

Oracle® Identity Manager

Reference

Release 9.1.0.1

E14066-01

February 2009

Oracle Identity Manager Reference, Release 9.1.0.1

E14066-01

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

Primary Author: Debapriya Datta

Contributing Author: Lyju Vadassery

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

Preface	v
Audience	v
Documentation Accessibility	v
Related Documents	vi
Documentation Updates	vi
Conventions	vi
Organization of This Guide	vi
1 The Administrative and User Console	
1.1 Components of the Administrative and User Console	1-1
1.2 Settings for Configuring Administrative and User Console Functions.....	1-7
1.2.1 Settings for Configuring User Registration Operations.....	1-7
1.2.2 Settings for Configuring Access Privileges.....	1-8
1.2.3 Settings for Configuring Account Creation Operations	1-8
1.2.4 Settings for Configuring Profile Editing Operations for Users.....	1-9
1.2.5 Settings for Configuring Account Modification Operations.....	1-9
2 Oracle Identity Manager Customization	
2.1 Forms Accessible from the Design Console	2-1
2.1.1 Forms in the User Management Folder	2-2
2.1.2 Forms in the Resource Management Folder	2-3
2.1.3 Forms in the Process Management Folder	2-3
2.1.4 Forms in the Design Console Administration Folder	2-3
2.1.5 Forms in the Development Tools Folder	2-4
2.1.6 Forms in the Business Rule Definition Folder	2-4
2.2 Rule Elements, Variables, Data Types, and System Properties.....	2-4
2.3 Service Accounts	2-24
2.4 Design Console Actions	2-25
2.5 Adapter Mapping Information	2-26
2.5.1 Adapter Task Mapping Information.....	2-26
2.5.1.1 Adapter Variables.....	2-27
2.5.1.2 Adapter Task	2-27
2.5.1.3 Literal	2-27
2.5.1.4 Adapter References	2-27
2.5.1.5 Organization Definition.....	2-28

2.5.1.6	Process Definition.....	2-28
2.5.1.7	User Definition.....	2-28
2.5.2	Adapter Variable Mapping Information.....	2-29
2.5.2.1	From the Variable List Tab.....	2-30
2.5.2.2	Process Task Adapter Variable Mappings.....	2-31
2.5.2.3	Task Assignment Adapter Variable Mappings.....	2-33
2.5.2.4	Rule Generator and Entity Adapter Variable Mappings.....	2-35
2.5.2.5	Prepopulate Adapter Variable Mappings.....	2-36

3 Oracle Identity Manager Connectors

Glossary

Index

Preface

This guide provides information that can be applied when performing Oracle Identity Manager administrative and configuration tasks. This guide discusses the functionality offered by the Oracle Identity Manager interfaces. It also provides information about the settings and configurations for customizing Oracle Identity Manager.

Audience

This guide is intended for users who want administration and configuration information when working with Oracle Identity Manager.

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.

TTY Access to Oracle Support Services

To reach AT&T Customer Assistants, dial 711 or 1.800.855.2880. An AT&T Customer Assistant will relay information between the customer and Oracle Support Services at 1.800.223.1711. Complete instructions for using the AT&T relay services are available at <http://www.consumer.att.com/relay/tty/standard2.html>. After the AT&T Customer Assistant contacts Oracle Support Services, an Oracle Support

Services engineer will handle technical issues and provide customer support according to the Oracle service request process.

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 release documentation set, visit Oracle Technology Network at

<http://www.oracle.com/technology/documentation>

Conventions

The following text conventions are used in this document:

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

Organization of This Guide

This guide consists of the following chapters:

- Chapter 1: Administrative and User Console
This chapter discusses the menu items in the Oracle Identity Manager Administrative and User Console that you can use to perform various administrative tasks in Oracle Identity Manager. It also describes the settings in the Administrative and User Console for configuring functions such as user registration and account creation.
- Chapter 2: Oracle Identity Manager Customization
This chapter provides information about customizing Oracle Identity Manager that is enabled by the Design Console. It lists the various forms accessible from the Design Console. It also discusses system properties, data types, service accounts, and the Form Version Control Utility that you can use to customize Oracle Identity Manager.
- Chapter 3: Oracle Identity Manager Connectors
This chapter lists the Oracle Identity Manager connectors and the corresponding target systems and target system platforms for each connector.
- Glossary
This defines the frequently-used terms in Oracle Identity Manager.

The Administrative and User Console

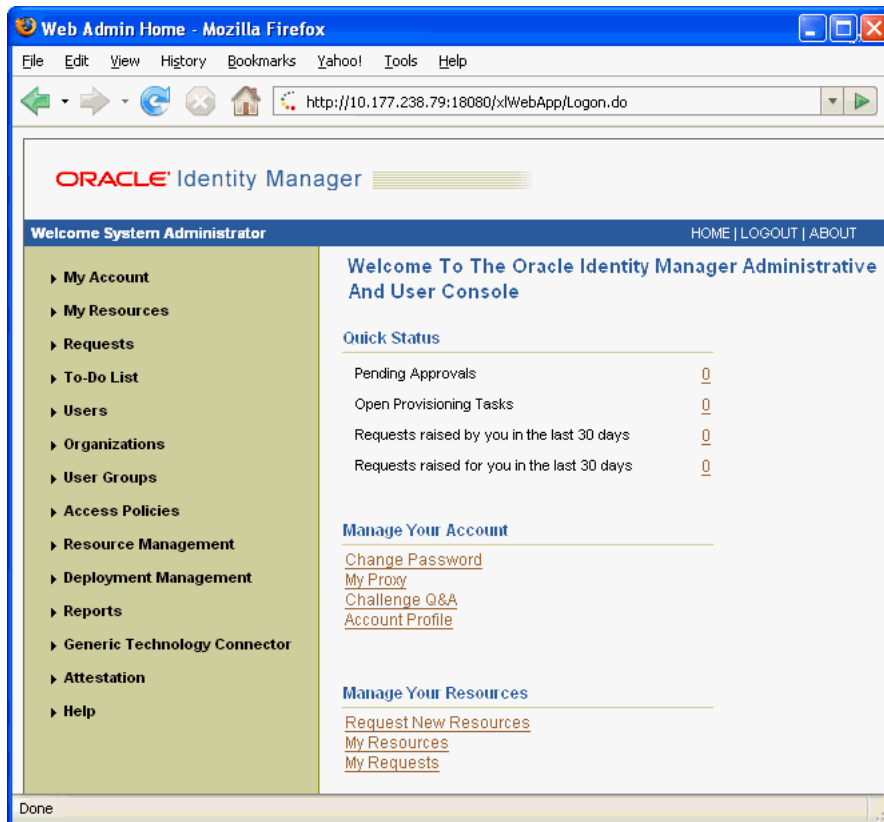
Oracle Identity Manager client tier consists of two interfaces, the Administrative and User Console and the Design Console. Using the Administrative and User Console, you can create requests for resources and approve the provisioning of resources of the users that you manage. Users can search for, edit, and delete account information in the Oracle Identity Manager database by using the Administrative and User Console.

This chapter contains the following topics:

- [Components of the Administrative and User Console](#) on page 1-1
- [Settings for Configuring Administrative and User Console Functions](#) on page 1-7

1.1 Components of the Administrative and User Console

The left navigation pane of the Administrative and User Console lists the menu items that enable you to perform various administrative tasks, such as managing Oracle Identity Manager accounts and managing resources. The menu items are grouped together according to functionality; for example, the menu items for creating and managing users are grouped under one head. [Figure 1-1](#) shows the Welcome screen of the Administrative and User Console.

Figure 1–1 The Welcome Screen of the Administrative and User Console

This section describes the functionalities offered by the Administrative and User Console that are grouped under the following top-level menu items:

- [My Account](#) on page 1-2
- [My Resources](#) on page 1-3
- [Requests](#) on page 1-3
- [To-Do List](#) on page 1-3
- [Users](#) on page 1-4
- [Organizations](#) on page 1-4
- [User Groups](#) on page 1-4
- [Access Policies](#) on page 1-4
- [Resource Management](#) on page 1-4
- [Deployment Management](#) on page 1-5
- [Reports](#) on page 1-5
- [Generic Technology Connector](#) on page 1-6
- [Attestation](#) on page 1-6

My Account

In the My Account section, you can access and manage your Oracle Identity Manager account by using the following menu items:

- **Account profile:** View and edit your account.

- **Change Password:** Change your password.
- **Challenge Q&A:** Change challenge questions and answers.
- **My Proxy:** Designate a proxy user.

My Resources

In the My Resources section, you can view resources that have been provisioned to you and request access to resources for yourself and others by using the following menu items:

- **My Resources:** View the resources that have been provisioned to you.
- **My Requests:** View all resource requests that are raised for you or are raised by you.
- **Request New Resources:** Make a new request for resources.

Requests

In the Requests section, you can create and track requests for resources that you have requested for users and organizations by using the following menu items:

- **Resources:** Create and manage requests for provisioning resources to yourself, other users, and organizations. Using the Resources menu item, you can make the following types of requests:
 - **Grant Resource:** Grant resources to targets.
 - **Disable Resource:** Temporarily prevent targets from accessing a resource.
 - **Reenable Resource:** Activate targets who have been temporarily suspended from using resources.
 - **Revoke Resource:** Remove resources from targets.
- **Track:** View requests for resources based on the privileges that have been assigned to you in Oracle Identity Manager. Additionally, you can edit details or approve tasks within those requests.

To-Do List

A To-Do list is a list of tasks within a process. The processes for approving requests and their associated resources and making them available for provisioning consist of tasks, which can be performed by using the following menu items:

- **Pending Approvals:** View and complete the tasks that are assigned to you and view requests that are assigned to users that you manage. You can also view all the tasks based on your indirect group membership.
- **Open Tasks:** The Open Tasks menu item lists tasks that are defined for a provisioning process. The Open Tasks menu item displays all open provisioning tasks that are assigned to you or a person that you manage. You can also view a list of provisioning tasks assigned to you based on your indirect group membership. Use the Open Tasks menu item to retry a task if it has the `Rejected` status, reassign a provisioning task to another user, or specify a response for a provisioning task.
- **Attestation:** Attestation is a mechanism by which reviewers are periodically notified of a report they must review. This report outlines the provisioned resources that certain users have. The reviewer can attest to the accuracy of the entitlements with an appropriate response. You can display all open attestation

tasks that are assigned to you, and certify, reject, decline, or delegate attestation tasks.

Users

In the Users section, you can create and manage user records, for example, Oracle Identity Manager accounts, that your employees require. You can create and manage user records by using the following menu items:

- **Create:** Create a user account.
- **Manage:** Enable, disable, provision resources to, and unlock user accounts. A user account must be disabled to be eligible for enabling. Only locked accounts can be unlocked. An account becomes locked if a user has exceeded the maximum number of login retry attempts or maximum number of password reset attempts. You can manage a user account by editing a user's Oracle Identity Manager record.

Organizations

In the Organizations section, you can create and manage information pertaining to your organization by using the following menu items:

- **Create:** Create an organization.
- **Manage:** Manage an organization by:
 - Searching for and Viewing Organizations.
 - Enabling an Organization.
 - Disabling an Organization.
 - Deleting an Organization.

User Groups

You use user groups to create and manage records of collections of users to whom you can assign some common functionality, such as access rights, roles, or permissions. You can modify the permissions associated with these user groups, and you can create additional user groups by using the following menu items:

- **Create:** Create a user group.
- **Manage:** Find user groups, add information to them, and perform other administrative functions for user groups.

Access Policies

In the Access Policies section, you can create and use access policies for users and resources in Oracle Identity Manager. You define an access policy for provisioning resources to user groups and users. You can create and use access policies by using the following menu items:

- **Create:** Create an access policy by using the Create Access Policy wizard.
- **Manage:** Manage access policies by modifying information in existing access policies.

Resource Management

The Resource Management feature lets you manage resource objects for an organization or an individual user by using the menu items:

- **Manage:** Manage resources, which includes the ability to:
 - Search for a resource and view its details.

- Disable, enable, or revoke a resource from users or organizations.
- Manage Resource Administrator and Authorizer groups.
- View and define work flows.
- View and define resource audit objectives.
- **Create IT Resource:** Create IT resources and set access permissions to user groups on the IT resource.
- **Manage IT Resource:** View, modify, and delete IT resources.
- **Create Scheduled Task:** Create scheduled tasks by specifying the schedule and adding scheduled task attributes.
- **Manage Scheduled Task:** View and modify scheduled tasks.

Deployment Management

The Deployment Manager is a tool used for exporting and importing Oracle Identity Manager configurations. The Deployment Manager enables you to export the objects that constitutes your Oracle Identity Manager configuration. You use the Deployment Manager to exchange Oracle Identity Manager items between environments. Usually, you use the Deployment Manager to migrate a configuration from one deployment to another, for example, from a test to a production deployment, or to create a backup of your system. The Deployment Management section provides the following menu items:

- **Export:** You can export objects from your Oracle Identity Manager system and save them in an XML file. The Deployment Manager has an Export Wizard that enables you to build up your export file.
- **Import:** You can import objects that were saved in an XML file into your Oracle Identity Manager system by using the Deployment Manager. You can import all or part of the XML file, and you can import multiple XML files at once.
- **Install Connector:** You can install predefined connectors, and automate copying connector files to the specified installation directory, importing the connector XML files, and compiling adapters.

Reports

Based on whether you access current operational data or historical data, the reports you can generate by using Oracle Identity Manager are divided into Operational Reports and Historical Reports. These reports describe the resources available to users.

