designer form

The Lookup Definition form shown in [Figure 7-2](#) is in the Design Console Administration folder. You use this form to create and manage lookup definitions.

**Figure 7–2 Lookup Definition Form**

Lookup Definition

Code: Password Policies: Policy Key

Field: PWR\_KEY

☐ Lookup Type ☒ Field Type

Required: ☒

Group: Password Policies

Lookup Code Information

	Code Key	Decode	Language	Country
1	Policy Key	Policy Key	en	US

Add

Delete

Lookup Definition

Table 7–2 describes the data fields of the Lookup Definition form.

**Table 7–2 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.
Lookup Type/Field Type	<p>These options designate if the lookup definition is to represent a text field, a lookup field, or a box.</p> <p>If you select the <b>Field Type</b> option, the lookup definition will represent a text field.</p> <p>If you select the <b>Lookup Type</b> option, 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.</p> <p><b>Note:</b> For forms or tabs that come packaged with Oracle Identity Manager, the lookup definition has already been set as either a lookup field <i>or</i> a box. This cannot be changed. However, you can add or modify the values that are accessible from the lookup field or box.</p> <p>For forms or tabs that are user defined, the user determines whether the lookup definition represents a lookup field or a box through the <b>Additional Columns</b> tab of the Form Designer form.</p> <p>For more information about specifying the data type of a lookup definition, see "<a href="#">Additional Columns Tab</a>" on page 8-5.</p>
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 be displayed.

The following sections describe how to create a lookup definition.

## 7.3.1 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** option.

If the lookup definition is to represent a text field, select the **Field Type** option.

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, go 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 is displayed.

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

**See Also:** See ["Lookup Definition Form"](#) on page 7-4 for more information about naming conventions

7. Click **Save**.

The lookup definition is created. The associated text field, lookup field, or box will be displayed in the Oracle Identity Manager or user-defined form or tab you specified.

## 7.3.2 Lookup Code Information Tab

The Lookup Code Information tab is in the lower half of the Lookup Definition form. You use this tab to create and manage detailed information about 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.

### 7.3.2.1 Creating and Modifying a Lookup Value

To create or modify a lookup value:

---

---

**Note:** For internationalization purpose, 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.

---

---

1. Open the Lookup Definition form.
2. Access a lookup definition.
3. If you are creating a lookup value, click **Add**.



A blank row is displayed in the **Lookup Code Information** tab.

If you are modifying a lookup value, select 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** option is selected, this field also represents what is displayed 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.

If the **Lookup Type** option is selected, this field also represents one of the following:

- The items that is displayed 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.

### 7.3.2.2 Deleting a Lookup Value

To delete a lookup value:

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

## 7.4 User Defined Field Definition Form

You might want 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 are displayed on the **User Defined Fields** tab of the form that is displayed in the **Form Name** data field. For example, [Figure 7-3](#) 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 7-3](#) is displayed 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 7–3 User Defined Field Definition Form**

Table 7–3 describes the data fields of the User Defined Field Definition form.

**Table 7–3 Fields of the User Defined Field Definition Form**

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

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

### 7.4.1 Selecting 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 is displayed, 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.

## 7.4.2 Tabs on the User Defined Field Definition Form

After you start 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.

### 7.4.2.1 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 is displayed on the **User Defined Fields** tab of the target form.

The field's order number determines the order in which a user-defined field is displayed on a form. In [Figure 7-4](#), the **Access Code Number** user-defined field has an order number of 1, so it is displayed 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 7-4](#) shows the User Defined Columns tab of the User Defined Field Definition Form.

**Figure 7-4 User Defined Columns Tab of the User Defined Field Definition Form**

	Label	Variant Type	Length	Column Name	Order	Field Type	Encrypted
1	Access Code Number	String	25	ACT_UDF_ACN	1	TextField	0

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.

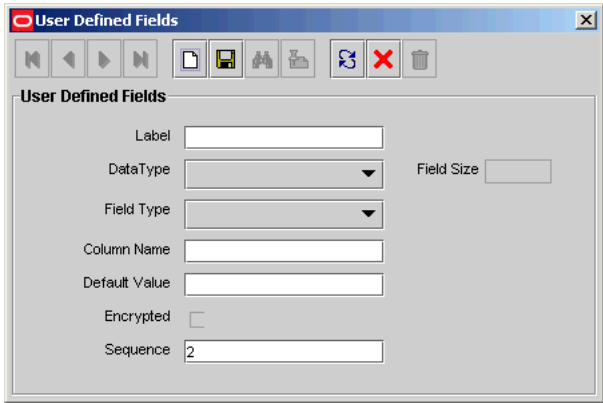
### Adding a User-Defined Field to an Oracle Identity Manager Form

To add a user-defined field:

1. Click **Add**.

The User Defined Fields dialog box is displayed, as shown in [Figure 7-5](#).

**Figure 7-5 User Defined Fields Dialog Box**



[Table 7-4](#) describes the fields in the User Defined Fields dialog box.

**Table 7-4 Fields of the User Defined Fields Dialog Box**

Field Name	Description
Label	<p>The label for the user-defined field. This label is displayed next to the user-defined field on the <b>User Defined Fields</b> tab of the target form.</p> <p>The maximum length for a label is 30 characters.</p>
Data Type	<p>From this box, select one of the following data types for the user-defined field:</p> <ul style="list-style-type: none"><li>▪ <b>String.</b> A user can enter a series of alphanumeric characters in this field.</li><li>▪ <b>Date.</b> When a user double-clicks this field, the Date and Time dialog box is displayed.</li><li>▪ <b>Integer.</b> A user can enter a number without a decimal point (for example, 3) in this user-defined field.</li><li>▪ <b>Boolean.</b> A user can enter two values into this field: True (1) or False (0).</li><li>▪ <b>Double.</b> A user can enter a double-precision floating-point number (or a double number) in this field.</li></ul>
Field Size	<p>The <b>Field Size</b> text field is enabled only for the String data type.</p> <p>In this field, enter the maximum amount of numbers or characters that a user can enter in the field.</p>

**Table 7–4 (Cont.) Fields of the User Defined Fields Dialog Box**

Field Name	Description
Field Type	<p>From this box, select one of the following field types for the user-defined field:</p> <ul style="list-style-type: none"> <li>■ Text Field. The field is displayed on the <b>User Defined Fields</b> tab of the target form as a text field.</li> <li>■ Lookup Field. The field is displayed on the <b>User Defined Fields</b> tab of the target form as a lookup field.</li> <li>■ Combo Box. The field is displayed on the <b>User Defined Fields</b> tab of the target form as a box.</li> <li>■ Text Area. The field is displayed on the <b>User Defined Fields</b> tab of the target form as a text area.</li> <li>■ Password Field. The field is displayed on the <b>User Defined Fields</b> tab of the target form as a text field. From this text field, a user can either query for an encrypted password (it is displayed as a series of asterisks [*]), or populate the field with an encrypted password, and save it to the database.</li> <li>■ Check Box. The field is displayed on the <b>User Defined Fields</b> tab of the target form as a check box.</li> <li>■ Date Field with Dialog. This field is displayed on the <b>User Defined Fields</b> tab of the target form as a lookup field. Once the user double-clicks this lookup field, a Date &amp; Time window is displayed. Oracle Identity Manager will then populate the data field with the date and time that the user selects from this window.</li> </ul> <p><b>Note:</b> The field types that are displayed in this box reflect the data type that is displayed in the <b>Data Type</b> box.</p>
Column Name	<p>The name of the user-defined field that is recognized by the database.</p> <p><b>Note:</b> This name consists of a <code>TABLE_NAME_UDF_</code> prefix, followed by the label that is associated with the user-defined field.</p> <p>For example, if the <b>Table Name</b> field of the <b>Organizations</b> form is <b>ACT</b>, and the name for the data field is <b>ACN</b>, the name of the user-defined field, which the database recognizes, would be <b>ACT_UDF_ACN</b>.</p> <p><b>Note:</b> The name in <b>Column Name</b> field cannot contain any spaces.</p>
Default Value	<p>This value is displayed in a user-defined field on the target form. Oracle recommends that you do not specify default values for passwords and encrypted fields.</p>
Encrypted	<p>This check box determines if the information that is displayed in the associated user-defined field is encrypted when it is exchanged between the client and the server.</p> <p>Select this check box to encrypt the information displayed in the user-defined field.</p> <p>Deselect this check box to not encrypt the information in the user-defined field.</p>
Sequence	<p>This field represents the order in which the user-defined field is displayed on the form. For example, if a 2 is displayed in the <b>Sequence</b> field, it is displayed below the user-defined field with a sequence number of 1.</p>

- Set the parameters for the user-defined field you are adding to a form, as shown in [Figure 7–6](#).

**Figure 7–6 User Defined Fields Dialog Box - Filled**

The screenshot shows a 'User Defined Fields' dialog box. It has a title bar with a close button. Below the title bar is a toolbar with icons for back, forward, save, delete, and other actions. The main content area is titled 'User Defined Fields' and contains several input fields and a checkbox. The 'Label' field contains 'Access Code Number'. The 'DataType' dropdown is set to 'String'. The 'Field Size' text box contains '25'. The 'Field Type' dropdown is set to 'Text Field'. The 'Column Name' text box contains 'ACT\_UDF\_ACN'. The 'Default Value' text box is empty. There is an 'Encrypted' checkbox which is unchecked. The 'Sequence' text box contains '1'.

In [Figure 7–6](#), the **Access Code Number** user-defined field is displayed 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 characters into it.

- From this window, click **Save**.
- Click **Close**.

The user-defined field is displayed in the **User Defined Columns** tab. Once the target form is started, this user-defined field usually is displayed in the **User Defined Fields** tab of that form. Because 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

To remove a user-defined field:

- Select the desired user-defined field.
- Click **Delete**.

The user-defined field is removed.

### 7.4.2.2 Properties Tab

You use this tab to assign properties and property values to the data fields that are displayed 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 or not the data field must be populated for the **Requests** form to be saved. The default property value for the **Required** property is **false**.
- Visible Field**, which determines whether or not the data field is displayed on the **Requests** form. The default property value for the **Visible Field** property is **true**.

Because the property values for the **Required** and **Visible Field** properties are **true** for this data field, once the **Requests** form is started, the **Issue Tracking Item** data field is displayed in the **User Defined Fields** tab. In addition, this field must be populated for the form to be saved.

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

**Figure 7–7 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.

**See Also:** See ["Form Designer Form"](#) on page 8-2 for more information about how to add a property and property value to a data field, or remove a property and property value from a data field

### 7.4.2.3 Administrators Tab

Figure 7–8 shows the Administrators tab of the User Defined Field Definition form.

**Figure 7–8 Administrators Tab of the User Defined Field Definition Form**

	Group Name	Write	Delete
1	SYSTEM ADMINISTRATORS	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	OPERATORS	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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 about 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

To assign administrative privileges to a user group for a UDF definition:

1. Click **Assign**.

The Assignment dialog box is displayed.

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

The user group is displayed 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, go to Step 5.
- 5. To enable this user group to delete information in the current definition, double-click the associated **Delete** check box. Otherwise, go 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**

To remove administrative privileges:

- 1. Select 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.