Operational Reports

Operational reports can be used by administrators and auditors for operational and compliance purposes. Operational reports are of the following types:

- **Resource Access List:** Queries all existing users provisioned to a resource
- **Policy List:** Displays a list of policies for a specified group
- **Policy Detail:** Displays complete details about specified policies
- **Oracle Identity Manager Password Expiration:** Lists user password expiration settings
- **User Resource Access:** Queries access rights for users that match specified query parameters

- **Entitlements Summary:** Lists the number of users for each status within each resource
- **Attestation Requests by Process:** Lists attestation requests by process
- **Attestation Request Detail:** Returns complete details of a specified attestation request
- **Resource Password Expiration:** Returns a list of users whose resource passwords are about to expire
- **Group Membership:** Lists the number of users in each group
- **Attestation Process List:** Lists all defined attestation processes
- **Attestation Requests by Reviewer:** Lists attestation requests by reviewer
- **Group Membership Profile:** Lists user group memberships

Historical Reports

Administrators and auditors can use historical reports for compliance and forensic auditing purposes. Historical reports are of the following types:

- **User Membership History:** Displays a history of a user's group memberships
- **User Resource Access History:** Lists a user's resource access history over the life cycle of the account
- **Group Membership History:** Displays a history of a group's memberships
- **User Profile History:** Lists a user's profile history over the life cycle of the account
- **Resource Access List History:** Queries all users provisioned to a resource over its life cycle

See Also: The "Oracle Identity Manager Reporting" chapter in *Audit Report Developer's Guide* for the entire list of operational and historical reports

Generic Technology Connector

Using this menu item, you can create and manage generic technology connectors.

Attestation

In this section, you can create, manage, and view attestation tasks by using the following menu items:

- **Create:** Create a new attestation process.
- **Manage:** Manage attestation processes by:
 - Editing an attestation process
 - Disabling an attestation process
 - Enabling an attestation process
 - Deleting an attestation process
 - Running an attestation process
 - Managing attestation process administrators
 - Viewing attestation process execution history

- **Dashboard:** View the state of any attestation processes that are owned by any group of which you are a member. To use the Attestation Dashboard, expand the Attestation link and click Attestation Dashboard. The Attestation Dashboard page is displayed with a table listing the state of any attestation processes that are owned by any group of which you are a member.

1.2 Settings for Configuring Administrative and User Console Functions

This section describes the settings in the Administrative and User Console for configuring functions such as user registration and account creation. Review this section prior to deploying the Oracle Identity Manager Administrative and User Console to ensure that you have configured the product to function as intended.

This section discusses the following topics:

- [Settings for Configuring User Registration Operations](#) on page 1-7
- [Settings for Configuring Access Privileges](#) on page 1-8
- [Settings for Configuring Account Creation Operations](#) on page 1-8
- [Settings for Configuring Profile Editing Operations for Users](#) on page 1-9
- [Settings for Configuring Account Modification Operations](#) on page 1-9

To customize the Oracle Identity Manager Administrative and User Console user interface, see *Oracle Identity Manager Administrative and User Console Customization Guide*.

1.2.1 Settings for Configuring User Registration Operations

Table 1–1 describes the settings for user registration operations.

Table 1–1 User Registration Operation Settings

Function	Description
To allow users to self-register in Oracle Identity Manager	Set the Is Self-Registration Allowed property in the System Configuration form to true . The System Configuration form is available in the Oracle Identity Manager Design Console.
To require users to select their verification questions and provide answers to these question when registering	Set the Does user have to provide challenge information during registration property in the System Configuration form to true . The System Configuration form is available in the Oracle Identity Manager Design Console.
To designate the number of verification questions that the user must answer	Set the Number of Questions property in the System Configuration form to the number of questions that you want users to answer. Ensure that the number of questions you supply in the Lookup.WebClient.Questions lookup definition is equal to or greater than the value of the Number of Questions property. You might need to create additional questions. The System Configuration form is available in the Oracle Identity Manager Design Console.

Table 1–1 (Cont.) User Registration Operation Settings

Function	Description
To designate the list of questions that users select from when setting their verification questions and answers	Define a row on the Lookup.WebClient.Questions lookup definition for each question in the Lookup Definition form. The Lookup Definition form is available in the Oracle Identity Manager Design Console.
To require an approval for self-registration	Define an approval task in the User Registration approval process.
To configure different workflow approvals for self-registration depending on user profile information	Define additional approval processes for the Request resource definition and create a rule of type process determination with a rule element that at least requires that the request object action is Create Entity . Associate the new rule with the approval process on the Request resource definition to enable Oracle Identity Manager to determine which process to select.
To automatically add a user to groups based on self-registration	Define rules of type general and attach them to the user group definitions to which you want users to be added on registration. This enables Oracle Identity Manager to determine which groups to add users to based on the criteria they enter on registration. The criteria in the rules must match the user-entered criteria.

1.2.2 Settings for Configuring Access Privileges

Table 1–2 describes the settings for configuring access privileges.

Table 1–2 Access Privileges Settings

Function	Description
To designate the pages to which all users are to be allowed access	Specify these pages on the Menu Items tab of the All Users user group.
To designate the pages to which various administrative groups are to be allowed access	Specify these pages on the Menu Items tab of the applicable administrative user groups, for example, System Administrator, AdminGroup1, and so on.

1.2.3 Settings for Configuring Account Creation Operations

Table 1–3 describes the settings for configuring account creation operations for administrators.

Table 1–3 Account Creation Operation Settings

Function	Description
To allow administrators to create an Oracle Identity Manager account for other users	Ensure that the groups that these administrators belong to are added to the Administrators tab of the organizations that contain the users they are to administer.
To configure fields for administrators to supply data when creating the user account	Create these fields in the <code>FormMetaData.xml</code> file. See the <i>Oracle Identity Manager Administrative and User Console Customization Guide</i> for details.

Table 1–3 (Cont.) Account Creation Operation Settings

Function	Description
To specify fields that are required when creating a user account	Modify these fields in the <code>FormMetaData.xml</code> file and set the optional property to <code>false</code> . See the <i>Oracle Identity Manager Administrative and User Console Customization Guide</i> for details.
To specify the groups of which a user is automatically made a member	Define rules of type general and attach them to the user group definitions to which you want users automatically added upon registration. This enables Oracle Identity Manager to determine which groups to add users to based on the criteria entered when their account was created. The criteria in the rules must match the entered criteria.
To designate the groups to which administrators can add users whom they administer	Ensure that the groups of which these administrators are members are added to the Administrators tab of the group definitions to which you wish to allow them to add users.

1.2.4 Settings for Configuring Profile Editing Operations for Users

[Table 1–4](#) describes the settings for configuring profile editing operations for users.

Table 1–4 Profile Editing Operation Settings

Function	Description
To specify that an approval is required for self-initiated Oracle Identity Manager profile updates	Define an approval task in the User Profile Edit approval process
To configure different workflow approvals for self-initiated profile updates	Define additional approval processes for the Request resource definition and create a rule of type process determination with a rule element that at least requires the request object action to be Modify Entity . Associate the rule with the approval process on the Request resource definition to enable Oracle Identity Manager to determine which process to select.
To control which fields users can edit in their own profiles	Configure the fields in the <code>FormMetaData.xml</code> file. See the <i>Oracle Identity Manager Administrative and User Console Customization Guide</i> for details.

1.2.5 Settings for Configuring Account Modification Operations

[Table 1–5](#) describes the settings for configuring account modification operations for administrators.

Table 1–5 Account Modification Operation Settings

Function	Description
To control which users can edit the profiles of other users	You must designate the forms to which members of the various administrative groups are to have access. You must also add these groups to the Administrators tab of the Organizations that contain the users they are to administer.

Table 1–5 (Cont.) Account Modification Operation Settings

Function	Description
To control which Oracle Identity Manager system fields (for example user ID, first name, and so on) administrators can edit	You must designate which fields you want to allow administrators to edit for other users. The fields you want to make editable must be specified in the <code>FormMetaData.xml</code> file. See the <i>Oracle Identity Manager Administrative and User Console Customization Guide</i> for details.
To control which user-defined fields (for example Social Security number, local identity, and so on) administrators can edit.	You must designate which fields you want to allow administrators to edit for other users. Depending on the pages in the Administrative and User Console on which these fields are displayed, you might need to edit the <code>FormMetaData.xml</code> file to add attribute definitions and references for these fields. See the <i>Oracle Identity Manager Administrative and User Console Customization Guide</i> for details.

Oracle Identity Manager Customization

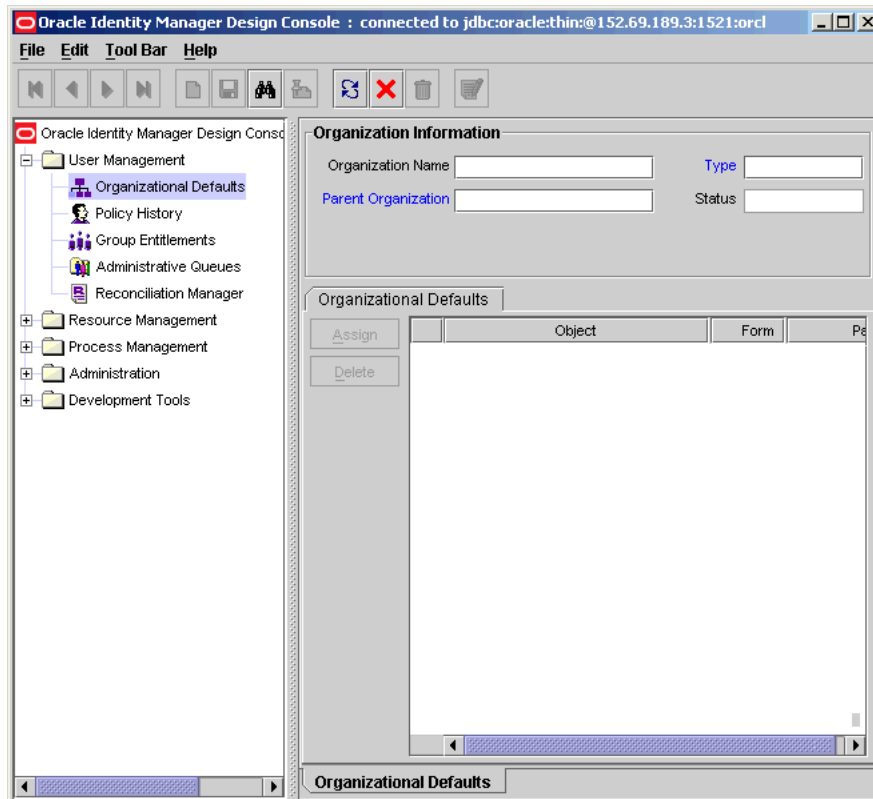
Oracle Identity Manager customization is enabled by the Design Console that lets you deal with configuration and design functions, such as designing forms and workflows and creating and managing adapters. Using the Design Console, you can grant user privileges to work on particular areas of the application configuration.

This chapter discusses the following topics:

- [Forms Accessible from the Design Console](#) on page 2-1
- [Rule Elements, Variables, Data Types, and System Properties](#) on page 2-4
- [Service Accounts](#) on page 2-24
- [Design Console Actions](#) on page 2-25
- [Adapter Mapping Information](#) on page 2-26

2.1 Forms Accessible from the Design Console

The left side of the Design Console main screen is the Design Console Explorer. The Explorer consists of a list of icons that represent forms that you have permissions to access. These icons are grouped under folders based on functionality and are displayed to the users according to the access rights that you assign to them. [Figure 2-1](#) shows the Explorer in the Design Console main screen.

Figure 2–1 The Design Console Main Screen

The following topics are discussed in this section:

- [Forms in the User Management Folder](#) on page 2-2
- [Forms in the Resource Management Folder](#) on page 2-3
- [Forms in the Process Management Folder](#) on page 2-3
- [Forms in the Design Console Administration Folder](#) on page 2-3
- [Forms in the Development Tools Folder](#) on page 2-4
- [Forms in the Business Rule Definition Folder](#) on page 2-4

2.1.1 Forms in the User Management Folder

The User Management folder provides tools to create and manage information about 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 specify the default values that the organization users should have for certain resources.
- **Policy History:** Use this form to view resources that are allowed and disallowed for users through policies.
- **Group Entitlements:** Use this form to specify which Design Console forms are available for which user groups.
- **Administrative Queues:** Use this form to define queues or list of groups, which can be used to define as administrators for the requests.

- Reconciliation Manager: Use this form to manage reconciliation events in Oracle Identity Manager.

2.1.2 Forms in the Resource Management Folder

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

- IT Resources Type Definition: Use this form to create resource types that 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, auto-group membership, provisioning process selection, task assignment, and prepopulating adapters.
- Resource Objects: Use this form to create and manage resource objects. These objects represent resources that you want to make available to users and organizations.

2.1.3 Forms in the Process Management Folder

The Process Management folder provides you 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.

2.1.4 Forms in the Design Console Administration Folder

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

- Form Information: Use this form to specify the class name, form label, form type, menu item, and graphic icon 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: 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: Use this form to create and manage user-defined fields. A user-defined field enables you to store additional information, such as user, request, and resource information.
- System Configuration: Use this form to define and set the value of properties that control the behavior of the Client and/or Server. You can specify the users and user groups that a property value applies to, or you can specify that the value applies to all users.
- Remote Manager: 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:** 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:** Use this form to create tasks and set up the schedules that determine when these tasks are to be run.

2.1.5 Forms in the Development Tools Folder

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 any IT Resource by connecting to that resource's API. This code is known as an adapter.
- **Adapter Manager:** You use this form to compile multiple adapters simultaneously.
- **Form Designer:** You use this form to create process and resource object forms that do not come packaged with Oracle Identity Manager.
- **Error Message Definition:** You use this form to create error messages that can be used for reporting 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.
- **Reconciliation Rules:** You use this form to create and manage reconciliation rules in Oracle Identity Manager.

2.1.6 Forms in the Business Rule Definition Folder

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:** You use this form to create and manage the event handlers that are used with Oracle Identity Manager.
- **Data Object Manager:** Through this form, you can define a data object, assign event handlers and adapters to it, and map any adapter variables associated with it.

2.2 Rule Elements, Variables, Data Types, and System Properties

The Design Console lets you perform Oracle Identity Manager customization tasks such as adding and modifying rule elements for a rule, creating or editing e-mail definitions, creating forms, and setting system properties. For these customization tasks, you must set parameters, variables, and data types. This section describes these parameters, variables, and data types.

In the Rule Elements tab of the Rule Designer form, you can create and manage elements and nested rules for a rule. [Table 2-1](#) lists the rule elements that can be used to create Oracle Identity Manager rules, by using the Rule Designer form.

Table 2-1 Rule Elements to Create Oracle Identity Manager Rules

Type	Sub-Type	Attribute Source	Variable
General	NA	User Profile Data	Email

Table 2–1 (Cont.) Rule Elements to Create Oracle Identity Manager Rules

Type	Sub-Type	Attribute Source	Variable
General	NA	User Profile Data	End Date
			First Name
			Identity
			Last Name
			Manager Full Name
			Manager Login
			Middle Name
			Organization Name
			Role
			Start Date
			Status
			User Group Name
			User Login
			Oracle Identity Manager Type
			Any fields that are displayed in the User Defined Fields region of the User Profile tab of the Users form.
Process Determination	Organization Provisioning	Requester Information	Email
			End Date
			First Name
			Identity
			Last Name
			Location Name
			Manager Full Name
			Manager Login
			Middle Name
			Organization Name
			Role
			Start Date
			State
			Status
			User Group Name
User Login			
Oracle Identity Manager Type			

Table 2–1 (Cont.) Rule Elements to Create Oracle Identity Manager Rules

Type	Sub-Type	Attribute Source	Variable
Process Determination	Organization Provisioning	Object Information	Any fields that are displayed in the User Defined Fields region of the User Profile tab of the Users form.
			Object Type
		Request Target Information	Organization Customer Type
			Organization Name
			Organization Status
			Parent Organization
			Any fields that are displayed in the User Defined Fields tab of the Organizations form.
		Object Data Information	Any fields that are displayed in the Additional Columns tab of the Form Designer form for the custom form associated with the resource object.
		Process Data Information	Any fields that are displayed in the Additional Columns tab of the Form Designer form for the custom form associated with the process.
	User Provisioning	Requester Information	Email
		Request Target Information	End Date
			First Name
			Identity
			Last Name
			Manager Full Name
			Manager Login
			Middle Name
			Organization Name
			Role
			Start Date
			Status
			User Group Name
			User Login

Table 2–1 (Cont.) Rule Elements to Create Oracle Identity Manager Rules

Type	Sub-Type	Attribute Source	Variable
			Oracle Identity Manager Type
		Request Details	Any field defined on the FormMetadata.xml user self-registration and user profile modification section with property useInRule set to true
Process Determination	User Provisioning	Requester Information; Request Target Information	Any fields that are displayed in the User Defined Fields region of the User Profile tab of the Users form.
		Object Information	Object Name Object Type
		Object Data Information	Any fields that are displayed in the Additional Columns tab of the Form Designer form for the custom form associated with the resource object.
		Process Data Information	Any fields that are displayed in the Additional Columns tab of the Form Designer form for the custom form associated with the process.
	Approval; Standard Approval		Email End Date First Name Identity Last Name Manager Full Name Manager Login Middle Name Organization Name Role Start Date Status User Group Name User Login Oracle Identity Manager Type

Table 2–1 (Cont.) Rule Elements to Create Oracle Identity Manager Rules

Type	Sub-Type	Attribute Source	Variable
			Any fields that are displayed in the User Defined Fields region of the User Profile tab of the Users form.
		RequestInformation	Request Creation Date Request ID Request Object Action Request Priority Requestor
Process Determination	Approval	Object Information	Object Name Object Type
		Object Data Information	Any field that is displayed in the Additional Columns tab of the Form Designer form for the custom form associated with the resource object
		Process Data Information	Any field that is displayed in the Additional Columns tab of the Form Designer form for the custom form associated with the process
Task Assignment	Organization Provisioning; User Provisioning	Task Information	Allow Cancellation while Pending Allow Multiple Instances Assign Task to Manager Disable Manual Insert Task Conditional Task Data Label Task Default Assignee Task Name Task Required for Completion Task Sequence
		Process Information	Object Name Process Name Process Type
		Object Information	Object Name Object Type
		Requester Information	Email End Date

Table 2–1 (Cont.) Rule Elements to Create Oracle Identity Manager Rules

Type	Sub-Type	Attribute Source	Variable
			First Name
			Identity
Task Assignment	Organization Provisioning; User Provisioning	Requester Information	Last Name
			Manager Full Name
			Manager Login
			Middle Name
			Organization Name
			Role
			Start Date
			State
			Status
			User Group Name
			User Login
			Oracle Identity Manager Type
			Any field that is displayed in the User Defined Fields region of the User Profile tab of the Users form
		Object Data Information	Any field that is displayed in the Additional Columns tab of the Form Designer form for the custom form associated with the resource object
		Process Data Information	Any field that is displayed in the Additional Columns tab of the Form Designer form for the custom form associated with the process
Pre-Populate	Organization Provisioning; User Provisioning	Requester Information	Email
			End Date
			First Name
			Identity
			Last Name
			Manager Full Name
			Manager Login
			Middle Name
			Organization Name

Table 2–1 (Cont.) Rule Elements to Create Oracle Identity Manager Rules

Type	Sub-Type	Attribute Source	Variable
Pre-Populate	Organization Provisioning; User Provisioning	Requester Information	Role
			Start Date
			Status
			User Group Name
			User Login
		Request Information	Email
			Any field that is displayed in the User Defined Fields region of the User Profile tab of the Users form
			Request Creation Date
		Object Information	Request ID
			Request Object Action
Request Priority			
Requestor			
Object Name			
Object Data Information	Object Type		
	Any field that is displayed in the Additional Columns tab of the Form Designer form for the custom form associated with the resource object		
Process Data Information	Any field that is displayed in the Additional Columns tab of the Form Designer form for the custom form associated with the process		
Organization Provisioning	Request Target Information	Organization Customer Type	
		Organization Name	
		Organization Status	
		Parent Organization	
		Any field that is displayed in the User Defined Fields tab of the Organizations form	
User Provisioning	Request Target Information	Email	
		End Date	
		First Name	

Table 2–1 (Cont.) Rule Elements to Create Oracle Identity Manager Rules

Type	Sub-Type	Attribute Source	Variable
			Identity
			Last Name
			Manager Full Name
			Manager Login
Pre-Populate	User Provisioning	Request Target Information	Middle Name
			Organization Name
			Role
			Start Date
			Status
			User Group Name
			User Login
			Oracle Identity Manager Type
			Any field that is displayed in the User Defined Fields region of the User Profile tab of the Users form

You can use the Email Definition form to create templates for e-mail notifications to be sent to the users. [Table 2–2](#) lists the variables that can be used to create e-mail templates by using the Email Definition form.

Table 2–2 Variables to Create Templates

Type	Target	Location Type	Contact Type	Variable
Provisioning Related	User Profile Information; Assignee Profile Information	NA	NA	First Name
				Identity
				Last Name
				Manager Login
				Middle Name
				Role
				Status
				End Date
				User Group Name
				User Login
				User Manager
				Start Date

Table 2–2 (Cont.) Variables to Create Templates

Type	Target	Location Type	Contact Type	Variable
				Oracle Identity Manager Type
				Manager Full Name
				Organization Name
				Email
Provisioning Related	User Profile Information; Assignee Profile Information	NA	NA	Any field that is displayed in the User Defined Fields region of the User Profile tab of the Users form
	Object Information	NA	NA	Object Name
				Object Target Type
				Object Type
	Process Information	NA	NA	Object Name
				Process Name
				Process Type
	Object Data Information	NA	NA	Any field that is displayed in the Additional Columns tab of the Form Designer form for the custom form associated with the resource object
	Process Data Information	NA	NA	Any field that is displayed in the Additional Columns tab of the Form Designer form for the custom form associated with the process
Request Related	Requester Information	NA	NA	First Name
				Identity
				Email Address
				Manager Login
				Middle Name
				Role
				Status
				User End Date
				User Group Name
				User Login

Table 2–2 (Cont.) Variables to Create Templates

Type	Target	Location Type	Contact Type	Variable
				User Manager
				User Start Date
				Oracle Identity Manager Type
				Any field that is displayed in the User Defined Fields region of the User Profile tab of the Users form
Request Related	Request Information	NA	NA	List of objects being requested
				List of targets being provisioned
				Request Creation Date
				Request ID
				Request Name
				Request Object Action
				Request Priority
				Requestor
				List of user Targets
General	User Profile Information	NA	NA	First Name
				Identity
				Last Name
				Email Address
				Manager Login
				Middle Name
				Role
				Status
				User End Date
				User Group Name
				User Login
				User Manager
				User Start Date
				Oracle Identity Manager Type

Table 2–2 (Cont.) Variables to Create Templates

Type	Target	Location Type	Contact Type	Variable
				Any field that is displayed in the User Defined Fields region of the User Profile tab of the Users form

Table 2–3 describes the properties that can be associated with different data types used to create Oracle Identity Manager forms, by using the Form Designer form.

Table 2–3 Properties Associated with Data Types for Creating Oracle Identity Manager Forms

Data Type	Data Property	Description
Text Field	Required	If this text field must be populated for the form to be saved, then enter "true" into the corresponding Property Value field. Otherwise, type "false" into this field. Note: The default value for this data property is false.
	Is Visible	If you want this text field to be displayed when Oracle Identity Manager generates the form, then enter "true" into the corresponding Property Value field. Otherwise, type "false" into this field. Note: The default value for this data property is true.
Lookup Field	Auto Complete	By entering "true" in the corresponding Property Value field, Oracle Identity Manager filters the lookup field. A user can then add characters to the lookup field before double-clicking it. By doing so, only those Lookup values which match these characters are displayed in the Lookup window. As an example, for a State lookup field, a user can enter "new" into the field. Then, once the user double-clicks the lookup field, only those states that begins with the letters "new" (for example, New Hampshire, New Jersey, New Mexico, and New York) are displayed in the Lookup window. If you do not want Oracle Identity Manager to filter the lookup field, then enter "false" into the associated Property Value field. The default property value for the Auto Complete property is false.
	Column Captions	In the corresponding Property Value field, enter the name of the column heading that is displayed in the Lookup window when a user double-clicks the lookup field. If the Lookup window has multiple columns, then enter each column heading into the Property Value field, separating them with commas, for example, Organization Name, Organization Status .
	Column Names	In the corresponding Property Value field, enter the name of the database column that represents the column caption that you want to be displayed in the Lookup window. If the Lookup window has multiple columns, then enter each database column into the Property Value field, separating them with commas.
Lookup Field	Column Widths	In the corresponding Property Value field, enter the width of the column that is displayed in the Lookup window. If the Lookup window has multiple columns, then enter each column width into the Property Value field, separating them with commas, for example, 20,20 .
	Lookup Column Name	In the corresponding Property Value field, enter the name of the Lookup column as it is displayed in the database, which must be saved to the database.

Table 2–3 (Cont.) Properties Associated with Data Types for Creating Oracle Identity Manager Forms

Data Type	Data Property	Description
	Lookup Query	<p>In the corresponding Property Value field, enter the name of the SQL query that runs when a user double-clicks the lookup field. As a result, the appropriate Lookup columns are displayed in the Lookup window.</p> <p>To correctly display the data returned from a query, you must add a <code>lookupfield.header</code> property to the <code>xlWebAdmin_locale.properties</code> file. For example, consider the following SQL query: <code>select usr_status from usr</code>. To view the data returned from the query, you must add the following entry to the <code>xlWebAdmin_locale.properties</code> files:</p> <pre>lookupfield.header.users.status=User Status</pre> <p>If the <code>xlWebAdmin_locale.properties</code> file does not contain a <code>lookupfield.header</code> property for your specified query, then the Administrative and User Console displays a lookup window after you click the corresponding lookup icon.</p> <p>The syntax for a <code>lookupfield.header</code> property is as follows:</p> <pre>lookupfield.header.column_code=display value</pre> <p>The <code>column_code</code> portion of the entry must be lowercase and any space must be replaced by the underscore character (<code>_</code>).</p> <p>By default, the following entries for lookup field column headers are already available in the system resource bundle:</p> <pre>lookupfield.header.lookup_definition.lookup_code_information .code_key=Value lookupfield.header.lookup_definition.lookup_code_information .decode=Description lookupfield.header.users.manager_login=User ID lookupfield.header.organizations.organization_name=Name lookupfield.header.it_resources.key=Key lookupfield.header.it_resources.name=Instance Name lookupfield.header.users.user_id=User ID lookupfield.header.users.last_name=Last Name lookupfield.header.users.first_name=First Name lookupfield.header.groups.group_name=Group Name lookupfield.header.objects.name=Resource Name lookupfield.header.access_policies.name=Access Policy Name</pre>
Lookup Field	Lookup Code	<p>In the corresponding Property Value field, enter the lookup definition code. This code contains all information pertaining to the lookup field, including lookup values and the text that are displayed with the lookup field once a lookup value is selected.</p> <p>Important: The Lookup Code data property can be used in lieu of the Column Captions, Column Names, Column Widths, Lookup Column Name, and Lookup Query properties. In addition, the information contained in the Lookup Code property supersedes any values set in these five data properties.</p> <p>Tip: An easy way to enter a lookup code is by starting the Lookup Definition form, querying for the desired code, copying this code to the Clipboard, and pasting it into the Lookup Code field.</p> <p>Note: The classification type of the lookup definition code must be of Lookup Type (the Lookup Type radio button on the Lookup Definition form must be selected).</p>
	Required	<p>If this Lookup field must be populated for the form to be saved, then enter "true" into the corresponding Property Value field. Otherwise, type "false" into this field.</p> <p>Note: The default value for this data property is false.</p>

Table 2–3 (Cont.) Properties Associated with Data Types for Creating Oracle Identity Manager Forms