**7.5 System Configuration Form**

The System Configuration form, as shown in [Figure 7–9](#), is in the Design Console Administration folder. You use this form to define and set the value of properties that control the actions 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 7–9 System Configuration Form**

The screenshot shows the 'System Configuration' form. At the top, there is a 'Key' field with the value '2' and four radio buttons: 'System' (unchecked), 'Client' (unchecked), 'Client/Server' (unchecked), and 'Server' (checked). Below these are three text fields: 'Name' with 'Organization Process Restriction', 'Keyword' with 'XL.OrganizationProcessRestrict', and 'Value' with 'FALSE'. There are two tabs, 'Users' and 'Groups', with 'Groups' selected. Below the tabs are 'Assign' and 'Delete' buttons. A table with the header 'Group Name' contains one entry: '1 SYSTEM ADMINISTRATORS', which is highlighted in blue. At the bottom left, there is a 'System Configuration' label.

[Table 7–5](#) describes the data fields of this form.



**Table 7–5 Fields of the System Configuration Form**

Field Name	Description
Key	The system-generated ID for one instance of the property definition. There can be more than one instance of a definition, for example, one for system administrators and another for all users.
System	<p>This check box designates if this instance of the property definition applies to all users in Oracle Identity Manager, that is, it is a systemwide instance, or only to selected users and user groups.</p> <p>Select this check box to apply this setting to all users. The <b>Users</b> and <b>Groups</b> tabs will be grayed out.</p> <p>Deselect this check box to specify that an instance of the property applies to certain users and groups.</p> <p><b>Note:</b> The <b>System</b> check box is grayed out if the <b>Server</b> option is selected.</p>
Client Client/Server Server (Radio buttons)	<p>These options determine if this instance of the property definition applies to the client, the server, or both.</p> <p>Select the <b>Client</b> option to apply property value only to the client.</p> <p>Select the <b>Client/Server</b> option to apply the property value to both the client and server.</p> <p>Select the <b>Server</b> option to apply the property value only to the server. Selecting this option disables the <b>System</b> check box. Systemwide settings do not apply to the server.</p>
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	<p>The property's unique ID.</p> <p>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 retrieve) differently for two separate users, you must create two instances of this property definition.</p> <p><b>Note:</b> For more information about the various properties you can set for the client and server, see "Rule Elements, Variables, Data Types, and System Properties" in <i>Oracle Identity Manager Reference</i>.</p>
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 <b>System</b> check box 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.

### 7.5.1 Creating and Editing an Instance of a Property Definition

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

1. Go to the System Configuration form.
2. If you are creating a new instance of a property definition, then 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 the errors.

---

If you are editing an existing instance of a property definition, then query for the property definition.

3. Select the **Client**, **Client/Server**, or **Server** option.
4. Determines whether or not you want this instance of the property definition to apply to all users or only to select users and user groups by selecting or deselecting the **System** check box.

---

**Note:** If you selected the **Server** option in Step 3, then the **System** check box will be grayed out. If this is the case, then go 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.

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

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

---

**Note:** If this is a systemwide 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.

---

1. Go to the System Configuration form.
2. Query for the instance of the property definition you want to assign to a user or group.  
  
**See Also:** See the "Rule Elements, Variables, Data Types, and System Properties" section in *Oracle Identity Manager Reference* for more information about how to add a property and property value to a data field, or remove a property and property value from a data field.
3. Select the **Client**, **Client/Server**, or **Server** option, depending on whether the instance of this property definition will apply to the client only, both the client and the server, or just the server.
4. To assign the property instance to one or more users, click the **Users** tab. Otherwise, to assign the property instance to one or more user groups, click the **Groups** tab.
5. Click **Assign**.  
The Assignment dialog box is displayed.

6. Select and assign the desired users or groups and then, click **OK**.
7. Click **Save**.

The instance of the property definition is assigned to the users or groups you selected in Step 6.

### 7.5.3 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. Go to the System Configuration form.
2. Query for the instance of the property definition from which you want to remove a user or group.
3. Select the desired 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.

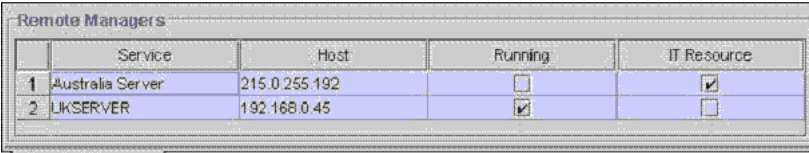
## 7.6 Remote Manager Form

The Remote Manager is a lightweight network server that enables you to integrate with target systems whose APIs cannot 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 7–10](#) is 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 or not the remote manager is running
- Whether or not it represents IT resources that Oracle Identity Manager can use

**Figure 7–10 Remote Manager Form**



	Service	Host	Running	IT Resource
1	Australia Server	215.0.255.192	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2	UKSERVER	192.168.0.45	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Remote Manager

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. Although it can handshake with Oracle Identity Manager, because the **Running** check box is deselected, the remote server is unavailable. 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. Because the **Running** check box is selected, the remote server is operable. However, because the **IT Resource** check box is deselected, this remote manager does not represent an IT resource or resources that Oracle Identity Manager can use.

---

**See Also:** See *Oracle Identity Manager Tools Reference* for information about how the Remote Manager form is used with other Oracle Identity Manager forms

---

## 7.7 Password Policies Form

The Password Policies form is in the Design Console Administration/Policies folder. You can use this form to:

- Set password restrictions (for example, define the minimum and maximum length of passwords).
- See rules and resource objects that are associated with a password policy.

Figure 7–11 shows the Password Policies form.

**Figure 7–11 Password Policies Form**

**Password Policies**

Policy Name

Policy Description

Policy Rules **Usage**

Minimum Length  Warn After (Days)  Expires After (Days)

Minimum Password Age (Days)  Disallow Last  Passwords

☐ Complex Password

1. The password is at least six characters long.

2. The password contains characters from at least three of the following five categories

a. English Uppercase Characters (A-Z) b. English Lowercase Characters (a-z)

c. Base 10 Digits (0-9) d. Non-alphanumeric (for example: !, \$, # or ^)

e. Unicode Characters

3. The password does not contain three or more characters from the user's account name.

☒ Custom Policy

Maximum Length  Characters Required

Maximum Repeated Characters  Characters Not Allowed

Minimum Numeric Characters  Characters Allowed

Minimum Alphanumeric Characters  Substrings Not Allowed

Minimum Unique Characters  Start With Alphabet ☐ Disallow User ID ☐

Minimum Alphabet Characters  Disallow First Name ☐ Disallow Last Name ☐

Minimum Uppercase Characters

Minimum Lowercase Characters

Special Characters: Minimum  Maximum

Unicode Characters: Minimum  Maximum

**Password Dictionary Details**

Password File

Password File Delimiter

**Password Policies**

To create a password policy, you must first enter the required values in the following fields of the Password Policies form:

- **Policy Name:** The name of the password policy
- **Policy Description:** Short description of the password policy

The following sections provide more information about using the Password Policy form:

- [Creating a Password Policy](#)
- [Tabs on the Password Policies Form](#)

### 7.7.1 Creating a 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. In the **Policy Description** field, enter a short description of the password policy.
4. Click **Save**.

---



---

**Note:**

- A password policy is not applied during the creation of an OIM user through trusted reconciliation.
  - After you create a password policy, 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 applied when the criteria for the rule are met. Each password policy can be used by multiple resources.
- 
- 

### 7.7.2 Tabs on the Password Policies Form

The tabs in this form become functional after you create a password policy. The following sections discuss these tabs:

- [Policy Rules Tab](#)
- [Usage Tab](#)

#### 7.7.2.1 Policy Rules Tab

You use the Policy Rules tab to specify criteria for your password policy, for example, the minimum and maximum length of passwords.

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

- Enter information in the appropriate fields, or select the required check boxes. For example, to indicate that a password must have a minimum length of four characters, enter **4** in the **Minimum Length** field.
- In the **Password File** field, enter the directory path and name of the password policy file (for example, `c:\xellerate\userlimits.txt`). This file contains predefined terms that you do not want to be used as passwords. The delimiter specified in the **Password File Delimiter** field separates these terms.

[Figure 7-11](#) shows the **Policy Rules** tab of the Password Policies form.

[Table 7-6](#) describes the data fields on the **Policy Rules** tab. You specify the password policy criteria in these fields.

---

**Note:** If a data field is empty, then passwords do not have to meet the criteria of that field for it to be valid. For example, when the **Minimum Numeric Characters** data field is blank, Oracle Identity Manager will accept a password, regardless of the number of characters included in it.

---

**Table 7–6 Fields of the Policy Rules Tab of the Password Policies Form**

Field Name	Description
Minimum Length	<p>The minimum number of characters that a password must contain for the password to be valid.</p> <p>For example, if you enter <b>4</b> in the <b>Minimum Length</b> field, then the password must contain at least four characters.</p> <p>This field accepts values from 0 to 999.</p>
Expires After Days	<p>The duration in days for which users can use a password.</p> <p>For example, if you enter <b>30</b> in the <b>Expires After Days</b> field, then users must change their passwords by the thirtieth day from when it was created or last modified.</p> <p><b>Note:</b> After the number of days specified in the <b>Expires After Days</b> field passes, a message is displayed asking the user to change the password.</p> <p>This field accepts values from 0 to 999.</p>
Disallow Last Passwords	<p>The frequency at which old passwords can be reused. This policy ensures that users do not change back and forth among a set of common passwords.</p> <p>For example, if you enter <b>10</b> in the <b>Disallow Last Passwords</b> field, then users are allowed to reuse a password only after using 10 unique passwords.</p> <p>To disable this option, you can enter <b>0</b> in the <b>Disallow Last Passwords</b> field.</p> <p>This field accepts values from 0 to 999.</p>
Minimum Password Age	<p>The duration in days for which users must keep a password before changing it. This is to prevent users from entering a new password and then immediately reverting to the previous password.</p> <p>For example, if you enter <b>15</b> in the <b>Minimum Password Age</b> field, the users cannot change their passwords before 15 days.</p> <p>This field accepts values from 0 to 999.</p>
Warn After (Days)	<p>The number of days that must pass before a user is notified that the user's password will expire on a designated date.</p> <p>For example, suppose you enter <b>30</b> in the <b>Maximum Password Age</b> field, and <b>20</b> in the <b>Warn After (Days)</b> field, and the password is created on November 1. On November 21, the user will be informed that the password will expire on December 1.</p> <p>This field accepts values from 0 to 999.</p>

On the Policy Rules tab of the Password Policies form, you can configure either a complex password or custom password policy. If you select the **Complex Password** option, then you cannot use the Custom Password option setup and passwords will be evaluated against the complex password criteria that you enter on the Policy Rules tab.

The remaining fields in the Policy Rules tab are discussed in the following sections:

- [Complex Password](#)
- [Custom Policy](#)

### Complex Password

The following are the complex password criteria:

- The password is at least six characters long. This password length overrides the **Minimum Length** field if the value entered in the **Minimum Length** field is less than 6. For example, if you enter 2 in the **Minimum Length** field, at least six characters will be required for the password because it must have at least six characters according to the complex password criteria.
- The password must contain characters from at least three of the following five categories:
  - English uppercase characters (A - Z)
  - English lowercase characters (a - z)
  - Base 10 digits (0 - 9)
  - Non-alphanumeric characters (for example: !, \$, #, or %)
  - Unicode characters
- The password cannot contain three or more consecutive characters from the user name.