Data Type	Data Property	Description
	Visible Field	<p>If you want this lookup field to be displayed when Oracle Identity Manager generates the form, then enter "true" into the corresponding Property Value field. Otherwise, type "false" into this field.</p> <p>Note: The default value for this data property is true.</p>
Text Area	Number of Rows	<p>In the corresponding Property Value field, enter the row length of the text area. So, if you want the text area to be five rows in length, then type "5" into the Property Value field.</p>
	Required	<p>If this text area must be populated for the form to be saved, then enter "true" into the corresponding Property Value field. Otherwise, type "false" into this field.</p> <p>Note: The default value for this data property is false.</p>
	Visible Field	<p>If you want this text area to be displayed when Oracle Identity Manager generates the form, then enter "true" into the corresponding Property Value field. Otherwise, type "false" in this field.</p> <p>Note: The default value for this data property is true.</p>
IT Resource Lookup Field	Type	<p>If you select this data property, then a box is displayed in the Property Value field. From this box, select the type of Server for the IT Resource.</p> <p>Important: This property is required.</p>
	Required	<p>If this lookup field must be populated for the form to be saved, then enter "true" into the corresponding Property Value field. Otherwise, type "false" in this field.</p> <p>Note: The default value for this data property is false.</p>
	Visible Field	<p>If you want this lookup field to be displayed when Oracle Identity Manager generates the form, then enter "true" into the corresponding Property Value field. Otherwise, type "false" into this field.</p> <p>Note: The default value for this data property is true.</p>
Date Field (Display Only)	Visible Field	<p>If you want this text field to be displayed when Oracle Identity Manager generates the form, then enter "true" into the corresponding Property Value field. Otherwise, type "false" into this field.</p> <p>Note: The default value for this data property is true.</p>
Date and Time Window	Required	<p>If this text field must be populated for the form to be saved, enter "true" into the corresponding Property Value field. Otherwise, type "false" into this field.</p> <p>Note: To populate this text field, double-click it, and select a date and time from the Date & Time window that is displayed.</p> <p>Note: The default value for this data property is false.</p>
	Visible Field	<p>If you want this text field to be displayed when Oracle Identity Manager generates the form, then enter "true" into the corresponding Property Value field. Otherwise, type "false" in this field.</p> <p>Note: The default value for this data property is true.</p>
Password Field	Required	<p>If this text field must be populated for the form to be saved, enter "true" into the corresponding Property Value field. Otherwise, type "false" in this field.</p> <p>Note: The default value for this data property is false.</p>
	Visible Field	<p>If you want this text field to be displayed when Oracle Identity Manager generates the form, then enter "true" into the corresponding Property Value field. Otherwise, type "false" in this field.</p> <p>Note: The default value for this data property is true.</p>

Table 2–3 (Cont.) Properties Associated with Data Types for Creating Oracle Identity Manager Forms

Data Type	Data Property	Description
Radio Button	Button Labels	<p>In the corresponding Property Value field, enter the label for the radio button. For multiple radio buttons, this label represents the heading for the group box, containing the radio buttons.</p> <p>When you are applying a label to multiple radio buttons, enter each label into the Property Value field, separating them with commas, for example Sun or Microsoft. When Oracle Identity Manager generates the form, then a group box encompasses these radio buttons, signifying that the buttons are associated with one another.</p>
	Button Values	<p>In the corresponding Property Value field, enter the value for the radio button. This value goes to the database when a user selects the radio button.</p> <p>For multiple radio buttons, enter each value into the Property Value field, separating them with commas (for example, on, off).</p>
Radio Button	Required	<p>If a radio button must be selected for the form to be saved, then enter "true" into the corresponding Property Value field. Otherwise, type "false" in this field.</p> <p>Note: The default value for this data property is false.</p>
	Visible Field	<p>If you want this radio button (or group of radio buttons) to be displayed when Oracle Identity Manager generates the form, then enter "true" into the corresponding Property Value field. Otherwise, type "false" in this field.</p> <p>Note: The default value for this data property is true.</p>
Check Box	Required	<p>If this check box must be selected for the form to be saved, then enter "true" into the corresponding Property Value field. Otherwise, type "false" in this field.</p> <p>Note: The default value for this data property is false.</p>
	Visible Field	<p>If you want this check box to be displayed when Oracle Identity Manager generates the form, then enter "true" into the corresponding Property Value field. Otherwise, type "false" in this field.</p> <p>Note: The default value for this data property is true.</p>
Combo Box	Lookup Code	<p>In the corresponding Property Value field, enter the Lookup definition code. This code contains all information pertaining to the box, including box items and the text that is displayed with the box once a lookup value is selected.</p> <p>Important: The Lookup Code data property can be used in lieu of the Column Captions, Column Names, Column Widths, Lookup Column Name, and Lookup Query properties. In addition, the information contained in the Lookup Code property supersedes any values set in these five data properties.</p> <p>Tip: An easy way to enter a lookup code is by starting the Lookup Definition form, querying for the desired code, copying this code to the Clipboard, and pasting it into the Lookup Code field.</p> <p>Note: The classification type of the lookup definition code must be of Lookup Type (the Lookup Type option on the Lookup Definition form must be selected).</p>
	Required	<p>If this item from this box field must be selected for the form to be saved, then enter "true" into the corresponding Property Value field. Otherwise, type "false" in this field.</p> <p>Note: The default value for this data property is false.</p>
	Visible Field	<p>If you want this box to be displayed when Oracle Identity Manager generates the form, then enter "true" into the corresponding Property Value field. Otherwise, type "false" in this field.</p> <p>Note: The default value for this data property is true.</p>

Table 2–3 (Cont.) Properties Associated with Data Types for Creating Oracle Identity Manager Forms

Data Type	Data Property	Description
Text Field (Display Only)	Visible Field	If you want this text field to be displayed when Oracle Identity Manager generates the form, then enter "true" into the corresponding Property Value field. Otherwise, type "false" in this field. Note: The default value for this data property is true.

You can use the System Configuration form to define and set the value of properties that control the behavior of Oracle Identity Manager. [Table 2–4](#) lists and describes the system properties of Oracle Identity Manager:

Note: After you change a system property, you must clear the cache for the change to take effect. To clear the server cache, perform any one of the following steps:

- Enter the following command:

- For Microsoft Windows:

```
OIM_HOME\xellerate\bin\PurgeCache.bat category_name
```

- For UNIX:

```
OIM_HOME/xellerate/bin/PurgeCache.sh category_name
```

- Restart the application server.
-

Table 2–4 System Properties

Name	Description	Keyword	Value
Organization Process Inheritance	If a resource is added to an organization as permitted resource, then by setting this property to <code>TRUE</code> , the same resource is automatically added as the permitted resource for suborganizations.	XL.OrganizationProcessInherit	TRUE
Organization Process Restriction	Note: This property is for internal use by Oracle Identity Manager. You must not use this property.	XL.OrganizationProcessRestrict	FALSE
Base Help URL	Note: This property is for internal use by Oracle Identity Manager. You must not use this property.	XL.BaseHelpUrl	//docs/thortech.com/72/ /

Table 2–4 (Cont.) System Properties

Name	Description	Keyword	Value
Pending Cancelled Tasks	If this property is set to <code>TRUE</code> and tasks are configured to allow cancellation while they are pending, then these tasks are moved to Pending Cancelled (PX) status if the corresponding process instance is cancelled. If the property is set to <code>FALSE</code> , then tasks are moved to Cancelled (X) status when corresponding process instance is cancelled. Note that process instances are called by Oracle Identity Manager when the corresponding resource instances are revoked.	<code>XL.PendingCancelled</code>	<code>true</code>
Use Row Restriction	Note: This property is for internal use by Oracle Identity Manager. You must not use this property.	<code>XL.UseRowRestriction</code>	<code>FALSE</code>
Enable disabled resource instances when a user is enabled	If the value is <code>TRUE</code> , then the disabled resource instances are enabled when a user is enabled.	<code>XL.EnableDisabledResources</code>	<code>TRUE</code>
Proxy User Email Notification	The corresponding <code>PTY_VALUE</code> is the e-mail definition name that is sent when a proxy user is created. User gets a notification e-mail when the user is made proxy for some other user.	<code>XL.ProxyNotificationTemplate</code>	Notify Proxy User
Internal date format for reporting errors and reporting stored procedures	Date format used in stored procedure for reporting.	<code>Reports.InternalDateFormat</code>	<code>mm/dd/yyyy</code>
Property to indicate whether the auditing engine should send a JMS message	Note: This property is for internal use by Oracle Identity Manager. You must not use this property.	<code>XL.SendAuditJMSMessage</code>	<code>false</code>
Compiler Path for Connectors	Specifies the Java home depending on the application server. Note: If the path of the JDK directory is not included in the System Path variable, then you must set the path of the JDK directory in the <code>XL.CompilerPath</code> system property. If this is not done, then an error is encountered during the adapter compilation stage of the process performed when you import an XML file by using the Deployment Manager.	<code>XL.CompilerPath</code>	
Record Read Limit	Sets the maximum number of records that can be displayed in a query result set.	<code>XL.READ_LIMIT</code>	<code>500</code>

Table 2–4 (Cont.) System Properties

Name	Description	Keyword	Value
Number of Questions	Sets the number of questions that must be completed by a user who is using the Web Application to reset the user's password.	PCQ.NO_OF_QUES	3
Use of Default Questions	Determines whether a user is required to answer questions defined in the Web Application, or if the user is required to provide his or her own questions.	PCQ.USE_DEF_QUES	TRUE
Force to set questions at startup	When the user logs into the Web Application for the first time, he/she must set the default questions for resetting his/her password.	PCQ.FORCE_SET_QUES	TRUE
Default Date Format	When creating reconciliation events by calling the APIs and date format is not passed as one of the arguments to the API, Oracle Identity Manager assumes that all the date field values are specified in Default Date Format. If no value is set for this system property, Oracle Identity Manager assumes the format to be <code>yyyy/mm/dd hh:mm:ss z</code> .	XL.DefaultDateFormat	yyyy/mm/dd hh:mm:ss z
Shows tasks assigned to group users with highest priority or least load only	If the value is TRUE, then the tasks are assigned to group users with highest priority or least load only when the assignment types are <code>Group User With Highest Priority</code> , <code>Group User With Least Load</code> , and so on.	XL.ShowTaskAssignedToGroup	FALSE
Property to indicate the duration in months of open tasks and pending approvals	Note: Do not use this property. It is retained in this release for internal use only. It will be removed in a future release of Oracle Identity Manager.	XL.OpenTasksPendingApproval	3
Property for counter display flag for open tasks and pending approvals	<p>The following property entries are used to speed up the login process:</p> <ul style="list-style-type: none"> ■ Property Name: <code>XL.WebAdminHome.CounterDisplay.Type</code> ■ Property Value: <code>DayLimit</code> <p>If the above system property is set to <code>DayLimit</code>, then respective counter APIs will read the following system properties:</p> <ul style="list-style-type: none"> ■ <code>XL.RequestRaisedByYou.DayLimit=30</code> ■ <code>XL.RequestRaisedForYou.DayLimit=30</code> 	XL.WebAdminHome.CounterDisplay	DayLimit

Table 2–4 (Cont.) System Properties

Name	Description	Keyword	Value
User Id reuse property	Determines whether a deleted user account can be reused. To reuse a deleted user account, assign this property a value of <code>TRUE</code> and drop the unique index for the <code>USR_LOGIN</code> column in the <code>USR</code> table and create a nonunique index. To prevent a user account from being reused, assign this property a value of <code>FALSE</code> .	<code>XL.UserIDReuse</code>	<code>FALSE</code>
Organization Self-Serviceable	Determines whether the default value for a process is self-serviceable and if it is set or not. This is used to determine which resources can be self requested. This is same as selecting the option from the Design Console. The only difference is that from here it is allowed for a particular organization.	<code>ORG.SELF_SERVICEABLE_DEFAULT</code>	<code>FALSE</code>
Property to indicate day limit set for pending approvals	Used prior to implementation of the Separation of active/non-active task feature to specify the duration for which the pending approval tasks would be fetched. Used at the API level to get the Pending approval related counters.	<code>XL.PendingApproval.DayLimit</code>	<code>30</code>
Property dictates whether database name will be displayed	If the value is <code>TRUE</code> , then the database name is displayed.	<code>XL.TOOLBAR_DBNAME_DISPLAY</code>	<code>TRUE</code>
Direct Provisioning vs. Request for Access Policy Conflicts	If multiple access policies are evaluated to be true for a user that requires the same resource to be provisioned and some of the policies are defined to provision resource with approvals and some without approval, and if the Direct Provisioning vs. Request for Access Policy Conflicts property is set to <code>FALSE</code> , then Oracle Identity Manager creates a request for provisioning the corresponding resource. If there are no conflicts, then resources are provisioned based on what is defined on the access policy.	<code>XL.DirectProvision</code>	<code>FALSE</code>
Organization Delete/Disable Action	If this property is set to <code>TRUE</code> , then users can disable/delete the organization even if the organization contains users and suborganizations. If this property is <code>FALSE</code> , then users cannot disable/delete the organization if the organization contains users and suborganizations. The default value is <code>FALSE</code> .	<code>ORG.DisableDeleteActionEnabled</code>	<code>FALSE</code>

Table 2–4 (Cont.) System Properties

Name	Description	Keyword	Value
Property to indicate day limit set for open provisioning tasks	Used prior to implementation of the separation of active or nonactive task feature to specify the duration for which the pending approval tasks would be fetched. This is used at the API level to get the Pending approval-related counters.	XL.OpenTask.DayLimit	30
Email Server	Name of the e-mail server.	XL.MailServer	Email Server
User Language	The <code>user.language</code> value is configured during installation for Locale handling at server side.	user.language	en
User Region	The <code>user.region</code> value is configured during installation for Locale handling at server side.	user.region	US
User Variant	The <code>user.variant</code> value is configured during installation for Locale handling at server side.	user.variant	
Property to indicate day limit set for Request raised by you	Day limit value to fetch the requests raised by you in the past n number of days . Here, n is fetched from this property and is used to show counters for the same on the home page.	XL.RequestRaiseByYou.DayLimit	30
Property to indicate day limit set for Request raised for you	Day limit value to fetch the requests raised for you in the past n number of days. Here, n is fetched from this property and is used to show counters for the same on the home page.	XL.RequestRaiseForYou.DayLimit	30
Reassign Email Notification	Email Template name, which is sent when the task is re-assigned if no value found. The default value is <code>Notify Task Reassign</code> .	XL.ReassignNotificationTemplate	Notify Task Reassign
Force Password Change at First Login	If the value is <code>TRUE</code> , then the user is forced to change the password when the user logs in for the first time.	XL.ForcePasswordChangeAtFirstLogin	TRUE
Request complete status	Ensures that the request status is set to <code>Request Complete</code> after a object approval completes.	XL.RequestCompleteStatus	TRUE
Request Email	This property value contains an e-mail template name that is used for sending e-mail notifications when a request is Approved.	Request.Approval Email	
Assign Task to Requesters Manager	Assign Task to Requesters Manager when the assignment type is Request Target User's Manager.	XL.AssignTaskToRequestersManager	true
Number of Correct Answers	This value represents how many questions the user must answer correctly to reset user password.	PCQ.NO_OF_CORRECT_ANSWERS	3

Table 2–4 (Cont.) System Properties

Name	Description	Keyword	Value
Maximum Number of Login Attempts	This value represents how many consecutive times the user can attempt to login to Oracle Identity Manager unsuccessfully before Oracle Identity Manager locks the user account. Note: If the user account is locked, then the user can unlock it by resetting the "challenge" questions associated with resetting the password.	XL.MaxLoginAttempts	3
Maximum Number of Password Reset Attempts	This value represents how many consecutive times the user can attempt to reset the password unsuccessfully before Oracle Identity Manager locks the user account. Important: When the user account is locked, the user cannot unlock it. If this occurs, then contact the system administrator.	XL.MaxPasswordResetAttempts	3
Self Registration Email From Address	The e-mail address from which the user, who raised a self-registration request, receives an e-mail.	XL.SelfRegistrationEmailFromAddress	selfreg@xselfreg.com
Profile Edit Email From Address	The e-mail address from which the user, who created a profile edit request, receives an e-mail.	XL.ProfileEditEmailFromAddress	selfreg@xselfreg.com
Is Self-Registration Allowed	If the value is TRUE, then the users are allowed to self-register.	XL.SelfRegistrationAllowed	TRUE
Does user have to provide challenge information during registration	If the value is TRUE, then users will have to provide challenge information during registration.	PCQ.PROVIDE_DURING_SELFREG	TRUE
Resource Form Data + task information for resources	Depending upon the property value such as Resource Form, NULL, the data will be populated in UPA table.	XL.UserProfileAuditDataCollection	Resource Form
Defines if UPA should be in the secondary DS	If the value is set to True, then auditing occurs in separate db. By default, it is set to False.	XL.UserProfileAuditInSecondaryDS	False

Table 2–4 (Cont.) System Properties

Name	Description	Keyword	Value
Use semicolon as delimiter in API parameters	This property is used to specify whether or not semicolon should be used as a delimiter to the API input parameter values. Some APIs accepted string input values that are separated by semicolon. This has been changed to use a vertical bar " " instead. To keep backward compatibility, this new property can be used to go back to using semicolons. The default value is FALSE signifying the usage of " ". When set to TRUE, the input for those APIs are accepted with semicolon as separator.	XL.UseSemiColonAsDelimiter	FALSE
Enable exception reports	This property is used to enable the exception reporting feature. Exception reporting will be enabled only if the value is set to TRUE.	XL.EnableExceptionReports	FALSE

2.3 Service Accounts

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.

When a user is provisioned with a service account, Oracle Identity Manager manages a mapping from the user's identity to the service account. This user is considered the owner of the Service Account. When the user is deleted or the resource is revoked, the provisioning process for the service account does not get canceled, which would cause the undo tasks to fire. Instead, a task is inserted into the provisioning process in the same way Oracle Identity Manager handles Disable and Enable actions. This task removes the mapping from the user to the service account, and returns the service account to the pool of available accounts. This management capability is exposed through APIs.

[Table 2–5](#) describes the service account management tasks and their corresponding APIs.

Table 2–5 Service Account Management Tasks and Corresponding APIs

Tasks	Description	API Methods
Service Account Change	You can change an existing regular account to be a service account or change an existing service account to be a regular account. If any of these changes occur, then the Service Account Change task is inserted in the provisioning process, becoming active in the Tasks tab of the Process Definition. Any adapter that is associated with this provisioning process runs. If there is no adapter, then a predefined response code is attached.	<pre>tcUserOperations.changeFromServiceAccount tcUserOperations.changeToServiceAccount</pre>

Table 2–5 (Cont.) Service Account Management Tasks and Corresponding APIs

Tasks	Description	API Methods
Service Account Alert	When a user is deleted or disabled to whom a service account is linked, the Service Account Alert task is inserted into the provisioning process of that service account instance. You can use this task to start the appropriate actions in response to the event that occurred for the user.	NA
Service Account Moved	You can transfer ownership of a service account from one user to another. This translates into the provisioning instance showing up in the resource profile of the new owner, and no longer in the resource profile of the old user. The Service Account Moved task is inserted into the provisioning process of the resource instance after the account is moved. Any adapter associated with this provisioning process runs. If there is no adapter, then a predefined response code is attached.	<code>tcUserOperationsIntf.moveServiceAccount</code>

2.4 Design Console Actions

Table 2–6 lists the Oracle Identity Manager actions, and the conditions and results of these actions.

Table 2–6 Oracle Identity Manager Actions, Conditions, and Results

Action	Condition	Result
A user is deleted.	Oracle Identity Manager cancels all the existing tasks in process instance and inserts undo tasks for these tasks, if they are defined.	If so, then the condition for this task has been met (the user has been revoked), and Oracle Identity Manager inserts the task into the existing process. If the task has an adapter attached to it, then it will run.
A user is disabled.	Oracle Identity Manager checks each process for any tasks that display the Disable selection in the Task Effect combo box.	If so, then the condition for this task has been met (the user has been disabled), and Oracle Identity Manager inserts the task into the existing process. If the task has an adapter attached to it, then it will run.
A user is enabled.	Oracle Identity Manager checks each process for any tasks that display the Enable selection in the Task Effect combo box.	If so, then the condition for this task has been met (the user has been enabled), and Oracle Identity Manager inserts the task into the existing process. If the task has an adapter attached to it, then it will run.
A user's password has been modified on the Users form	Oracle Identity Manager checks each process to see if it has a Change User Password task.	If so, then the condition for this task has been met (the user's password has been modified), and Oracle Identity Manager inserts the task into all existing processes, which have that task defined. If the task has an adapter attached to it, then it will run.

Table 2–6 (Cont.) Oracle Identity Manager Actions, Conditions, and Results

Action	Condition	Result
The data fields of an application process form have been modified.	Oracle Identity Manager checks each process to see if it has a task that starts with the <i>field label Updated</i> naming convention (for example, HomeDirectory Updated).	The condition for this task is met (the process task begins with the <i>field label Updated</i> naming convention). Oracle Identity Manager inserts the task into all existing processes, which have that task defined. If the task has an adapter attached to it, then it will run.
A user's profile information has been moved to a different organization.	Oracle Identity Manager checks each process to see if it has a task that begins with the words Move User.	The condition for this task is met (the user's profile information has been moved to a different organization). Oracle Identity Manager inserts the task into the existing process. If the task has an adapter attached to it, then it will run.

2.5 Adapter Mapping Information

An adapter is a Java class, generated by the Adapter Factory, which enables Oracle Identity Manager to interact with an external JAR file, a target IT resource (for example, a resource asset), or a user-defined form. The Adapter Factory is a code-generation tool provided by Oracle Identity Manager, which enables a User Administrator to create Java classes.

An adapter extends the internal logic and functionality of Oracle Identity Manager. It automates process tasks, and defines the rules for the auto-generation and validation of data in fields within Oracle Identity Manager. There are five types of adapters: task assignment adapters, task adapters, rule generator adapters, pre-populate adapters, and entity adapters.

The following topics are discussed in this section:

- [Adapter Task Mapping Information](#) on page 2-26
- [Adapter Variable Mapping Information](#) on page 2-29

2.5.1 Adapter Task Mapping Information

An adapter task is one of the several possible components within an adapter. And this is a logical step within an adapter, equivalent to calling a programming language method. The following types of adapter tasks are available: Functional Tasks (Java Task, Remote Task, and Stored Procedure Task), Utility Tasks (Utility Task and Oracle Identity Manager API Task), and Logic Tasks (Set Variable Task and Error Handler Task).

This section lists the mappings that you can set for the parameters of an adapter task, in the following topics:

- [Adapter Variables](#) on page 2-27
- [Adapter Task](#) on page 2-27
- [Literal](#) on page 2-27
- [Adapter References](#) on page 2-27
- [Organization Definition](#) on page 2-28
- [Process Definition](#) on page 2-28

- [User Definition](#) on page 2-28

2.5.1.1 Adapter Variables

The following table lists and describes the items of the Map To list box of the Data Mapping for Variable window and the Name list box to which you can map the parameters of an adapter variable for an adapter task.

Map To Combo Box	Name Combo Box	Description
Adapter Variables	A list of adapter variables are displayed	<p>You can map the parameter to the adapter variables that you created for this adapter.</p> <p>Note: When the adapter variable's classification type is Object, it cannot be used with process task adapters.</p> <p>Note: If the adapter variable's classification type is IT Resource, then an Attribute combo box is displayed. From this combo box, select the attribute of the IT resource to which you wish to map the parameter.</p>

2.5.1.2 Adapter Task

The following table lists and describes the items of the Map To, Name, and Output combo boxes of the Adapter Factory form to which you can map the parameters of an adapter task.

Map To Combo Box	Name Combo Box	Output combo Box	Description
Adapter Task	A list of adapter tasks are displayed.	A list of output variables pertaining to the selected adapter task is displayed.	You can map the parameter to the adapter tasks that you created for this adapter.

2.5.1.3 Literal

The following table lists and describes the items of the Map To and Type combo boxes, as well as the Value field of the Adapter Factory form, to which you can map the parameters of a constant (or literal) for an adapter task.

Map To Combo Box	Type Combo Box	Value Field	Description
Literal	String, Boolean, Character, Byte, Date, Integer, Float, Long, Short, Double	Enter the value of the literal into this field.	You can map the parameter to a String, Boolean, Character, Byte, Date, Integer, Float, Long, Short, or Double data type, respectively.

2.5.1.4 Adapter References

The following table lists and describes the items of the Map To and Type combo boxes of the Adapter Factory form to which you can map the parameters of an adapter reference for an adapter task.

Map To Combo Box	Type Combo Box	Description
Adapter References	Event Handler Name or Database Reference	You can map the parameter to the active adapter.

2.5.1.5 Organization Definition

The following table lists and describes the items of the Map To and Field combo boxes of the Adapter Factory form to which you can map the parameters of an organization definition for an adapter task.

Map To combo box	Field Combo Box	Description
Organization Definition	Organization Name	You can map the parameter to the Organization Name field of the Organizations form.
	Organization Type	You can map the parameter to the Type field of the Organizations form.
	Organization ID	You can map the parameter to the Organization # field of the Organizations form.
	Organization Parent	You can map the parameter to the Parent Organization field of the Organizations form.
	Organization Status	You can map the parameter to the Status field of the Organizations form.
	Organization Parent ID	You can map the parameter to the parent_key field in the ACT database table.
	Any fields that are displayed in the User Defined Fields tab of the Organizations form.	You can map the parameter to the selected user-defined field.

2.5.1.6 Process Definition

The following table lists and describes the items of the Map To and Field combo boxes of the Adapter Factory form to which you can map the parameters of a process definition for an adapter task.

Map To Combo Box	Field Combo Box	Description
Process Definition	Name	You can map the parameter to the Name field of the Process Definition form.
	Type	You can map the parameter to the Type field of the Process Definition form.

2.5.1.7 User Definition

The following table lists and describes the items of the Map To and Field combo boxes of the Adapter Factory form to which you can map the parameters of a user definition for an adapter task.

Map To Combo Box	Field Combo Box	Description
User Definition	User Key	You can map the parameter to a key, representing a unique record of the Users form.
	First Name	You can map the parameter to the First Name field of the Users form.
	Middle Initial	You can map the parameter to the Middle Name field of the Users form.
	Last Name	You can map the parameter to the Last Name field of the Users form.
	User Login	You can map the parameter to the User ID field of the Users form.
	Password	You can map the parameter to the New Password and Confirm Password fields of the Users form.
	Type	You can map the parameter to the Xellerate Type field of the Users form.
	User Status	You can map the parameter to the Status field of the Users form.
	Role	You can map the parameter to the Role field of the Users form.
	Identity	You can map the parameter to the Identity field of the Users form.
	Disabled	You can map the parameter to the Disable User check box of the Users form.
	Organization	You can map the parameter to the Organization field of the Users form.
	Manager	You can map the parameter to the Manager field of the Users form.
	Start Date	You can map the parameter to the Start Date field of the Users form.
End Date	You can map the parameter to the End Date field of the Users form.	
Email	You can map the parameter to the Email field of the Users form.	
	Any fields that are displayed in the User Defined Fields tab of the Users form.	You can map the parameter to the selected user-defined field.

2.5.2 Adapter Variable Mapping Information

For a newly created adapter to work, you can map data to the parameters of the adapter's tasks. For this reason, you create placeholders, also known as adapter variables, to map the data at run time. Once an adapter variable is not needed for the adapter to run, you can remove it from the adapter. After you have deleted the adapter variable, recompile the adapter.

When an adapter variable is not the adapter return variable, or it is not designated as Resolve at Run time, it should be mapped within the Variable List tab of the Adapter Factory form. On the other hand, if the adapter variable is classified as an adapter

return variable, or the adapter variable is set to Resolve at Run time, it can be mapped at another location within Oracle Identity Manager. This location is contingent upon the adapter's type. For example, the variables of a process task adapter will be mapped at a different place than the variables of a pre-populate adapter. The following table lists the variables of a particular type of adapter that can be mapped.