When checking against the user's full name, characters such as commas, periods, dashes or hyphens, underscores, spaces, pound signs, and tabs are treated as delimiters that separate the name into individual character sets. Each character set that has three or more characters is searched in the password. If the character set is present in the password, then the password change is rejected. For example, the name John Richard-Doe is split into three character sets: John, Richard, and Doe. This user cannot have a password that consists of three continuous characters from either John or Richard or Doe anywhere in the password. However, the password can contain the substring d-D because the hyphen (-) is treated as the delimiter between the substrings Richard and Doe. In addition, the search for character sets in the password is not case-sensitive.

---

**Note:** If the user's full name is less than three characters in length, then the password is not checked against it because the rate at which passwords will be rejected is too high.

---

### Custom Policy

If you select the **Custom Policy** option, then you can set a custom password policy by using the fields listed in [Table 7-7](#).

**Table 7-7** *Fields of the Policy Rules Tab for Setting Custom Password Policy*

Field Name	Description
Maximum Length	<p>The maximum number of characters that a password can contain.</p> <p>For example, if you enter 8 in the <b>Maximum Length</b> field, then a password is not accepted if it has more than eight characters.</p> <p>This field accepts values from 1 to 999.</p>

**Table 7–7 (Cont.) Fields of the Policy Rules Tab for Setting Custom Password Policy**

Field Name	Description
Maximum Repeated Characters	<p>The maximum number of times a character can be repeated in a password.</p> <p>For example, if you enter <b>2</b> in the <b>Maximum Repeated Characters</b> field, then a password is not accepted if any character is repeated more than two times. For example, RL112211 would not be a valid password because the character 1 is repeated three times.</p> <p><b>Note:</b> In this example, there are four instances of the character 1, which means that it is repeated three times.</p> <p>This field accepts values from 1 to 999.</p>
Minimum Numeric Characters	<p>The minimum number of digits that a password must contain.</p> <p>For example, if you enter <b>1</b> in the <b>Minimum Numeric Characters</b> field, then a password must contain at least one digit.</p> <p>This field accepts values from 0 to 999.</p>
Minimum Alphanumeric Characters	<p>The minimum number of letters or digits that a password must contain.</p> <p>For example, if you enter <b>6</b> in the <b>Minimum Alphanumeric Characters</b> field, then a password must contain at least six letters or numbers.</p> <p>This field accepts values from 0 to 999.</p>
Minimum Unique Characters	<p>The minimum number of nonrepeating characters that a password must contain.</p> <p>For example, if you enter <b>1</b> in the <b>Minimum Unique Characters</b> field, then a password is accepted if at least one character in the password is not repeated. For example, 1a23321 would be a valid password because the character a in the password is not repeated although the remaining characters are repeated.</p> <p>This field accepts values from 0 to 999.</p>
Minimum Alphabet Characters	<p>The minimum number of letters that a password must contain.</p> <p>For example, if you enter <b>2</b> in the <b>Minimum Alphabet Characters</b> field, then the password is not accepted if it has less than two letters.</p> <p>This field accepts values from 0 to 999.</p>
Special Characters: Minimum	<p>The minimum number of non-alphanumeric characters (for example, #, %, or &amp;) that a password must contain.</p> <p>For example, if you enter <b>1</b> in the <b>Special Characters: Minimum</b> field, then a password must have at least one non-alphanumeric character.</p> <p>This field accepts values from 0 to 999.</p>
Special Characters: Maximum	<p>The maximum number of non-alphanumeric characters that a password can contain.</p> <p>For example, if you enter <b>3</b> in the <b>Special Characters: Maximum</b> field, then a password is not accepted if it contains more than three non-alphanumeric characters.</p> <p>This field accepts values from 1 to 999.</p>
Minimum Uppercase Characters	<p>The minimum number of uppercase letters that a password must contain.</p> <p>For example, if you enter <b>8</b> in the <b>Uppercase Characters: Minimum</b> field, then a password is not accepted if it contains less than eight uppercase letters.</p> <p>This field accepts values from 0 to 999.</p>



**Table 7–7 (Cont.) Fields of the Policy Rules Tab for Setting Custom Password Policy**

Field Name	Description
Minimum Lowercase Characters	<p>The minimum number of lowercase letters that a password must contain.</p> <p>For example, if you enter <b>8</b> in the <b>Minimum Lowercase Characters</b> field, then a password is not accepted if it has less than eight lowercase letters.</p> <p>This field accepts values from 0 to 999.</p>
Unicode Characters: Minimum	<p>The minimum number of Unicode characters that a password must contain.</p> <p>For example, if you enter <b>3</b> in the <b>Unicode Characters: Minimum</b> field, then the password is not accepted if it has less than three Unicode characters.</p> <p>This field accepts values from 0 to 999.</p>
Unicode Characters: Maximum	<p>The maximum number of Unicode characters that a password can contain.</p> <p>For example, if you enter <b>8</b> in the <b>Unicode Characters: Maximum</b> field, then a password is not accepted if it has more than eight Unicode characters.</p> <p>This field accepts values from 1 to 999.</p>
Characters Required	<p>The characters that a password must contain.</p> <p>For example, if you enter <b>x</b> in the <b>Characters Required</b> field, then a password is accepted only if it contains the character <b>x</b>.</p> <p>The character you specify in the <b>Characters Required</b> field, must be mentioned in the <b>Characters Allowed</b> field.</p>
Characters Not Allowed	<p>The characters that a password must not contain.</p> <p>For example, if you enter an exclamation point (!) in the <b>Characters Not Allowed</b> field, then a password is not accepted if it contains an exclamation point.</p>
Characters Allowed	<p>The characters that a password can contain.</p> <p>For example, if you enter the percent sign (%) in the <b>Characters Allowed</b> field, then a password is accepted if it contains a percent sign.</p> <p><b>Note:</b> The password is valid if it contains only the characters specified in the <b>Characters Allowed</b> field.</p> <p>If you specify the same character in the <b>Characters Allowed</b> and <b>Characters Not Allowed</b> fields, then an error message is returned when you create the password policy.</p>
Substrings Not Allowed	<p>A series of consecutive alphanumeric characters that a password must not contain.</p> <p>For example, if you enter <b>IBM</b> in the <b>Substrings Not Allowed</b> field, then a password is not accepted if it contains the letters <b>I</b>, <b>B</b>, and <b>M</b>, in successive order.</p>
Start With Alphabet	<p>The letters with which a password must begin.</p> <p>For example, if you specify the character <b>a</b> in the <b>Start With Alphabet</b> field, then a password will be accepted if it starts with the character <b>a</b>.</p>

**Table 7–7 (Cont.) Fields of the Policy Rules Tab for Setting Custom Password Policy**

Field Name	Description
Disallow User ID	<p>This check box specifies if the user ID will be accepted as the whole password or as part of the password.</p> <p>When this check box is selected, a password will not be valid if the user ID is entered in the <b>Password</b> field.</p> <p>If you deselect this check box, then the password will be accepted, even if it contains the user ID.</p>
Disallow First Name	<p>This check box specifies if the user's first name will be accepted as the whole password or as part of the password.</p> <p>When this check box is selected, a password will not be valid if the user's first name is entered in the <b>Password</b> field.</p> <p>If you deselect this check box, then the password will be accepted, even if it contains the user's first name.</p>
Disallow Last Name	<p>This check box specifies if the user's last name will be accepted as the whole password or as part of the password.</p> <p>When this check box is selected, a password will not be valid if the user's last name is entered in the <b>Password</b> field.</p> <p>If you deselect this check box, then the password is accepted, even if it contains the user's last name.</p>
Password File	<p>The path and name of a file that contains predefined terms, which are not allowed as passwords.</p> <p><b>Note:</b> If settings on the <b>Policy Rules</b> tab differ from the specifications in the password file, then Oracle Identity Manager will use the settings on the <b>Policy Rules</b> tab.</p>
Password File Delimiter	<p>The delimiter character used to separate terms in the password file.</p> <p>For example, if a comma (,) is entered in the Password File Delimiter field, then the terms in the password file will be separated by commas.</p>

On the System Configuration form, you can set the value of the Force Password Change At First Login property, which has the `XL.ForcePasswordChangeAtFirstLogin` keyword, to `True` for forcing a user to change the password when the user logs in for the first time. Note that the user is forced to change the password at first logon only when the user is created with the `XL.ForcePasswordChangeAtFirstLogin` keyword already set to `True`.

---

**Note:**

- See the "Creating Users" section in the *Oracle Identity Manager Administrative and User Console Guide* for information about forcing users to change their password at first logon.
  - If the password field is present on a form, the password policy is applied to the resource object to which this form is associated and if the form is displayed in the Administrative and User Console, then the **View Password Policies** link is displayed in the Administrative and User Console.
- 

Whenever you change the value of the Force Password Change At First Login property, you must restart the server or purge the cache for the change to take effect. For purging the cache, the cache category is `ServerCachedProperties`.

**See Also:** "Purging the Cache" in *Oracle Identity Manager Best Practices Guide* for information about purging the cache by using the `PurgeCache` utility

---

**Note:** The default value of the `Force Password Change At First Login` property is `True`. To disable this property, set the value to `False`.

---

You can attach a process form with one of the Password fields to a resource. If you apply a password policy to the same resource and create an access policy for the resource, then the password entered by the user in the process form is not validated against the password policy rules. This is because when a resource is provisioned to the user, the user must provide the password, which will be validated against the password policy rules applied to the resource.

### Setting the Criteria for a Password Policy

To set the criteria for a password policy:

1. Open the required password policy definition.
2. Click the **Policy Rules** tab.
3. Either enter information into the appropriate fields, or select the required check boxes.
4. Click **Save**.

#### 7.7.2.2 Usage Tab

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

For example, [Figure 7-12](#) shows the **Solaris** password policy, and the **Password Validation Rule** have been assigned to the Solaris resource object.

[Figure 7-12](#) shows the **Usage** tab of the Password Policies form.

**Figure 7-12 Usage Tab of the Password Policies Form**

The screenshot shows the 'Password Policies' form with the 'Usage' tab selected. The 'Policy Name' is 'Solaris' and the 'Policy Description' is 'P/W limits for Solaris'. Below the tabs, there is a table with two columns: 'Rule' and 'Object'. The table contains one entry: '1 Password Validation Rule' under the 'Rule' column and 'The Solaris Resource Object' under the 'Object' column.

Rule	Object
1 Password Validation Rule	The Solaris Resource Object

**See Also:** "Password Policies Rule Tab" on page 5-25 for more information about the relationship between password policies and resource objects

# 7.8 Task Scheduler Form

The Task Scheduler form shown in [Figure 7-13](#) is 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 7-13 Task Scheduler Form**

The screenshot shows the 'Task Scheduler Form' with the following details:

- Task Definition**
  - Scheduled Task: Password Expiration Task
  - Class Name: Thor.Schedule.Task.tc.TaskPasswordExpiration
  - Status: INACTIVE
  - Max Retries: 5
  - Start: Start time 10/18/04 12:00:00 AM
  - Interval: Recurring Intervals, 1 Minute(s)
  - Buttons: Add, Delete
- Task Attributes**
  - Table with columns: Attribute Name, Attribute Value
- Deployment Utility**
  - Task Scheduler

**Note:** As stated earlier, 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**.

Because the scheduler daemon cannot perform its designated function if it is not running, you must verify that it is active.