Adapter Type	Location
Process Task	The Integration tab of the Editing Task window
Task Assignment	The Assignment tab of the Editing Task window
Rule Generator	The Map Adapters tab of the Data Object Manager form
Pre-Populate	The Pre-Populate tab of the Form Designer form
Entity	The Map Adapters tab of the Data Object Manager form

The following topics are discussed in this section:

- [From the Variable List Tab](#) on page 2-30
- [Process Task Adapter Variable Mappings](#) on page 2-31
- [Task Assignment Adapter Variable Mappings](#) on page 2-33
- [Rule Generator and Entity Adapter Variable Mappings](#) on page 2-35
- [Prepopulate Adapter Variable Mappings](#) on page 2-36

2.5.2.1 From the Variable List Tab

The following table lists the mappings that you can set from the Variable List tab.

Variable Type	Map To	Qualifier/Resource Type
Object	Adapter References	Database References
		Data Object References
	Set at run time (for Task Assignment adapters only)	Database References
		Data Object References
IT Resource	Resolve at Run time	The IT Resource types that are displayed in the Table view of the IT Resources Type Definition form
String, Character, Byte, Integer, Float, Long, Short, Double	Literal	If you are mapping the adapter variable to a literal, a Literal Value field is displayed below the Resource Type combo box. Within this field, enter the value of this literal.
	Resolve at Run time	NA
	Adapter References	Event Handler Name
		Note: If the data type of the adapter variable is not String, Adapter References cannot be selected from the Map To combo box.

Variable Type	Map To	Qualifier/Resource Type
Boolean	Literal	Boolean. If you select this resource type, two Literal Value options are displayed below the Resource Type combo box: True and False. Select the option that corresponds to the value of the adapter variable.
	Resolve at Run time	NA
Date	Literal	If you are mapping the adapter variable to a literal, a Literal Value lookup field is displayed below the Resource Type combo box. Double-click this lookup field. From the Date & Time window that is displayed, select the date and time that will be the value of this literal.
	Resolve at Run time	NA
	System Date	NA Note: This variable's value will reflect Oracle Identity Manager's date and time. Hence, you do not map it.

2.5.2.2 Process Task Adapter Variable Mappings

The following table lists the process task adapter variable mappings.

Variable Type	Map To	Qualifier/Description
Object (Adapter Return Variable)	Process Data	You can map the parameter to a field of either the associated custom process form, or a child table that belongs to this form.
	Response Code	NA
	Task Information	Note. You can map the parameter to the Note tab of the Task List form. Reason. You can map the parameter to the Error Details window. To access this window, double-click a task that is displayed within the Task List form.
	Process Definition	Name. You can map the parameter to the Name field of the Process Definition form. Type. You can map the parameter to the Type lookup field of the Process Definition form.
Object (Adapter Return Variable)	Organization Definition	The fields of the Organizations form to which you can map the adapter variable. Note: Because the data type of the adapter variable is Object, you cannot select Organization ID and Organization Parent ID from the Qualifier combo box.

Variable Type	Map To	Qualifier/Description
	User Definition	The fields of the Users form to which you can map the adapter variable.
IT Resource	IT Resource	You can map the parameter to an IT resource. This IT resource is a member of the IT resource type that is displayed in parenthesis from within the Data Type field.
	Process Data	You can map the parameter to a field of the associated process-specific form. Note: The only field names that are displayed in this combo box are ones with a data type of IT Resource Lookup Field.
String, Boolean, Character, Byte, Date, Integer, Float, Long, Short, Double	Process Data	You can map the parameter to a field of either the associated custom process form, or a child table that belongs to this form.
	Task Information	Note. You can map the parameter to the Note tab of the Task List form. Reason. You can map the parameter to the Error Details window. To access this window, double-click a task that is displayed within the Task List form.
	Process Definition	Name. You can map the parameter to the Name field of the Process Definition form. Type. You can map the parameter to the Type lookup field of the Process Definition form.
	Organization Definition	The fields of the Organizations form to which you can map the adapter variable.
String, Boolean, Character, Byte, Date, Integer, Float, Long, Short, Double	User Definition	The fields of the Users form to which you can map the adapter variable.

Variable Type	Map To	Qualifier/Description
	Literal	<p>If you are mapping the adapter variable to a literal, and the variable's data type is String, Character, Byte, Integer, Float, Long, Short, or Double, a Literal Value field is displayed below the Qualifier combo box. Within the field, enter the value of this literal.</p> <p>When you are mapping the adapter variable to a literal, and the variable's data type is Boolean, two Literal Value options are displayed below the Qualifier combo box: True and False. Select the option that corresponds to the value of the adapter variable.</p> <p>If you are mapping the adapter variable to a literal, and the variable's data type is Date, a Literal Value lookup field is displayed below the Qualifier combo box. Double-click this lookup field. From the Date & Time window that is displayed, select the date and time that will be the value of this literal.</p>
String	IT Resources	<p>If you are mapping the adapter variable to an IT Resource, three combo boxes are displayed below the Map To combo box: Qualifier, IT Asset Type, and IT Asset Property. From these combo boxes, select the qualifier for the mapping, the specific name of the IT resource, and the field of the IT resource that will receive the results of the mapping.</p> <p>Note: If the data type of the adapter variable is not String, IT Resources cannot be selected from the Map To combo box.</p>

2.5.2.3 Task Assignment Adapter Variable Mappings

The following table lists the task assignment adapter variable mappings.

Variable Type	Map To	Qualifier/Description
IT Resource	Object Data	You can map the parameter to an IT resource's instance key. This IT resource is a member of the IT resource type that is displayed in parenthesis from within the Data Type field.
	IT Resource	You can map the parameter to an IT resource.
Object (Adapter Return Value)	Object Data	You can map the parameter to a field of either the associated custom resource object form, or a child table that belongs to this form.
	Response Code	NA

Variable Type	Map To	Qualifier/Description
	Task Information	The fields of the Task List form to which you can map the adapter variable.
	Process Definition	The fields of the Process Definition form to which you can map the adapter variable.
	Organization Definition	The fields of the Organizations form to which you can map the adapter variable.
	User Definition	The fields of the Users form to which you can map the adapter variable.
String, Boolean, Character, Byte, Date, Integer, Float, Long, Short, Double	Object Data	You can map the parameter to a resource object's instance key.
	Task Information	The fields of the Task List form to which you can map the adapter variable.
	Process Definition	The fields of the Process Definition form to which you can map the adapter variable.
	Organization Definition	The fields of the Organizations form to which you can map the adapter variable.
String, Boolean, Character, Byte, Date, Integer, Float, Long, Short, Double	User Definition	The fields of the Users form to which you can map the adapter variable.
	Request Info	Request ID. You can map the parameter to the Request ID field of the Requests form. Request Action. You can map the parameter to the Request Action field of the Requests form. Request Priority. You can map the parameter to the Request Priority field of the Requests form.
	Request Target User	The fields of the Users form to which you can map the adapter variable.
	Request Target Organization	The fields of the Organizations form to which you can map the adapter variable.
	Requester Info	The fields of the Users form to which you can map the adapter variable.

Variable Type	Map To	Qualifier/Description
	Literal	<p>If you are mapping the adapter variable to a literal, a Literal Value field is displayed below the Qualifier combo box. Within the field, enter the value of this literal.</p> <p>Note: If the data type of the adapter variable is Boolean, two options are displayed in place of the field: True and False. Select the option that reflects the value of the adapter variable.</p> <p>Note: If the data type of the adapter variable is Object, Literal cannot be selected from the Map To combo box.</p>
String	IT Resources	<p>Resource Instance. You can map the parameter to an IT resource's instance key. This IT resource is a member of the IT resource type that is displayed in parenthesis from within the Data Type field.</p> <p>IT Asset Type. You can map the parameter to an IT resource type.</p>
String	IT Resources	<p>IT Asset Property. You can map this parameter to one of the properties that comprise the selected IT resource type.</p>

2.5.2.4 Rule Generator and Entity Adapter Variable Mappings

The following table lists the rule generator and entity adapter variable mappings.

Variable Type	Map To	Qualifier/Description
Object (Adapter Return Variable), IT Resource, String, Boolean, Character, Byte, Date, Integer, Float, Long, Short	Literal	<p>If you are mapping the adapter variable to a literal, a Literal Value field is displayed below the Qualifier combo box. Within the field, enter the value of this literal.</p> <p>Note: If the data type of the adapter variable is Object, Literal cannot be selected from the Map To combo box.</p>
	Entity Field	<p>You can map the adapter variable to a field of the associated process form. The name of this form is displayed in the Form Description field of the Data Object Manager form.</p>
	Contact	<p>The fields of the Contact Information tab to which you can map the adapter variable.</p>
	Location	<p>The fields of the Location form to which you can map the adapter variable.</p>

Variable Type	Map To	Qualifier/Description
	Organization Definition	The fields of the Organizations form to which you can map the adapter variable. Note: If the data type of the adapter variable is not Object, you cannot select Organization ID and Organization Parent ID from the Qualifier combo box.
	User Definition	The fields of the Users form to which you can map the adapter variable.

2.5.2.5 Prepopulate Adapter Variable Mappings

The following table lists the prepopulate adapter variable mappings.

Variable Type	Map To	Qualifier/Description
IT Resource	IT Resource	You can map the parameter to an IT resource. This IT resource is a member of the IT resource type that is displayed in parenthesis from within the Data Type field.
	Process Data	You can map the parameter to a field of the associated process-specific form. Note: The only field names that are displayed in this combo box are ones with a data type of IT Resource Lookup Field.
String, Boolean, Character, Byte, Date, Integer, Float, Long, Short, Double	Process Data	You can map the parameter to a field of the associated process-specific form.
	Organization Definition	The fields of the Organizations form to which you can map the adapter variable.
	User Definition	The fields of the Users form to which you can map the adapter variable.
	Location	The fields of the Location form to which you can map the adapter variable.
	Contact	The fields of the Contact Information tab to which you can map the adapter variable.

Variable Type	Map To	Qualifier/Description
String, Boolean, Character, Byte, Date, Integer, Float, Long, Short, Double	Literal	<p>If you are mapping the adapter variable to a literal, and the variable's data type is String, Character, Byte, Integer, Float, Long, Short, or Double, a Literal Value field is displayed below the Qualifier combo box. Within the field, enter the value of this literal.</p> <p>When you are mapping the adapter variable to a literal, and the variable's data type is Boolean, two Literal Value options are displayed below the Qualifier combo box: True and False. Select the option that corresponds to the value of the adapter variable.</p> <p>If you are mapping the adapter variable to a literal, and the variable's data type is Date, a Literal Value lookup field is displayed below the Qualifier combo box. Double-click this lookup field. From the Date & Time window that is displayed, select the date and time that will be the value of this literal.</p>
String	IT Resources	<p>If you are mapping the adapter variable to an IT Resource, three combo boxes are displayed below the Map To combo box: Qualifier, IT Asset Type, and IT Asset Property. From these combo boxes, select the qualifier for the mapping, the specific name of the IT resource, and the field of the IT resource that will receive the results of the mapping.</p> <p>Note: If the data type of the adapter variable is not String, then IT Resources cannot be selected from the Map To combo box.</p>

Oracle Identity Manager Connectors

The Oracle Identity Manager Connector Pack contains predefined connectors that you can use to integrate Oracle Identity Manager with the following target systems:

Note: Refer to the latest Oracle Identity Manager Connector Pack documentation for information about updates to this list.

- BMC Remedy User Management
- BMC Remedy Ticket Management
- CA-ACF2 Advanced
- CA-Top Secret Advanced
- Database User Management
- Database Application Tables
- IBM RACF Standard
- IBM RACF Advanced
- IBM i5/OS (OS/400) Advanced
- IBM Lotus Notes and Domino
- JD Edwards EnterpriseOne
- Microsoft Active Directory
- Microsoft Exchange 2000 and 2003
- Microsoft Windows
- Novell eDirectory
- Novell GroupWise
- Oracle e-Business Employee Reconciliation
- Oracle e-Business User Management
- Oracle Internet Directory
- Oracle Retail Warehouse Management System
- PeopleSoft Employee Reconciliation
- PeopleSoft User Management
- RSA Authentication Manager

-
- RSA ClearTrust
 - SAP CUA
 - SAP Employee Reconciliation
 - SAP Enterprise Portal
 - SAP User Management
 - Siebel Enterprise Applications
 - Sun Java System Directory
 - UNIX SSH
 - UNIX Telnet

If there is no predefined connector for your target system, then you can use the Administrative and User Console to create a generic technology connector that is customized to the requirements of your target system. Refer to Part II, "Integration Solutions Features" of *Oracle Identity Manager Administrative and User Console Guide* for information about generic technology connectors.

Glossary

This glossary lists all the terms that are frequently used in Oracle Identity Manager.

access

Access is the granting of enterprise resources to Oracle Identity Manager users and/or organizations. Access to these resources depends upon the specific policies adopted by the enterprise. The customer defines (and Oracle Identity Manager implements) policies that determine whether, how, and under what circumstances users gain access to various corporate resources.

access policy

This is a list of user groups and the resources with which users in the group are to be provisioned or deprovisioned. Access policies are defined by using the Access Policies menu item in Oracle Identity Manager Administrative and User Console.

access rights management

This is the process by which access to enterprise resources is granted or revoked. This includes decisions regarding which users can access specific resources and when they are allowed to access them.

adapter

A Java class, generated by the Adapter Factory, that enables Oracle Identity Manager to interact with an external JAR file, a target IT resource (for example, a resource asset), or a user-defined form.

An adapter extends the internal logic and functionality of Oracle Identity Manager. It automates process tasks and defines the rules for the auto generation and validation of data in fields within Oracle Identity Manager.

There are five types of adapters: task assignment adapters, task adapters, rule generator adapters, prepopulate adapters, and entity adapters.

adapter factory

A code-generation tool provided by Oracle Identity Manager, which enables a User Administrator to create Java classes, known as adapters.

adapter task

This is one of several possible components within an adapter. And this is a logical step within an adapter, equivalent to calling a programming language method. The following types of adapter tasks are available: Java Task, Remote Task, Stored Procedure Task, Utility Task, Oracle Identity Manager API Task, Set Variable Task, Error Handler Task, and Logic Task.

adapter variable

This is a user-defined placeholder within the adapter that contains run-time application data used by its adapter tasks. An adapter variable can be used multiple times within a single adapter.

administrative queue

This is a list of user groups (or other administrative queues). Users who are members of groups that comprise a queue can be assigned administrative privileges on a particular data element. Administrative queues serve as a mechanism for mass-assigning users with administrative privileges on a given record. Each administrative queue consists of one or more user groups (and/or administrative queues) and the privileges (for example, read, write, and delete) the members of the queue have on the records to which the queue is assigned.