For more information about modifying the value of a system property, see ["System Configuration Form"](#) on page 7-14.

[Table 7-8](#) lists and describes the fields of the Task Scheduler form.

**Table 7-8 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. <b>Note:</b> The scheduler daemon triggers the execution of a scheduled task. The Java class actually executes the task.

**Table 7–8 (Cont.) Fields of the Task Scheduler Form**

Field Name	Description
Status	<p>The task's status. Currently, a scheduled task has four status levels:</p> <ul style="list-style-type: none"> <li>■ <b>INACTIVE</b>: The scheduled task ran successfully, and it is set to run again at the date and time specified in the <b>Next Start</b> field.</li> <li>■ <b>RUNNING</b>: The scheduled task is running.</li> <li>■ <b>COMPLETED</b>: The scheduled task ran successfully, but it will not run again (the frequency is set to <b>Once</b>).</li> <li>■ <b>ERROR</b>: An error occurred due to which the task could not be started.</li> <li>■ <b>FAILED</b>: The scheduled task failed while running.</li> </ul>
Max Retries	<p>If the task is not completed, the number of times that Oracle Identity Manager tries to complete the task before assigning a status of <b>ERROR</b> to it.</p>
Disabled	<p>This check box is used to designate whether or not the scheduler daemon triggers a scheduled task.</p> <p>If this check box is selected, the scheduler daemon does not trigger the task, even when the date and time that is displayed in the <b>Start Time</b> or <b>Next Start Time</b> fields matches the current date and time.</p> <p>When this check box is deselected, and the date and time that is displayed in the <b>Start Time</b> or <b>Next Start Time</b> fields matches the current date and time, the scheduler daemon triggers the task.</p>
Stop Execution	<p>This check box is used to designate whether or not the scheduler daemon can stop a scheduled task with a status of <b>RUNNING</b>.</p> <p>If this check box is selected, and the task's status is <b>RUNNING</b>, the scheduler daemon stops the task from being executed. In addition, the task's status changes to <b>INACTIVE</b>.</p> <p>When this check box is deselected, the scheduler daemon does not stop a task with a status of <b>RUNNING</b> from being executed.</p>
Start Time	<p>The date and time of when the task is scheduled to run for the first time.</p> <p><b>Note:</b> If the task is set to be run more than once, the scheduler daemon refers to the date and time that is displayed in the <b>Next Start Time</b> field.</p>
Last Start Time	<p>The latest date and time of when the task started to run.</p>
Last Stop Time	<p>The most recent date and time of when the task stopped running.</p>
Next Start Time	<p>The subsequent date and time of when the task is scheduled to run.</p> <p><b>Note:</b> If the task is set to be run only once, the scheduler daemon refers to the date and time that is displayed in the <b>Start Time</b> field.</p>

**Table 7–8 (Cont.) Fields of the Task Scheduler Form**

Field Name	Description
Daily, Weekly, Monthly, Yearly	<p>These options are used to designate if the task is to be run daily, weekly, monthly, or annually.</p> <p>If one of these radio buttons is selected, then the scheduler daemon triggers the associated task once a day, week, month, or year, at the date and time specified in the <b>Start Time</b> field.</p> <p>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.</p>
Recurring Intervals	<p>This option designates that the task is to be run on a fixed, recurring basis.</p> <p>If this option is selected, then the scheduler daemon triggers the associated task on a recurring basis.</p> <p>If this option is deselected, then the scheduler daemon does not trigger the associated task on a recurring basis.</p> <p><b>Note:</b> If the <b>Recurring Intervals</b> option is selected, you must set the interval by entering a value into the text field below the option, and selecting a unit of measure from the adjacent box.</p>
Once	<p>This option is used to designate that the task is to be run only once.</p> <p>If this option is selected, the scheduler daemon triggers the associated task once, at the date and time specified in the <b>Start Time</b> field.</p> <p>When this option is deselected, the scheduler daemon triggers the associated task more than once.</p>

The following sections provide more information about scheduled tasks:

- [Predefined Scheduled Tasks](#)
- [Creating a Scheduled Task](#)
- [Deleting a Custom Scheduled Task](#)

### 7.8.1 Predefined Scheduled Tasks

[Table 7–9](#) lists the predefined scheduled tasks that are available in this release of Oracle Identity Manager.

**Table 7–9 Predefined Scheduled Tasks**

Scheduled Task	Description	User-Configurable Attributes
Password Expiration Task	This scheduled task sends e-mail to users whose password expiration date has passed at the time when the task was run and then updates the USR_PWD_EXPIRED flag on the user profile.	None
Password Warning Task	This scheduled task sends e-mail to users whose password warning date had passed at the time when the task was run and then updates the USR_PWD_WARNED flag on the user profile.	None
User Operations	This scheduled task performs the operation specified by the UserOperation attribute on the user account specified by the UserLogin attribute.	<ul style="list-style-type: none"> <li>■ UserLogin: User ID of the user account</li> <li>■ UserOperation: Operation that you want to perform on the user account. The value of this attribute can be ENABLE, DISABLE, or DELETE.</li> </ul>
Attestation Grace Period Expiry Checker	This scheduled task delegates the attestation process after the grace period expires.	None
Task Escalation	This scheduled task escalates pending tasks whose escalation time had elapsed at the time when the scheduled task was run.	None
Task Timed Retry	This scheduled task creates a retry task for rejected tasks whose retry time has elapsed and whose retry count was greater than zero.	None
Set User Deprovisioned Date	A deprovisioning date is defined when a user account is created. For users whose deprovisioning date had passed at the time when this schedule task was run, the task sets the deprovisioned date as the current date.	None
Disable User After End Date	An end date is defined when a user account is created. This scheduled task disables user accounts for which the end date had passed the current date at the time when the task is run.	<ul style="list-style-type: none"> <li>■ Day Max: The maximum number of user accounts that can be disabled by the task in one day, regardless of the number of times the task runs in a given day.</li> <li>■ Task Max: The maximum number of user accounts that can be disabled in one run of the task.</li> </ul>
Set User Provisioned Date	<p>This scheduled task sets the provisioned date to the current date for users for whom all of the following conditions are true:</p> <ul style="list-style-type: none"> <li>■ The provisioning date is in the past.</li> <li>■ The deprovisioned date has not been set.</li> <li>■ The deprovisioning date has not been reached or is NULL.</li> </ul> <p>The setting of the provisioned date to the current date causes the policies to be evaluated for the users affected by an access policy update. After the evaluation is completed for the users, the usr_policy_update flag is set to NULL.</p>	None

**Table 7–9 (Cont.) Predefined Scheduled Tasks**

Scheduled Task	Description	User-Configurable Attributes
Enable User After Start Date	A start date is set when a user account is created. This scheduled task enables user accounts for which the start date has passed, and the user status is Disabled Until Start Date.	None
Trigger User Provisioning	This scheduled task approves resources that are in the Approved, Waiting To Provision status for all users whose provisioning date had passed when the task was run.	None
Scheduled Provisioning Task	When this scheduled task is run, it triggers scheduled request provisioning processes.	None
Remove Open Tasks	This scheduled task removes information about open tasks and pending approvals (that are older than the specified number of days) from the table that serves as the source for the list displayed in the Administrative and User Console.	Day Limit Number of days for which information about an open task or pending approval should be retained in the table before the information is deleted The default value is 60 days.
Remove Group Priority Gaps Task	A priority is assigned to every group that is created in Oracle Identity Manager. When a group is removed, the priority assigned to the next group in the priority list is <i>not</i> advanced automatically. When this scheduled task is run, it resequences group priorities up to the specified priority number. This scheduled task is needed only when you want to ensure that tasks are always assigned to groups with the highest priority.	Max Priority Gap Priority level up to which the scheduled task must resequence group priority levels For example, suppose you specified 10 as the value of this attribute. Groups with priority 3 and 7 were removed before the task was run. When the task runs, the priority levels of groups with priority level 4 through 10 are resequenced so that their new priority levels range from 3 through 8. The default value is 10.
ReSubmit Request Tasks	This scheduled task resubmits requests that are in the REQUEST_INITIALIZED state and sends e-mail notifications by using the specified e-mail template.	<ul style="list-style-type: none"> <li>Resubmit requests older than (hours) Number of hours that must elapse before a request is resubmitted</li> <li>Email Notification User (userid) User account that is to be shown as the sender of the e-mail</li> <li>Email Template (Template Name) Template of the e-mail to be sent</li> </ul>



**Table 7–9 (Cont.) Predefined Scheduled Tasks**

Scheduled Task	Description	User-Configurable Attributes
Resubmit Reconciliation Event	This scheduled task resubmits reconciliation events whose status remains at Event Received for the time that you specify by using the window attribute.	<p>window</p> <p>Number of hours for which the task has remained at the Event Received status</p>
Issue Audit Messages Task	This scheduled task fetches audit message details from the aud_jms table and sends a single JMS message for a particular identifier and auditor entry in the aud_jms table. An MDB processes the corresponding audit message.	<p>Max records: Use this attribute to specify the maximum number of audit messages to be processed for a specified scheduled task run. The default value of this attribute is 400.</p>
Initiate Attestation Processes	This scheduled task initiates a call to the Attestation Engine to run attestation processes that are scheduled to run at a time that has passed.	None

## 7.8.2 Creating a Scheduled Task

In addition to creating a scheduled task, if the task requires 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 you how to add an attribute to a scheduled task and remove a task attribute from a scheduled task.

To create a scheduled task:

1. Go to 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 tries to complete the task before assigning a status of ERROR to it.
5. Ensure that the **Disabled** and **Stop Execution** check boxes are not selected.
6. Double-click the **Start Time** field.

From the Date & Time window that is displayed, set the date and time that the task is scheduled to run. If you specified that the task is to be executed on a recurring basis (by selecting the **Recurring Intervals** option), 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** options.
  - To set the task to run only once, select **Once**.
  - To set the task to run on a fixed, recurring basis, select **Recurring Intervals**, set the interval by entering a value into the text field below the option, and 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 because 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.

**7.8.2.1 Adding 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, enter the attribute's value.
4. From the Toolbar, click **Save**.

The task attribute is added to the scheduled task.

**7.8.2.2 Removing a Task Attribute**

To remove a task attribute:

1. Select the task attribute that you want to remove.
2. Click **Delete**.

The attribute is removed from the scheduled task.

**7.8.3 Deleting a Custom Scheduled Task**

To delete a scheduled task:

---

---

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

---

---

1. Go to 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 existing task attributes by following the instructions in "[Removing a Task Attribute](#)" on page 7-32.
4. Click **Delete** 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.

---

## Development Tools

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

- [Overview of Developments Tools](#)
- [Adapter Factory Form](#)
- [Adapter Manager Form](#)
- [Form Designer Form](#)
- [Error Message Definition Form](#)

### 8.1 Overview of Developments Tools

The 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 an 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 are displayed 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 by 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:** You use this form to 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.

## 8.2 Adapter Factory Form

Adapters extend the internal logic and functionality of Oracle Identity Manager. In addition, they interact 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 8–1](#) shows the Adapter Factory Form.

**Figure 8–1 Adapter Factory Form**

**See Also:** *Oracle Identity Manager Tools Reference* for more information about adapters or the Adapter Factory

## 8.3 Adapter Manager Form

The Adapter Manager form is in the Development Tools folder. It is used to compile multiple adapters simultaneously, as shown in [Figure 8–2](#).

**Figure 8–2 Adapter Manager Form**

	Adapter Name	Status	Type
1	Grant DB Access		T
2	Display Uppercase Letters for User ID		P
3	Create DB User		T
4	Solaris Disable User	Recompile	T

**See Also:** *Oracle Identity Manager Tools Reference* for detailed information about how adapters are compiled

## 8.4 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 8–3](#) shows 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 by 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 8–3 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. For this example, because the name of the form is **SOLARIS**, its table name is **UD\_SOLARIS**.

---

Table 8–1 describes the data fields of the Form Designer form.

**Table 8–1 Fields of the Form Designer Form**

Field Name	Description
Table Name	<p>The name of the database table that is associated with the form.</p> <p><b>Note:</b> The table name contains the <b>UD_</b> prefix, followed by the form name. If the name of the form is <b>SOLARIS</b>, then its table name is <b>UD_SOLARIS</b>.</p>
Description	<p>Explanatory information about the form.</p> <p><b>Important:</b> The text that is displayed in the <b>Description</b> field is the name of the form.</p>
Preview Form	When you click this button, the form is displayed. This way, you can see how it looks and functions before you make it active.
Form Type	<p>These options are used to designate if the form is to be assigned to a process or a resource object.</p> <p>If you select the Process option, then the form is associated with an approval or provisioning process. By selecting the <b>Object</b>, the form is to be assigned to a resource object.</p>
Object Name	<p>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 <i>resource object name</i>.</p> <p>Double-click this field to see the available resource object names.</p>
Latest Version	The most recent version of the form.
Active Version	<p>The version of the form that is used with the designated process or resource object.</p> <p><b>Note:</b> After a version of the form is displayed in the Active Version field, it cannot be modified.</p>
Current Version	This version of the form is being viewed and contains information, which is displayed throughout the various tabs of the Form Designer form.
Create New Version	<p>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 effecting the original version of the form.</p> <p><b>Note:</b> If you create a new version of the form and click <b>Refresh</b>, the name that you provided for this version is displayed in the Current Version box.</p>
Make Version Active	<p>By clicking this button, you can specify that the current version of the form is the one that is to be assigned to the process or resource object. In other words, this version is now active.</p> <p><b>Note:</b> After a version of the form is active, it cannot be modified. Instead, you must create another additional version of the form (by clicking the <b>Create New Version</b> button).</p>

The following section describes how to create a form.

## 8.4.1 Creating a Form

To create a form:

1. Open the Form Designer form.
2. In the **Table Name** field, enter 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. If the name of the form is **SOLARIS**, its table name is **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** option.

If the form is to be assigned to a resource object, select the **Object** option.

5. Click **Save**.

The form is created. The words **Initial Version** are displayed 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.

## 8.4.2 Tabs of the Form Designer Form

After you open 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](#)

### 8.4.2.1 Additional Columns Tab

You use the **Additional Columns** tab to create and manage data fields. These data fields are displayed on the associated form that is created by using the Form Designer form.

[Figure 8–4](#) shows the Additional Columns tab of the Form Designer form.

Figure 8–4 Additional Columns Tab of the Form Designer Form

Name	Variant Type	Length	Field Label	Field Type	Default Value	Order	Application Profile	Encrypted
UD_SOLARIS_UID	String	20	UID	TextField		1	<input type="checkbox"/>	<input type="checkbox"/>
UD_SOLARIS_USERNAME	String	20	UserID	TextField		2	<input checked="" type="checkbox"/>	<input type="checkbox"/>
UD_SOLARIS_PASSWORD	String	20	Password	PasswordField		3	<input type="checkbox"/>	<input checked="" type="checkbox"/>
UD_SOLARIS_SHELL	String	20	Shell	TextField	/usr/bin/sh	4	<input checked="" type="checkbox"/>	<input type="checkbox"/>
UD_SOLARIS_HOME	String	20	Home Directory	TextField	/export/home	5	<input checked="" type="checkbox"/>	<input type="checkbox"/>
UD_SOLARIS_GROUP	String	20	User Group	TextField	other	6	<input checked="" type="checkbox"/>	<input type="checkbox"/>
UD_SOLARIS_ITASSET	long		IT Asset	LookupField		7	<input type="checkbox"/>	<input type="checkbox"/>

Table 8–2 describes the data fields of the Additional Columns tab.

Table 8–2 Fields of the Additional Columns Tab

Name	Description
Name	<p>The name of the data field that is displayed in the database and is recognized by Oracle Identity Manager.</p> <p><b>Note:</b> This name consists of the &lt;TABLENAME_&gt; prefix followed by the name of the data field.</p> <p>For example, if the name in the <b>Table Name</b> field of the Form Designer form is <b>UD_PASSWORD</b> and the name for the data field is <b>USERNAME</b>, then the data field name that is displayed in the database and that Oracle Identity Manager recognizes, would be <b>UD_PASSWORD_USERNAME</b>.</p>
Variant Type	<p>From this lookup field, select the variant type for the data field. The variant type denotes the type of data that the field accepts.</p> <p>This data field must be one of nine variant types: <b>Byte, Double, Date, Byte Array, Boolean, Long, String, Short, and Integer</b>.</p>
Length	<p>The length in characters of the data field.</p> <p><b>Note:</b> The following is applicable only if you have installed Oracle Identity Manager on Microsoft SQL Server:</p> <p>You can add User-Defined Fields (UDFs) on a system, process, or object form. However, after you add a field to a form, if the total length of all the fields on the form exceeds 8060 bytes, then the following error message is displayed:</p> <p>Maximum allowable length for a Table ROW is exceeding SQL Server ROW limit of 8060.</p> <p>To avoid this error, you must ensure that the total field length does not exceed 8060 bytes. If this error message is displayed, then you must reduce the length of fields so that it is less than the Microsoft SQL Server ROW limit of 8060.</p>
Field Label	<p>The label that is associated with the data field. This label is displayed next to the data field on the form that is generated by Oracle Identity Manager.</p>



**Table 8–2 (Cont.) Fields of the Additional Columns Tab**

Name	Description
Field Type	<p data-bbox="537 268 1430 321">From this lookup field, select the data type of the data field. The data type represents how the data must be displayed in the field.</p> <p data-bbox="537 338 1024 363">You can select one of the following data types:</p> <ul style="list-style-type: none"> <li data-bbox="537 380 1446 495"> <p>■ <b>TextField:</b> This data field is displayed on the generated form as a text field.</p> <p>If the text field is display-only (the text in the field is displayed in red font), then a user can use the field only to run a query. Otherwise, the user can also populate the field with information, and save it to the database.</p> </li> <li data-bbox="537 512 1446 627"> <p>■ <b>LookupField:</b> This data field is displayed on the generated form as a lookup field.</p> <p>If this lookup field is display-only, then a user can use the field only to run 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.</p> </li> <li data-bbox="537 644 1446 760"> <p>■ <b>TextArea:</b> This data field is displayed on the generated form as a text area.</p> <p>If this text area is display-only, then a user can only read the information that is displayed in it. Otherwise, the user can also populate the text area with data, and save this information to the database.</p> </li> <li data-bbox="537 777 1446 982"> <p>■ <b>ITResourceLookupField:</b> This data field is displayed on the generated form as a lookup field. From this lookup field, a user can select a lookup value that represents an IT resource, and save this value to the database.</p> <p><b>Note:</b> If you select this data field, then you must specify the type of server for the IT resource from the Property Value field.</p> <p>For more information about adding a property value to a data field, see <a href="#">"Adding a Property and Property Value to a Data Field"</a> on page 8-14.</p> </li> <li data-bbox="537 999 1446 1314"> <p>■ <b>DateFieldWithDialog:</b> This data field is displayed on the generated form as a text field.</p> <p>If this text field is display-only, then a user can use the field only to run a query.</p> <p>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 &amp; Time window). Then, this date and time can be saved to the database.</p> <p>■ <b>CheckBox:</b> This data field is displayed on the generated form as a check box.</p> <p>If this check box is display-only, then a user can only see whether the check box is selected or deselected. Otherwise, the user can also select or deselect the check box, and save this setting to the database.</p> </li> <li data-bbox="537 1331 1446 1478"> <p>■ <b>PasswordField:</b> The text entered in this field is displayed as a series of asterisk (*) characters.</p> <p>If the name of the column with field type as Password Field is PASSWORD and a password policy is attached to the associated resource object, then the password entered in this field is verified against the password policy.</p> </li> <li data-bbox="537 1495 1446 1583"> <p>■ <b>RadioButton:</b> This data field is displayed on the generated form as an option.</p> <p>A user can select or deselect the radio button, and save this setting to the database.</p> </li> <li data-bbox="537 1600 1446 1663"> <p>■ <b>DataCombobox:</b> This data field is displayed on the generated form as a list.</p> <p>A user can select an item from the list and save this selection to the database.</p> </li> <li data-bbox="537 1680 1446 1732"> <p>■ <b>DisplayOnlyField:</b> This data field is not enabled for the user to enter a value. This type of fields can only display data based on values in other fields.</p> </li> </ul>

**Table 8–2 (Cont.) Fields of the Additional Columns Tab**

Name	Description
Default Value	<p>This value is displayed in the associated data field after the form is generated and if no other default value was specified from the following scenarios:</p> <ul style="list-style-type: none"> <li>■ A pre-populate adapter, which is attached to the form field, is run.</li> <li>■ 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.</li> <li>■ 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.</li> <li>■ 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. It is strongly recommended that you do not specify default values for passwords and encrypted fields.</li> </ul>
Order	<p>The sequence number that represents where the data field is positioned on the generated form.</p> <p>For example, a data field with an order number of 2 is displayed below a data field with an order number of 1.</p>
Application Profile	<p>This check box designates if the most recent value of this field should be displayed on the Object Profile tab of the Users form after the resource associated with this form has been provisioned to the user and achieved the Enabled status.</p> <p>If this check box is selected, then the label and value of this field is displayed on the Object Profile tab of the Users form for users provisioned with the resource.</p>
Encrypted	<p>This check box determines if the information, which is displayed in the associated data field, is to be encrypted when it is transmitted between the server and the client.</p> <p>If this check box is selected, then the information that is displayed in the data field is encrypted when it is transmitted between the client and the server.</p>

**8.4.2.1.1 Adding a Data Field to a Form**

To add a data field to a form:

---

**Note:** When creating a data field of text (field type) with the Encrypted option selected, the values are displayed 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 is displayed as asterisks (\*) in the Administrative and User Console, and the data is encrypted in the database.

---

1. In the Additional Columns tab, click **Add**.  
A blank row is displayed in the Additional Columns tab.
2. In the **Name** field, enter the name of the data field, which is displayed 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 is displayed in the **Table Name** field is **UD\_PASSWORD**, and the name for the data field is **USERNAME**, the data field name that is displayed 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 is displayed, 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 is displayed 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.