Application Program Interface (API)

This is the interface (calling conventions) by which an application program accesses an operating system and other services. An API is defined at the source code level and provides a level of abstraction between the application and the kernel (or other privileged utilities) to ensure portability of the code.

An API can also provide an interface between a high-level language and lower-level utilities and services that were written without consideration for the calling conventions supported by compiled languages. In this case, the API's main task might be the translation of parameter lists from one format to another and the interpretation of call-by-value and call-by-reference arguments in one or both directions.

approval process

This is one of two Oracle Identity Manager process types. This type of process is generally used to approve the provisioning of Oracle Identity Manager resources to users or organizations. Unlike provisioning processes, approval processes are usually comprised of tasks that must be manually completed.

attestation

Attestation enables reviewers to be notified of a report they must review that describes the provisioned resources that certain users have. The reviewer can attest to the accuracy of the entitlements by providing a response. This attestation action, along with the response the reviewer provided, any associated comments, and an audit view of the data that the reviewer viewed and attested to, is tracked and audited to provide a complete trail of accountability. In Oracle Identity Manager, this process is known as an attestation task.

auditor

Software component used to audit a specific entity.

audit engine

The audit engine is the main component for creating audits history for different areas of the Oracle Identity Manager system. The engine is in charge of receiving changes to data objects and passing them along to auditors interested in those data object changes.

audit manager

Software component that manages the individual auditors and helps in auditing.

audit record

A collection of information of interest for one transaction.

audit subrecord

One subentry in the audit record. Audit subrecords are captured during transactions and applied to the previous snapshot.

auditor registration

A phase in which Audit Manager determines the existence of auditors and exchanges information such as data objects and change records.

auto-group membership

This is a rule-based mechanism by which Oracle Identity Manager automatically adds or removes users to and/or from user groups. See [rule](#).

authoritative identity reconciliation

This is also known as Trusted Source Reconciliation, which can be used to create, update, and delete users in Oracle Identity Manager.

automated task

This is any task within a process that does not require user-interaction for completion. Automated tasks always require a process task adapter. Provisioning processes are generally comprised of automated tasks. See [Process Task Adapter](#).

back end

A general term for the database server functions and procedures used to obtain and manipulate data on a network. This is also the storage location for Oracle Identity Manager's data.

certification authority

A third-party company that issues trusted certificates. See [trusted certificate](#).

child table

A subordinate database table used to store, access, and reference the information associated with one or more fields of a user-created form, which has been defined by using the **Form Designer** form.

client

This is the GUI tier of the client/server edition of Oracle Identity Manager. See [Oracle Identity Manager Administrative and User Console \(Web Application\)](#).

column header

The box containing the name of the column associated with the data in a table column. To change the order in which records are sorted in a particular table, click the column header for that table column.

conditional task

A process task that is not part of the default process instance. A conditional task is inserted into a process only when specific predefined conditions are satisfied. See [process task](#).

connector

Used to integrate Oracle Identity Manager with a specific third-party application, such as Microsoft Active Directory or Novell eDirectory.

custom lookup queries

See [lookup queries](#).

data field

Areas of a form into which information can be entered (for example, **Organization Name**). Data fields are used to contain, display, and potentially edit the data entered into them.

data flow

This is the transfer of information between processes or related forms (for example, from resource forms to process forms).

data object

Data Object is an internal object representation of tables in the Oracle Identity Manager data model in which business logic is applied. It is also responsible for inserting, updating, and deleting data from the data store.

data object manager

The Oracle Identity Manager form used to assign event handlers, rule generator adapters, or entity adapters to data objects. These event handlers or adapters can be run in a specific order on a database event on pre or post insert, pre or post update, or pre or post delete. See [event handler](#). See [data object](#).

data security

Protection of information from unauthorized release, use, editing, or deletion.

data set

A data set is a representation of data that is at a particular stage of transit between the target system and Oracle Identity Manager. Data sets can be visualized as data structures arranged in the form of layers, with data flowing from one layer to another during provisioning and reconciliation. Oracle Identity Manager provides features that enable you to specify the fields that constitute these data sets.

database

This is the storage facility for data within Oracle Identity Manager. Oracle Identity Manager controls this data by using a software application known as the Database Management System (DBMS). See [Database Management System \(DBMS\)](#).

Database Management System (DBMS)

This is software that controls the organization, storage, retrieval, security, and integrity of data in a database within Oracle Identity Manager. DBMS accepts requests from the application and instructs the operating system to transfer the appropriate data.

delegated administrators

This is an Oracle Identity Manager user who has been assigned administrative responsibilities. Administrative rights are assigned by using membership within administrative groups. Administrators have access only to those organizations, forms, data, and users for whom they are responsible. See [user group](#).

delimited field

This is a field containing data of varying length (as opposed to fixed-length fields). Individual fields of this type are separated by a field delimiter (for example, a comma or semicolon).

delimited file

A file comprising of data records of varying lengths. Individual records are separated by a record delimiter character (for example, a hard return or colon).

dependent object

This is a resource object that has a dependency relationship with another resource object. The processes of the parent resource object must be completed before the processes of the dependent resource object can be started. See [resource object](#).

dependent task

A process or adapter task that is dependent on another process or adapter task, respectively. Oracle Identity Manager or an Oracle Identity Manager user can only start this type of task once the process/adapter task on which it is dependent is completed.

deprovisioning

The rescinding of a user's, user group's, and/or organization's access to a resource. See [Process Task Statuses](#).

digital signature

This is an identification mechanism, which is used within Oracle Identity Manager to secure password propagation, by authenticating the application or device receiving the password.

direct provisioning

This is one of the methods by which a resource can be provisioned. Only users with specific administrative privileges can direct provision resources. When a resource is direct provisioned (to a user or organization), Oracle Identity Manager does not invoke the standard approval process (because this is only associated with requests) or the resource's approval process. Instead, Oracle Identity Manager proceeds directly to beginning the applicable provisioning process for the resource. See [request](#).

Electronic Data Interchange (EDI)

This is the electronic format for the automated communication of business transactions (for example, orders, confirmations, and invoices) between organizations. EDI services, provided by third parties, enable organizations with potentially disparate hardware to connect and exchange data. Although interactive access might comprise a component of such a solution, EDI implies direct computer-to-computer transactions within vendors' databases and ordering systems.

e-mail definition

This is a predefined template that is used when generating e-mail notifications. E-mail definitions are created by using the Email Definition form. See [e-mail notification](#).

e-mail notification

This is the act of informing an Oracle Identity Manager user of the occurrence of an action, process task assignment, or process task status change by using e-mail.

end-user

See [user](#).

end-user administrator

See [user](#).

entity adapter

This is one of five Oracle Identity Manager adapter types. This type of adapter is attached directly to a provisioning process and/or a form by using the Data Object Manager form. Oracle Identity Manager is able to trigger and run entity adapters on preinsert, preupdate, predelete, postinsert, postupdate, or postdelete.

error handler task

This is one of several adapter task types. This type of adapter task is used to display any errors associated with an adapter that occur at run time. In addition, you can view the reasons for the errors, along with possible solutions. See [adapter task](#).

error message

This is informative text that is displayed when a specific problem occurs within Oracle Identity Manager.

event

This is an action (started by Oracle Identity Manager, an external system, or a user) and/or a result of that action being performed.

event handler

This is a Java class that executes user-defined or system-generated actions. An event handler can be set to run on:

- PreInsert: Before information is added to the database.
- PreUpdate: Before information is modified within the database.
- PreDelete: Before information is removed from the database.
- PostInsert: After information is added to the database.
- PostUpdate: After information is modified within the database.
- PostDelete: After information is removed from the database.

See [event](#). See [data object manager](#).

explorer

This is the Windows-styled list of folders and forms displayed in the left-hand panel of the Oracle Identity Manager application window. The folders and forms displayed in the Explorer (as well as their nesting configuration and display sequence) might vary for each user depending on the user groups to which the user belongs.

export

This is the act of taking an XML data file (produced by Oracle Identity Manager), and using it to transmit information to additional Oracle Identity Manager environments.

field

This is a data element of a database record or area of a GUI form in which a particular item of data is stored.

form

A graphical user interface layout (or mechanism) used to view, insert, edit, and delete information associated with records in the Oracle Identity Manager database. A form can be displayed as two distinct views:

- Form View that contains detailed information related to a single record.
- Table View that contains minimal information related to multiple records.

See [record](#).

form designer

A form used to create customized forms. Forms created by using this form must be associated with a process or a resource object. These forms (and the fields that comprise the forms) are used to provide processes or resource objects with a mechanism for obtaining additional information they require to conduct provisioning.

form tab

A region of a form used to display details related to the primary form or record. Tabs allow for the conservation of active space on the screen while providing streamlined access to related data.

form view

See [form](#).

front end

This is a general term for the client within a client/server model. The front end provides for the display of information and supports actions started by users.

generated task

A process task that Oracle Identity Manager starts when another related process task achieves a predefined status (provided that this status is represented by a response). See [response](#).

generic adapter

The generic adapter contains the code for all the provisioning functions that a generic technology connector performs.

generic auditor

The generic auditor as the name suggests is a generic auditor. It is driven by an XML metadata contained in the AUD table. The metadata information specifies the auditor name that the generic auditor will use for the interested data objects and what other information is needed to record the snapshot.

generic technology connector

A generic technology connector is a collection of components. A component provides a service that is used by another component, the target system, or Oracle Identity Manager. Together, these components can be linked to support a wide variety of data formats and data transport mechanisms.

import

The act of taking a previously created XML data file, and using it to load information into Oracle Identity Manager by using the deployment manager. Import files are generated by other Oracle Identity Manager environments. They can contain either new information to be added to Oracle Identity Manager or updates to information

that already exists in Oracle Identity Manager (for example, a record insert or record update).

IT resource asset

This is Oracle Identity Manager representation of the physical component of the external target resources provisioned by Oracle Identity Manager (for example, the various Solaris servers in a company).

JAR file

This is a Java Archive file. A compressed archive file (denoted by a .jar extension) containing one or more Java class files. This file format is used to distribute and run Java applications.

JavaBean

JavaBeans allow developers to create reusable software components that can then be assembled together by using visual application builder tools. Within Oracle Identity Manager, it is a Java program module that is used by Oracle Identity Manager Remote Manager to communicate bidirectionally with non-network-aware APIs. See [remote manager](#).

Java DataBase Connectivity (JDBC)

A programming interface used by Java applications to access databases by using SQL. Because Java interpreters (or Java Virtual Machines) are available for all major operating systems, this interface supports the creation, modification, and deletion of platform-independent database applications.

Java task

This is one of several adapter task types available within the Adapter Factory form. This type of adapter task is used to communicate with an external source through a Java API. See [adapter task](#).

Logic task

This is one of several adapter task types available within the Adapter Factory form. This type of adapter task is used to build a conditional statement within an adapter (for example, an if statement, a for-loop, or a while loop). See [adapter task](#).

lookup definition

A definition that can represent:

- The name and description of a text field;
- A lookup field and the values that are accessible from that lookup field; or
- A combination box and the commands that can be selected from that combination box.

Lookup definitions are created by using the Lookup Definition form (for default forms) or the Form Designer form (for custom forms). See [lookup field](#).

lookup field

This is a data field that provides the user with a set of pre-defined values. Lookup fields only accept values selected from the pre-defined list as valid entries. See [data field](#).

lookup queries

You can define lookups (for lookup fields and combination boxes) in Oracle Identity Manager for user-defined fields (UDFs) in system forms (for example, User Form, Resource Object Form) and fields of user-defined resource and object forms. The lookups are defined in two ways:

- **Lookup Queries:** where the queries are statically defined for the field and are run against the appropriate database table.
- **Lookup Codes:** where the items are displayed in a list from a lookup definition table

The (custom) lookup queries have been enhanced to allow the lookup query to be parameter driven. The parameter property is a mapped parameter, where you can specify:

Filter Column: the column for which a value is specified in the "where" clause

Filter Map: the source from where the value comes from

While the enhancement itself is delivered as part of the existing Forms Designer feature in the Design Console, any updates made by this feature are rendered on the Administrative and User Console dynamically as administrators, approvers, or end-users access the updated form(s).

lookup value

This is an item, which contains information pertaining to the text field, lookup field, or combination box that represents the lookup definition. See [lookup definition](#).

manual task

This is any task within a process that requires user action in order to be completed. Approval processes generally comprise manual tasks.

Metadata

This is data about data. Metadata can represent information about or documentation of other data managed within an application or environment. For example, metadata can be used to provide information about data elements or attributes, (name, size, data type), records or data structures (length, fields, columns) or the physical location or permissions of data (where it is located, how it is associated, ownership). Within Oracle Identity Manager, there are two types of metadata, system metadata, which is internal to the Oracle Identity Manager system, and customer metadata, such as process definitions.

nested rule

This is a rule that is contained or embedded within another rule.

network

This is a system that connects computers and peripheral devices to allow for the sharing of information and resources. Networks are categorized by speed and distance between the computers. The most common kind of network is a LAN, which usually connects computers within an office. Another kind of network is a WAN, which connects computers at different locations. See [Wide Area Network \(WAN\)](#).

object

This is any resource that can be provisioned (for example, a database, server, software application, file, or directory access). Also referred to as a resource object.

OIM Account

An OIM Account is granted to an OIM User to give the OIM User the ability to log in to Oracle Identity Manager and access Oracle Identity Manager features. At the minimum, these features involve self-service and request. An OIM Account can be granted additional privileges including the ability to define workflows and the delegated administration of various entities, such as users, organizations, and roles. See [OIM User](#).

OIM User

An OIM User is an identity that exists within and is managed through Oracle Identity Manager. An OIM User can be created in the following ways:

- Through reconciliation from one or more trusted identity sources, such as HRMS or LDAP
- Manually, by using the Administrative and User Console
- Through the Java APIs or the SPML Web Service

An OIM User might or might not have an OIM Account. From release 9.1.0 onward, every OIM User has an OIM Account. See [OIM Account](#).