**See Also:** [Table 8–2](#) for more information about data types

7. In the **Default Value** field, enter the value that is displayed in the associated data field once the form is generated, and if no other default value has been specified.

**See Also:** [Table 8–2](#) for more information about the scenarios where a default value could be set

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 is displayed 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 is displayed in the **Default Value** field, select the **Application Profile** check box. Otherwise, go to Step 10.
10. If you want the information that is displayed in the data field to be encrypted when it is transmitted between the client and the server, then select the **Encrypted** check box. Otherwise, go to Step 11.

11. Click **Save**.

#### 8.4.2.1.2 Removing a Data Field From a Form

To remove a data field from a form:

---

**Note:** While adding a new field, if you assign it the same name as a field that was removed, then the variant type (data type) of the new field remains the same as that of the field that was removed. For example, suppose you remove the Addr1 field to which the String variant type was applied. You then create a field with the same name and apply the Boolean variant type to it. Now, when you view or use the form on which the new Addr1 field is added, the variant type of the field is String and not Boolean.

---

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 8-18.
2. Select the data field that you want to remove.
3. Click **Delete**.

The data field is removed from the form.

While adding a new field, if you assign it the same name as a field that was removed, then the variant type (data type) of the new field remains the same as that of the field that was removed. For example, suppose you remove the Addr1 field to which the String variant type was applied. You then create a field with the same name and apply the Boolean variant type to it. Now, when you view or use the form on which the new Addr1 field is added, the variant type of the field is String and not Boolean.

#### 8.4.2.2 Child Table(s) Tab

Sometime you might have to add the same data fields to multiple forms that are created by 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.

If this form contains the data fields that are required by another form, then 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, the Design Console enables you to do so. 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:** Adds a new value to the designated column of the child table
- **Update:** Modifies an existing value from the corresponding column of the child table
- **Delete:** Removes a value from the designated column of the child table

[Figure 8–5](#) shows the Child Table(s) tab on the Form Designer form.

**Figure 8–5 Child Table(s) Tab of the Form Designer Form**

Parent Table	Parent Version	Child Table	Child Version
1 UD_SOLARIS	Initial Version	UD_DBACCESS	Initial Version

---

**See Also:** See ["Process Definition Form"](#) on page 6-6 for more information about setting up Oracle Identity Manager to insert, edit, or delete a value from in a column of a child table

---

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 started, the data fields in the **UD\_SOUTH** child table are displayed 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.

**Note:** If the form, which is represented by the child table, has not been made active, you cannot assign it to the parent form.

#### 8.4.2.2.1 Assigning a Child Table to a Form

To assign a child table to a form:

---

**Note:** If the form that is represented by the child table is active, it will not be displayed in the Assignment window, and you will not be able to assign it to the parent form.

---

1. Click **Assign**.

The Assignment window is displayed.

2. From this window, select the child table, and assign it to the form.
3. Click **OK**.

The selected child table is assigned to the form.

#### 8.4.2.2.2 Removing a Child Table from a Form

To remove a child table from a form:

1. Select the child table that you want to remove.

## 2. Click **Delete**.

The child table is removed from the form.

### 8.4.2.3 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 not selected, 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 not selected, 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 not selected, the user group cannot delete data from fields of this form (when it is instantiated).

Figure 8–6 shows the Object Permissions tab of the Form Designer Form.

**Figure 8–6 Object Permissions Tab of the Form Designer Form**

Group Name	Allow Insert	Allow Update	Allow Delete
1 SYSTEM ADMINISTRATORS	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2 Web Client Group	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3 Sales Engineer Group	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4 Project L7 Admin Group	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5 ALL USERS	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Suppose the SYSTEM ADMINISTRATORS user group can create, modify, and delete information that is displayed 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 not selected). 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 not selected, 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.

#### 8.4.2.3.1 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 is displayed.

2. Select the user group, and assign it to the form that was created by a user.
3. Click **OK**.

The user group is displayed 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, go 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, go 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, go to Step 7.
7. Click **Save**.

The user group is assigned to the user-created form.

#### 8.4.2.3.2 Removing a User Group From a User-Created Form

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

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

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

#### 8.4.2.4 Properties Tab

Figure 8–7 shows the Properties Tab of the Form Designer Form. You use this tab to assign properties and property values to the data fields that are displayed on the form that is created through the Form Designer form.

**Figure 8–7 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 or not the data field must 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 is displayed on the form, once Oracle Identity Manager generates the form. The default value for the **Visible Field** property is `true`.

Because 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 are displayed. In addition, each field must 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 grayed out until you create a data field for the form by using the **Additional Columns** tab.

For more information about the properties and property values you can select, see the "Rule Elements, Variables, Data Types, and System Properties" section in *Oracle Identity Manager Reference*.

---

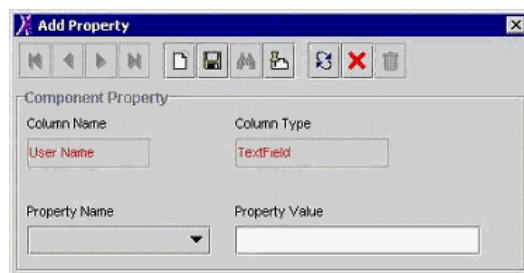
#### 8.4.2.4.1 Adding a Property and Property Value to a Data Field

To add a property and property value to a data field:

1. Select the data field to which you want to add a property and property value.
2. Click **Add Property**.

The Add Property dialog box is displayed, as shown in [Figure 8–8](#).

**Figure 8–8 Add Property Dialog Box**




---

**Note:** The text that is displayed in the Column Name and Column Type fields are the names and types of data fields you selected.

---

In this example, the User Name data field was selected (as indicated by User Name displayed in the **Column Name** field). In addition, the data type of this field is a text field.

[Table 8–3](#) lists the fields of the Add Property dialog box.



**Table 8–3 Fields of the Add Property Dialog Box for a Data Field**

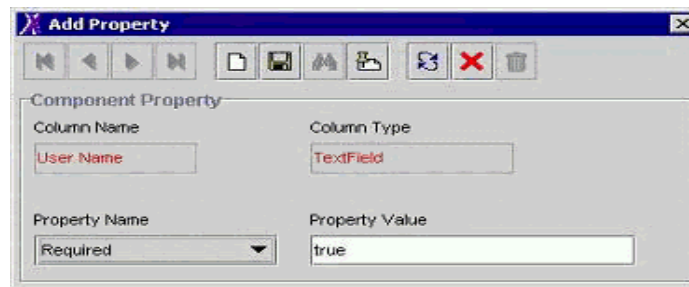
Name	Description
Column Name	The name of the data field.
Column Type	The data type of the data field.
Property Name	From this box, select the property for the data field.
Property Value	In this field, enter the property value, which is associated with the property that is displayed in the Property Name box.

---

**Note:** The menu items displayed in the Property Name box reflect the data type of the selected data field.

---

- Set the parameters for the property and property value that you are adding to the data field. [Figure 8–9](#) shows the Add Property dialog box with values.

**Figure 8–9 Add Property Dialog Box - Filled**

For this example, because the value of the Required property for the User Name data field was set to true, once the associated form is generated, this field must be populated. Otherwise, the form cannot be saved.

---

**See Also:** See the "Rule Elements, Variables, Data Types, and System Properties" section in *Oracle Identity Manager Reference* for more information about the parameters and property values to select

---

- From the Add Property window's Toolbar, click **Save**.
- Click **Close**.

The property and property value are added to the data field.

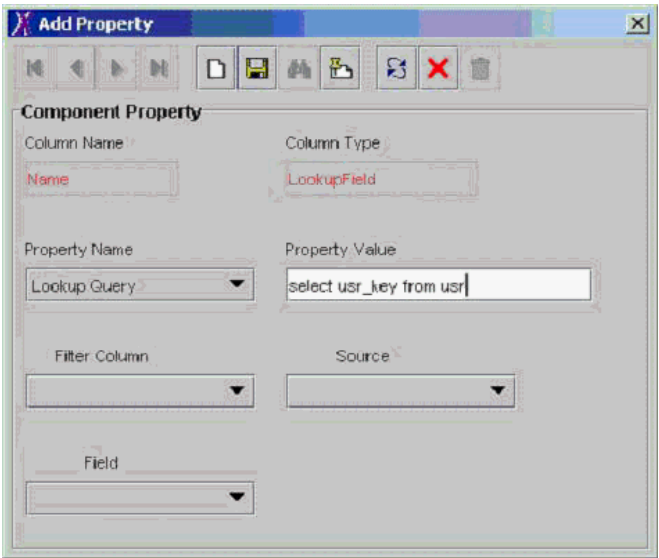
#### 8.4.2.4.2 Adding a Property and Property Value for Customized Look up Query

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

- Select the data field to which you want to add a property and a property value.
- Click **Add Property**.

The Add Property dialog box is displayed, as shown in [Figure 8–10](#).

Figure 8–10 Add Property Dialog Box



**Note:** The text that is displayed in the Column Name and Column Type fields shows 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 was selected (as indicated by **Name** displayed 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 menu), the WHERE clause is appended to the custom lookup query.

Table 8–4 describes the regions of the Add Property dialog box. Initially, all the fields are grayed out. After you have defined the lookup query and clicked **Save**, the fields become active.

Table 8–4 Fields of the Add Property Dialog Box for a Customized Look up Query

Name	Description
Column Name	The name of the data field.
Column Type	The data type of the data field.
Property Name	From this list, select the property for the data field.
Property Value	<p>In this field, enter the property value, which is associated with the property that is displayed in the <b>Property Name</b> box.</p> <p>In the case of a lookup query, you must specify both the Oracle Identity Manager form and field, which will be referenced for the query and will be recognized by the database.</p> <p>For example, if Oracle Identity Manager is referring to the user's login, then you enter <b>select usr_key fromusr</b> in the <b>Property Value</b> field. After clicking <b>Save</b>, the <b>Filter Column</b> is active with all the columns of tables.</p>

**Table 8–4 (Cont.) Fields of the Add Property Dialog Box for a Customized Look up**

Name	Description
<b>Filter Column</b>	<p>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 <b>Property Value</b> field. If multiple tables are used in the query, then all tables are shown.</p> <p>For example, <code>usr.USR_LOGIN</code> signifies that Oracle Identity Manager will see the <b>User Login</b> field from the Users form for the lookup query.</p>
<b>Source</b>	<p>After the <b>Filter Column</b> variable is selected, the <b>Source</b> 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 an Object form or a Process form. The <b>Source</b> field is a user-friendly name for the value that is displayed in the <b>Filter Column</b> box.</p> <p>For example, <b>Requester Information</b> refers to the <code>usr.USR</code> portion of the <b>Filter Column</b> value.</p>
<b>Field</b>	<p>This field is populated based on what value is selected in the <b>Source</b> field. Use this field to create the SELECT statement, which is needed for the column name.</p> <p>For example, the User Login corresponds to the <code>_LOGIN</code> part in the <b>Filter Column</b> value.</p>

---

**Note:** The menu items displayed in the **Property Name** box show the data type of the selected data field.

The **Source** and **Field** boxes of the Add Property dialog box are applicable only when **Lookup Query** is displayed in **Property Name**.

---

- Set the parameters for the property and the property value that you are adding to the data field. [Figure 8–11](#) shows the Edit Property dialog box.

**Figure 8–11 Edit Property Dialog Box**

The screenshot shows the 'Edit Property' dialog box. It contains the following fields and values:

- Column Name:** Name
- Column Type:** LookupField
- Property Name:** Lookup Query
- Property Value:** Y = \$Requester Information.User Login\$
- Filter Column:** usr.USR\_LOGIN
- Source:** Requester Information
- Field:** User Login

#### 8.4.2.4.3 Removing a Property and Property Value From a Data Field

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

1. Select the property and the property value that you want to remove.
2. Click **Delete Property**.

The property and its associated value are removed from the data field.

#### 8.4.2.5 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 by 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 not selected, 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 not selected, the user group cannot delete information from this record.

Figure 8–12 shows the Administrators tab of the Form Designer Form.

**Figure 8–12 Administrators Tab of the Form Designer Form**

The screenshot shows the 'Form Designer' window with the 'Administrators' tab selected. The window is divided into several sections:

- Table Information:** Includes fields for 'Table Name' (UD\_SOLARIS), 'Description' (Access to Solaris for Engineering), 'Form Type' (Process), and 'Object Name' (Solaris).
- Version Information:** Shows 'Latest Version' and 'Active Version' as 'Initial Version'.
- Operations:** Includes a 'Current Version' dropdown set to 'Initial Version' and buttons for 'Create New Version' and 'Make Version Active'.
- Administrators Tab:** A table with columns for 'Group Name', 'Allow Insert', 'Allow Update', and 'Allow Delete'. It lists five user groups: SYSTEM ADMINISTRATORS, Web Client Group, Sales Engineer Group, Project L7 Admin Group, and ALL USERS. All groups have checkboxes checked for all three permissions.

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.

##### 8.4.2.5.1 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 is displayed.
2. Select the user group, and assign it to the record of the user-created form.
3. Click **OK**.

The user group is displayed in the **Administrators** tab.

4. If you want this user group to be able to create and modify information for the current record of the user-created form, double-click the corresponding **Write** check box. Otherwise, go 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, go to Step 6.
6. Click **Save**.

The user group now has administrative privileges for this record of the user-created form.

#### 8.4.2.5.2 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. Select 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.

#### 8.4.2.6 Usage Tab

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

Figure 8–13 shows the **Usage** tab of the Form Designer Form.

**Figure 8–13 Usage Tab of the Form Designer Form**

The screenshot displays the 'Form Designer' application window with the 'Usage' tab selected. The 'Table Information' section shows 'Table Name' as 'UD\_SOLARIS' and 'Description' as 'Access to Solaris for Engineering'. The 'Form Type' is set to 'Process'. The 'Object Name' is 'Solaris'. The 'Version Information' section shows 'Latest Version' and 'Active Version' both as 'Initial Version'. The 'Operations' section shows 'Current Version' as 'Initial Version' with a dropdown arrow, and buttons for 'Create New Version' and 'Make Version Active'. Below these sections are tabs for 'Administrators', 'Usage', 'Pre-Populate', 'Default Columns', 'User Defined Fields', 'Additional Columns', 'Child Table(s)', 'Object Permissions', and 'Properties'. At the bottom, a table lists assigned objects:

	Resource Object	Process
1	Solaris	Solaris

The bottom of the window shows 'Form Designer' and 'Form Designer Table' tabs.

For example, the **Solaris** form (represented by the **UD\_SOLARIS** name in the **Table Name** field) was 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. For this example, because 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.

---

#### 8.4.2.7 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 prepopulate adapter to their correct locations.

---

**See Also:** See *Oracle Identity Manager Tools Reference* for more information about prepopulate adapters, attaching pre-populate adapters to fields of user-created forms, or mapping the variables of a pre-populate adapter

---

#### 8.4.2.8 Default Columns Tab

A form that is created by using the Form Designer form is composed of two types of data fields:

- Data fields that are created by a user (by 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 starting SQL\*Plus, or a similar database application.

#### 8.4.2.9 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 is displayed on this tab and is able to accept and supply data.

---

**See Also:** See ["User Defined Field Definition Form"](#) on page 7-7 for instructions about how to create fields for user-created forms

---

### 8.4.3 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 might want to create a different version of the form. This way, you can modify this version, without changing the original version of the form.

To create an additional version of a form:

1. Open the Form Designer form.
2. Search 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 is displayed, select the version of the form of which you are creating an additional version.

4. Click the **Create New Version** button.

The Create a New Version window is displayed.

5. In the **Label** field, enter the name of the additional version of the form.
6. From the Create a New Version window's toolbar, click **Save**.
7. 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, is displayed. By selecting this version, you can populate the tabs of the Form Designer form with information, without changing the original version of the form.

## 8.5 Error Message Definition Form

The Error Message Definition form, as shown in [Figure 8-14](#), is in the Development Tools folder. It is used to:

- Create the error messages that are displayed in dialog boxes when certain problems occur.
- Define the error messages that users can access when they create error handler tasks by using the Adapter Factory form.

The error messages you create are displayed on the Administrative and User Console if they are added to an adapter definition while creating a new adapter by using an error handler logic task based on a failure condition.

---

**Note:** If an entity adapter is attached to a process form or an object form for validation of field values, then these adapters will run if you edit data in these forms after completing direct or request provisioning.

For more information about creating error handler tasks, see *Oracle Identity Manager Tools Reference*.

---

**Figure 8–14 Error Message Definition Form**

The screenshot shows a web-based form for defining error messages. It includes input fields for a unique key, a descriptive code, a description, a remedy, a help URL, an action code, and a severity level. A 'Reset Count' button is also present. A note at the bottom explains the validation logic for the error message.

Table 8–5 describes the data fields of the Error Message Definition form.

**Table 8–5 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 zero. This counter is the number of times the error message is displayed.
Description	A description of the error message.
Remedy	A description of how to correct the condition that caused the error message to be displayed.
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 be displayed.  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 that results in the error message being displayed, even further.  An error message has five sub-levels of severity: None (N), Low (L), Medium (M), High (H), and Crash (C).
Note	Explanatory information about the error message.

### 8.5.1 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 occurs that causes the error message to be displayed, the text in the **Description** field is displayed in a dialog box.

---

**Note:** After you create an error message definition, to reset the count of how many times the error message is displayed, click the **Reset Count** button. This resets the count to zero.

---



To create an error message:

1. Open the Error Messaging Definition form.
2. In the **Code** field, enter the code that represents the error message definition.
3. In the **Description** field, enter a description for the error message.
4. In the **Remedy** field, you can enter a description for how to correct the condition that causes the error message to be displayed.
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 is displayed, you can select a code that represents the seriousness of the condition that causes the error message to be displayed. 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, the operation rolls back to the previous operation.
  - Reject (R). Oracle Identity Manager stores the rejection message, but it does not prevent subsequent operations from being executed.
  - Fatal Reject (F). Oracle Identity Manager stores the rejection message, and it stops any subsequent operations from being triggered. However, it stores all operations that were executed up to the fatal rejection.
7. (Optional) Double-click the **Severity Lookup** field. From the Lookup dialog box that is displayed, you can select a code (None (N), Low (L), Medium (M), High (H), or Crash (C)). This code presents a detailed classification of the code that is displayed 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.

After creating error messages by using the Error Message Definition form, you must add new error codes and advice messages in the Oracle Identity Manager `customResources.properties` resource bundle file. These localized error codes and advice messages will be shown in the Administrative and User Console.

**See Also:** The "Naming Convention for Defining Error Codes" section in the *Oracle Identity Manager Globalization Guide* for information about localizing error messages



---

## Business Rule Definition

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

- [Overview of Business Rule Definition](#)
- [Event Handler Manager Form](#)
- [Data Object Manager Form](#)
- [Reconciliation Rules Form](#)

### 9.1 Overview of Business Rule Definition

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 lets you create and manage the event handlers that are used with Oracle Identity Manager.
- **Data Object Manager:** This form lets you define a data object, assign event handlers and adapters to it, and map any adapter variables associated with it.

### 9.2 Event Handler Manager Form

This form is displayed 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.

By using 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 9–1 shows the Event Handler Manager form.

**Figure 9–1 Event Handler Manager Form**

Table 9–1 describes the fields of the Event Handler Manager form.

**Table 9–1 Fields of the Event Handler Manager Form**

Field Name	Descriptions
Event Handler Name	The name of the event handler.
Package	The Java package to which the event handler belongs.
Pre-Insert	If you select this check box, then Oracle Identity Manager will trigger the event handler before information is added to the database.
Pre-Update	If you select this check box, then Oracle Identity Manager will trigger the event handler before information is modified in the database.
Pre-Delete	If you select this check box, then Oracle Identity Manager will trigger the event handler before information is removed from the database.
Post-Insert	If you select this check box, then Oracle Identity Manager will trigger the event handler after information is added to the database.
Post-Update	If you select this check box, then Oracle Identity Manager can trigger the event handler after information is modified in the database.

**Table 9–1 (Cont.) Fields of the Event Handler Manager Form**

Field Name	Descriptions
Post-Delete	If you select this check box, then Oracle Identity Manager will trigger the event handler after 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 by using the Data Object Manager form. For more information about assigning event handlers to data objects, see ["Data Object Manager Form"](#) on page 9-3.

---



---

**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 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 modify an event handler, double-click the **Event Handler Name lookup** field.  
From the Lookup dialog box that is displayed, 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 the check boxes that correspond to when you want Oracle Identity Manager to trigger the event handler.

You can schedule an event handler to run on preinsert, preupdate, predelete, postinsert, postupdate, and postdelete.

**Note:** Selecting a check box does not mean that the event handler is triggered at that time, for example, on preinsert. 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.

## 9.3 Data Object Manager Form

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

- 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.

**See Also:** *Oracle Identity Manager Tools Reference* for more information about adapter variables, rule generator adapters, and entity adapters

Figure 9–2 shows the Data Object Manager form.

**Figure 9–2 Data Object Manager Form**

Data Object Information		
Form Description	Solaris	
Data Object	Thor CarrierBaseToUD_SOLARIS	

Pre-Insert Insert Permissions		
Assign	Event Handler Name	Pre-Insert Seq
	1 adpCONVERTTOLOWERCASE	1
	2 adpSOLARISHMDSTRINGGEN	2
	3 adpSETSOLARISASSET	3
	4 adpSETPASSWORDFROMMAIN	4

Pre-Update Update Permissions		
Assign	Event Handler Name	Pre-Update Seq

Pre-Delete Delete Permissions		
Assign	Event Handler Name	Pre-Delete Seq

Table 9–2 describes the fields of the Data Object Manager form.

**Table 9–2 Fields of the Data Object Manager Form**

Fields	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 is displayed, 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.

After you select a form, the name of the corresponding data object is displayed 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.

## 9.3.1 Tabs of the Data Object Manager Form

After you start 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.

### 9.3.1.1 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 following:

- 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 must no longer 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

#### 9.3.1.1.1 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-Insert** tab.

2. From the selected tab, click **Assign**.

The Assignment dialog box is displayed.

3. Select the event handler or adapter, and assign it to the data object.
4. Click **OK**.

The event handler or adapter is assigned to the data object.

#### 9.3.1.1.2 Organizing the Execution Schedule of Event Handlers or Adapters

To organize the execution schedule:

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

The Assignment dialog box is displayed.

3. Select 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 selected event handler or adapter will switch places and sequence numbers with the event handler or adapter that follows it.

5. Repeat Steps 3 and 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 correct order for the execution schedule or schedules that you organized.

#### 9.3.1.1.3 Removing an Event Handler or Adapter from a Data Object

To remove an event handler or adapter:

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

The event handler or adapter is removed.

#### 9.3.1.2 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 is displayed 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 any one of the following 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 not been mapped correctly.
- 
- 

For more information about compiling adapters and mapping its variables, see *Oracle Identity Manager Tools Reference*.

---

---

**Note:** If no adapters are assigned to a data object, then the Map Adapters tab is grayed out.

---

---

## 9.4 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 tries 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 by 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 by using the Rule Designer form except that the rules created by using the Reconciliation Rules form are specific to the resource object (because they relate to a single target resource) and only affect reconciliation-related functions.

### 9.4.1 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** check box is selected. If this check box is not selected, then 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 select this check box after Oracle Identity Manager has selected the **Valid** system check box. The **Valid** check box can 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. Go to 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.

## 9.4.2 Adding a Rule Element

To define individual elements in a reconciliation rule:

1. Go to the Rule definition to which you want to add elements.
2. Click **Add Rule Element** on the **Rule Elements** tab.  
The Add Rule Element dialog box is displayed.
3. Click the **Rule Element** tab.
4. Select a user-related data item from the **User Data** menu.

This will be the user data element that Oracle Identity Manager examines when evaluating the rule element. The menu will display all fields on the Oracle Users form (including any user-defined fields you 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.

**Note:**

- If you configure trusted source reconciliation of users, then you must ensure that the `User ID` field of the Oracle Identity Manager User account is used in the reconciliation matching rule.
- If you configure trusted source reconciliation of organizations, then you must ensure that the `Organization Name` field of the Oracle Identity Manager User account is used in the reconciliation matching rule.

- **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 perform the transformation correctly.

The possible transformations are described in [Table 9–3](#).

**Table 9–3 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. Select the **Case-Sensitive** check box.

For the rule element to be met, if this check box is selected, the value selected in the **Attribute** field must match the capitalization of the value being evaluated in

the reconciliation event record. If this check box is deselected, 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 not be selected.

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** check box is selected.

---

---

### 9.4.3 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 way 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. Go to 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 is displayed.  
Locate and select the desired rule.
4. Click **OK**.  
The selected reconciliation rule is added to rule.
5. Repeat steps 2 through 4 for each rule you want to nest in the rule.

### 9.4.4 Deleting a Rule Element or Rule

To delete a rule element or a rule:

1. Go to the rule from which you want to delete an element.
2. Select the rule element or rule to be deleted on the **Rule Elements** tab.
3. Click **Delete**.

---

## Oracle Identity Manager Logging Functions

This chapter describes the Oracle Identity Manager logging functions. It contains the following topics:

- [Overview of Oracle Identity Manager Logging Functions](#)
- [Setting Log Levels](#)

### 10.1 Overview of Oracle Identity Manager Logging Functions

Oracle Identity Manager comes preinstalled with the ability to create log files related to the activities performed in the application. You can customize the level of information gathered in these log files, the location of these log files, and the frequency of archiving the information by using configuration files. Oracle Identity Manager also provides log files that contain standard error and standard out messages.

You can use the log files created by Oracle Identity Manager to track activities being performed in the various modules (for example, the adapter factory and the 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 response.

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. If they are, then 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 the `log.properties` file, which is located in the `OIM_DC_HOME/xlclient/config/` directory.

### 10.2 Setting Log Levels

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

Oracle Identity Manager components are listed in the `OIM_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

*OIM\_DC\_HOME*/xlclient/config/log.properties logging properties file as follows:

1. Open the *OIM\_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 are part of Oracle Identity Manager.

By default, Oracle Identity Manager is configured to produce the 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, displayed 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 the Design Console to DEBUG:

```
log4j.logger.XELLERATE=WARN
log4j.logger.XELLERATE.ACCOUNTMANAGEMENT=INFO
log4j.logger.XELLERATE.JAVACLIENT=DEBUG
```

4. Save your changes.

5. Restart the Design Console so that the changes take effect.





In the previous release, this appendix listed and described:

- 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

From the current release onward, you will find this information in "Rule Elements, Variables, Data Types, and System Properties" in *Oracle Identity Manager Reference*.



---

## Service Account Management

Service accounts are general administrator accounts that are used for maintenance purpose. They are typically shared by a set of users. Service accounts are requested, provisioned, and managed in the same manner as regular accounts. A service account is distinguished from a regular account by an internal flag.

In the previous release, this appendix discussed managing service accounts. From the current release onward, you will find this information in "Service Accounts" in *Oracle Identity Manager Reference*.



---

## Form Version Control Utility

---

This appendix describes the scope, content, and description of the Form Version Control (FVC) utility. It contains the following topics:

- [FVC Utility Scope](#)
- [FVC Utility Content](#)
- [FVC Utility Description](#)
- [FVC Utility Features](#)

### C.1 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.

### C.2 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
<i>OIM_DC_HOME\xlclient\lib\xlFvcUtil.jar</i>	This JAR file contains the Form Version Control utility classes required to run it.

File Name with Path	Description
<i>OIM_DC_HOME</i> \xlclient\xlFvcUtil.ear	This EAR file contains the Form Version Control utility classes required to run it. This EAR file is packaged to run with IBM WebSphere Application Server launchClient utility.
<i>OIM_DC_HOME</i> \xlclient\fvc.properties	This file contains all the configuration properties regarding the source and target form versions, the fields on them, their values, and child form information.
<i>OIM_DC_HOME</i> \xlclient\fvcutil.cmd <i>OIM_DC_HOME</i> \xlclient\fvcutil_webSphere.cmd	These scripts are used to run the Form Version Control Utility on Microsoft Windows systems. When you run this script, you must provide the Oracle Identity Manager administrator user name and password as shown in the following command:  <i>OIM_DC_HOME</i> \xlclient\fvcutil.cmd xelsysadm password  <i>OIM_DC_HOME</i> \xlclient\fvcutil_webSphere.cmd xelsysadm password

### C.3 FVC Utility Description

The Form Version Control utility is designed to update the version number field of the custom process forms and data in the additional process form fields. The utility is started from the command console, and operates by using command-line parameters to login and a properties file. The properties in the parameters and validity of user's login and password are verified and appropriate error messages are produced to signify an error when one occurs.

### C.4 FVC Utility Features

The following list summarizes the FVC utility:

- Per system requirements, the 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 must be updated, but the 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 an error, but it will update field values for the version specified without 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. Therefore, if the following entries exist in the *fvc.properties* file, it will create three different rows in the child table, instead of creating and inserting a single child record with the specified values for the three fields:  
 Child;UD\_CF3\_FIELD7;tiger;Insert  
 Child;UD\_CF3\_FIELD8;mad;Insert  
 Child;UD\_CF3\_FIELD9;me2;Insert
- 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

## A

---

action field, 8-22  
Adapter Factory form, 8-1, 8-2  
Adapter Manager form, 8-1  
Administrative Queues form, 4-6  
application server, 1-3  
assigning and event handler or adapter, 5-21  
Assignment windows, 3-4

## C

---

client, 1-3  
Close, 2-3  
Code, 8-22  
column header, 2-8  
column name, 7-11  
combo box, 3-3  
complex password, 7-20  
comprehensive reporting for audit-trail  
    accounting, 1-2  
connection pooling, 1-3  
constructing a search query, 3-5  
context-sensitive help, 7-3  
create, 6-8  
    process definition, 6-8  
custom policy, 7-21

## D

---

data field, 3-1  
Data Object Manager, 8-1, 9-1  
data type, 7-10  
database, 1-3  
date, 3-2  
Default Value, 7-11  
defining IT resources, 5-2  
Delete check box, 5-5  
Description field, 8-22  
Design Console Explorer, 7-4

## E

---

Edit menu, 2-3  
Email Definition form, 6-1  
E-Mail Notification, 6-28  
    assign, 6-28

Encrypted field, 7-11  
end-user administrator, 4-2  
end-users, 4-3  
Error Message Definition, 8-1  
Error Message Definition form, 8-1  
Event Handler Manager Form, 9-1  
Event Handler Manager form, 8-1  
event handlers, 5-21  
executing a search, 3-6  
extensive user management, 1-1

## F

---

Field Size field, 7-10  
Field Type field, 7-11  
File menu, 2-2  
First, 2-3  
Form Designer form, 8-1  
Form Information form, 7-1  
Form view, 2-7  
FVC Utility content, C-1  
FVC Utility description, C-2  
FVC Utility scope, C-1

## G

---

General tab, 6-17  
Group Entitlements form, 4-4

## H

---

Help menu, 2-3  
Help URL, 8-22

## I

---

Integration, 6-21  
IT Resources form, 5-1  
IT Resources Type Definition Form, 5-1

## K

---

Key field, 8-22

## L

---

Label field, 7-10

Last, 2-3  
Lookup Definition form, 7-1  
lookup fields, 3-2  
Lookup shortcut, 2-5

## M

---

metadata, 1-3  
modifying process tasks, 6-17  
multiple trusted source reconciliation, 5-30

## N

---

Note field, 8-22  
Notes window, 3-3  
Notification tab, 6-28

## O

---

optimizing query performance, 3-6  
Oracle Identity Manager Explorer, 2-5  
Oracle Identity Manager menu bar, 2-2  
Oracle Identity Manager shortcuts, 2-4  
Oracle Identity Manager workspace, 2-6  
Organizational Defaults form, 4-1

## P

---

Password Policies Form, 7-18  
password policy, 7-18  
Policy History form, 4-2  
Policy History tab, 4-3  
Process Definition form, 6-6  
process engine, 1-1

## Q

---

query results set, 3-6  
querying capabilities, 3-5

## R

---

Reconciliation Manager form, 4-6  
Remedy field, 8-22  
Remote Manager form, 7-2  
removing an e-mail notification, 6-29  
Reset Count field, 8-22  
Resource Objects form, 5-1  
result set exceeds limit, 3-7  
row heading, 2-8  
Rule Designer form, 5-1

## S

---

scalable architecture, 1-1  
scheduled tasks  
    creating, 7-31  
    deleting, 7-32  
    predefined, 7-28  
Sequence field, 7-11  
Severity field, 8-22

System Configuration form, 7-1

## T

---

Table View, 2-7  
Task Dependency tab, 6-23  
Task Scheduler form, 7-2  
The Adapter Manager Form, 8-2  
The Form Designer Form, 8-2  
Time, 3-2  
toolbar menu, 2-3

## U

---

UDDI, 1-2  
User Defined Columns tab, 7-9  
User Defined Field Definition, 7-1  
User Defined Field Definition form, 7-7

## W

---

Web-based user self-service, 1-1  
wildcard, 3-5  
Workflow Definition Renderer, 6-9