Open DataBase Connectivity (ODBC)

A database-programming interface produced by Microsoft that provides a common language for Microsoft Windows applications to access databases on a network. ODBC comprises of the function calls programmers write into their applications and the ODBC drivers themselves.

For client/server database systems (such as Oracle Database and Microsoft SQL Server), the ODBC driver provides access to the database by using links to their database engines. For desktop database systems (such as dBASE and FoxPro), the ODBC drivers actually manipulate the data. ODBC supports SQL and non-SQL-compliant databases. Although the application always uses SQL to communicate with ODBC, ODBC communicates with non-SQL-compliant databases in their native language. See [Structured Query Language \(SQL\)](#).

operation

This is an operand (for example, and/or) that determines and illustrates the relationship among the multiple elements (or nested rules) of a rule.

Oracle Identity Manager

A software platform that automates access rights management and the provisioning of resources. Oracle Identity Manager instantly connects users to the resources that can be productive, and revokes and or prevents unauthorized access to protect proprietary information and enhance security.

Oracle Identity Manager API Task

This is one of several Oracle Identity Manager adapter task types. This type of adapter task enables an external third-party application to access Oracle Identity Manager functionality from outside of Oracle Identity Manager. See [adapter task](#).

Oracle Identity Manager Client

See [client](#).

Oracle Identity Manager Explorer

See [explorer](#).

Oracle Identity Manager Server

See [server](#).

Oracle Identity Manager System Administrators

These are members of Oracle Identity Manager user groups to which maximum system access has been assigned. See [system administrator](#). See [user](#).

Oracle Identity Manager User

See [user](#).

Oracle Identity Manager Administrative and User Console (Web Application)

This is the user interface using which end-users and delegated administrators access Oracle Identity Manager functionality by using the Internet (Web browser).

Oracle Identity Manager Workspace

See [workspace](#).

organization

A record used to represent an organizational unit within a company's hierarchy (for example, a department, division, or cost center). Oracle Identity Manager does not limit the number of suborganizations that can be created within an organization.

organization target

The Oracle Identity Manager organization that is to be provisioned with a resource specified within a request.

password policy

A collection of criteria used to validate password creation and modification within Oracle Identity Manager or on an external resource. The criteria within a policy are applied based on the rule associated with it on the resource object to which it has been attached. Password policies can be defined for Oracle Identity Manager and/or third-party system passwords.

password policy rule

A rule used to determine which password policy is to be applied to password creation and modification on a particular resource or within Oracle Identity Manager. Password policy rules are always of type General. See [rule](#).

Prepopulate Adapter

This is one of five Oracle Identity Manager adapter types that are used to populate data on user-defined fields on user-defined forms. This specific type of rule generator adapter can be attached either to custom fields of forms or to fields of custom forms. These fields are created by using the User Defined Field Definition form and the Form Designer form, respectively.

See [Rule Generator Adapter](#).

preceding task

A task that must have a status of Completed before Oracle Identity Manager or a user can start any tasks dependent on it. See [dependent task](#).

Presentation Layer

See [client](#).

process

This is a collection of one or more process tasks in addition to a requested instance of a process definition. See [process definition](#).

process definition

This is a record containing a detailed definition of all properties of a process as well as its workflow and the tasks that comprise it.

process status

This is the current state of execution for a process. The status of a process is determined by the status of its tasks. See [status](#).

process task

This is a step or component of a process (as specified within the **Process Definition form**). Process tasks can be independent or dependent on one another.

Process Task Adapter

This is one of five Oracle Identity Manager adapter types. This type of adapter helps Oracle Identity Manager to automate the execution of a process task. See [process task](#).

Process Task Statuses

A process task status indicates the status of the task throughout its entire life cycle. A task has following predefined statuses R, C, X, P, W, XLR, UCR, UT, S, UC, PX, and MC.

provisioning

This is the granting of access for resources to users in conformance with Oracle Identity Manager policies. See [deprovisioning](#).

provisioning policy

This is an access policy that is applied to a user group during resource provisioning. A provisioning policy is one of several factors that determine whether a resource object can ultimately be provisioned to the user. A provisioning policy definition specifies the resource objects that can be allowed or disallowed for one or more user groups. See [access policy](#). See [resource object](#). See [user group](#).

provisioning process

This is one of two Oracle Identity Manager process types. This type of process is used to provision Oracle Identity Manager resources to users or organizations.

provisioning status

The status of the resource object as it is being provisioned to a user or an organization. A resource object can have one of nine predefined statuses:

- **Provisioning:** The resource object has been assigned to a request, and an approval process and a provisioning process have been selected.
- **Provisioned:** The resources, represented by the resource object, have been provisioned to the users or organizations.
- **Enabled:** The resources, represented by the resource object, have been provisioned to the users or organizations. In addition, these users or organizations have access to the resources.

- **Disabled:** The resources, represented by the resource object, have been provisioned to the users or organizations. However, these users or organizations have temporarily lost access to the resources.
- **Revoked:** The resources, represented by the resource object, have been provisioned to the users or organizations. However, these users or organizations have been permanently deprovisioned from using the resources.
- **Provide Information:** Additional information is required before the resources, represented by the resource object, can be provisioned to the target users or organizations.
- **None:** This status does not represent the provisioning status of the resource object. Rather, it signifies that a task, which belongs to the provisioning process that Oracle Identity Manager selects, has no effect on the status of the resource object.

query

A method of searching for particular data records within a database by using a common characteristic. For example, a common query performed on the Organizations page in the Administrative and User Console is to retrieve all records related to a particular organizational unit. Oracle Identity Manager has many powerful built-in query syntax tools.

RACF server

See [Resource Access Control Facility \(RACF\) server](#).

record

A collection of related items of information organized as a single unit of data (for example, a single record comprising of a name, telephone number, and address). The record is the entity stored in the database that contains this related information (whereas forms are the mechanism employed by the user to view or edit that information).

reconciliation

The process by which any action to create, modify, or delete a target system identity started in the target system (by using traditional means) is communicated back to the provisioning system and recorded.

reconciliation rule

These are rules configured to identify a matching user in Oracle Identity Manager based on reconciliation fields.

recovery task

This is a process task that starts when a preceding process task achieves a status of Rejected. The relationship between the primary task and its recovery task must be predefined for this to occur. This relationship is set within the Undo/Recovery tab of the process task's Editing Task window.

remote manager

A server that enables Oracle Identity Manager to communicate with a remote application that is either non-network-aware, or is network-aware, but is not located on the Oracle Identity Manager Server. Remote managers are employed when Oracle Identity Manager has to perform some function with this third-party application (for example, call a method that resides within the external API).

remote task

This is one of several adapter task types. This type of adapter task enables an adapter to call a method on an API (for example, when the API resides on a computer that is external to Oracle Identity Manager).

Remote tasks are generally used within integrations of third-party APIs that are not network-enabled. In these cases, a remote manager runs the remote API method, which is located on a remote computer.

Remote tasks can also be used with integrations of third-party APIs, which are network-enabled, but are not located on the Oracle Identity Manager Server for scalability purposes. The remote API method is still executed by a remote manager. However, because the third-party API is network-enabled, the remote manager does not have to reside on the target system. See [adapter task](#).

request

This is an entity that represents the beginning of the approval and provisioning of one or more resources to one or more users or organizations. When a request for the provisioning of resources is submitted, Oracle Identity Manager will:

- Select and evaluate a standard approval process.
- Select and evaluate a resource-specific approval process for each resource in the request.
- Select and run a resource-specific provisioning process for each resource in the request.

The request record maintains information about the standard approval process and the resource-specific approval process instances. Administrators or end-users generally place requests. Requests can also originate in external systems.

Request-based provisioning differs from direct provisioning. Direct provisioning bypasses both the standard approval process and resource-specific approval process. See [direct provisioning](#).

request status

This is the current state of the request. A request can have one of six statuses:

- Request Initialized: This status signifies that the initial data fields of the Requests form have been populated, and the request has been saved.
- Request Received: This status signifies that both a resource object and a user or organization has been assigned to the request, and that the Complete Request Creation button has been clicked.
- Approved: This status signifies that the standard approval tasks are completed.
- Not Approved: This status signifies that the request has been rejected or canceled.
- Object Approval Complete: This status signifies that all the approval tasks in standard approval and object approvals are completed.
- Request Complete: Request goes to this status when the request is complete.

reset password

This is the ability of a user to change the password.

When the user first registers with Oracle Identity Manager (by using the Oracle Identity Manager Web Application), the user must select personal verification

questions, and specify the answers to these questions. Oracle Identity Manager then uses these questions to verify a user's identity and reset his or her password.

requester

This is the user who created and submitted a request. See [request](#).

resource

Also referred to as a Resource Object. This is any unit of hardware, software, or data over which a company wishes to enforce provisioning control. For example, hardware resources can be servers and printers in the network. Software resources can be programs, utilities, or even smaller elements within a program. Data resources could be any accessible files or databases.

The Oracle Identity Manager resource object definition is the virtual representation of the resources to be provisioned. For example, a resource object can have one or more approval processes, provisioning processes, rules, and password policies.

The Oracle Identity Manager resource object definition is used to control the various processes and policies associated with the resource, as well as set systemwide options that will determine how the resource is provisioned.

Resource Access Control Facility (RACF) server

A remote IBM mainframe security application used by Oracle Identity Manager to:

- Verify the ID and password of a user.
- Control the access of users to Oracle Identity Manager resources.

response

This is a predefined message or action that is generated when a process task is started and achieves a particular completion status.

resource object

See [resource](#).

result set

The data or records returned from a query. Most API results are returned in Result Set format.

row header

The rectangular box located along the left edge of each row in a table in the Oracle Identity Provisioning Design Console. The row header displays the row number of the associated record within the current sort order (if the sorting criteria are changed, then the row number can also change). In most forms, a record can be selected by double-clicking the row header.

rule

User-defined criteria employed by Oracle Identity Manager to match conditions and take action based on them. There are five types of rules (the first four are defined by using the Rule Designer form):

- **General:** This type of rule enables Oracle Identity Manager to add a user to a user group automatically. It also determines the password policy that will be assigned to a resource object.

- **Process Determination:** This type of rule determines the standard approval process that will be associated with a request, as well as the approval and provisioning processes, which will be selected for a resource object.
- **Task Assignment:** This type of rule is used to determine the user or user group to which a task is to be assigned.
- **Prepopulate:** This type of rule is used to determine the prepopulate adapter that Oracle Identity Manager selects when populating a custom field of an Oracle Identity Manager or user-defined form. See "[Prepopulate Adapter](#)".
- **Reconciliation:** This type of rule is used to specify the criteria Oracle Identity Manager applies when attempting to match changes to data within target resources or trusted sources (for example, external systems with which you have configured Oracle Identity Manager to compare and reconcile data) with data in Oracle Identity Manager. Reconciliation rules are defined by using the **Reconciliation Rules form**.

rule element

This is the logical component of a rule. It is a unit that consists of an attribute, an operator, and a value (for example, user role == full time).

Rule Generator Adapter

This is one of five Oracle Identity Manager adapter types. This type of adapter is responsible for automatically generating, modifying, or verifying the value of a form's field, and saving this information to the database. Values supplied by a rule generator can be overridden by user input.

scheduled task

These are tasks configured in Oracle Identity Manager to run on a scheduled time.

self-registration

This is the ability of a user to register with Oracle Identity Manager by using the Oracle Identity Manager Web Application.

server

The software architecture tier used to implement the business logic and manage the interaction between the Oracle Identity Manager Client and the database.

set variable task

This is one of several adapter task types. This type of adapter task lets you set the value of a variable within an adapter. See [adapter task](#).

Simple Object Access Protocol (SOAP)

A message-based protocol based on XML used for accessing services on the Web. started by Microsoft, IBM, and others, it employs XML syntax to send text commands across the Internet by using HTTP. Similar in purpose to the COM and CORBA[®] distributed object systems, but more portable and less programming intensive, SOAP is used to invoke services throughout the Web. Because of its simple exchange mechanism, SOAP can also be used to implement a messaging system. SOAP is supported in COM, DCOM, Internet Explorer, and Microsoft Java implementation.

Snapshot

State at the end of a transaction.

standard approval process

This is a type of approval process. This type of approval process is used to approve a request as a whole, which can include multiple resource objects, and users or organizations. It is not resource-specific but rather request-specific.

status

This is the current state of execution for a given process or process task. The statuses of each task within a process determine the overall status of the parent process (certain tasks statuses have a greater effect on the process' overall status). There are six main statuses within Oracle Identity Manager:

- **Canceled:** The process or process task has been stopped (once a status is canceled, its status cannot be changed).
- **Suspended:** The process or process task has temporarily been placed on hold.
- **Rejected:** The process or process task has not been completed successfully or has not been approved. The status of 'Rejected' process tasks can only be changed to 'Canceled' or 'Unsuccessfully Completed'. If a retry task has been specified, it will be inserted.
- **Pending:** A user or system action is currently being performed on the process or process task. This status also signifies that all preceding tasks and processes on which the process or process task might be dependent have been completed.
- **Completed:** The process or process task has been run successfully.
- **Waiting:** The process or process task cannot be completed until all preceding process tasks or processes, on which the current process or process task is dependent, are completed.

stored procedure

A SQL program located within a particular database schema. Stored procedures contain information, such as SQL statements, which are precompiled for greater efficiency. See [stored procedure task](#).

stored procedure task

This is one of several adapter task types. This type of adapter task help Oracle Identity Manager to map to and run SQL programs that are located within a particular database schema. Within Oracle Identity Manager, these programs are known as stored procedures.

By incorporating a stored procedure task into an adapter and attaching this adapter to a process task, Oracle Identity Manager can use stored procedures on any Oracle Database or Microsoft SQLServer database (assuming it is accessible on its network). This includes retrieving primitive values from stored procedures. See [adapter task](#). See [stored procedure](#).

Structured Query Language (SQL)

This is a database language created by IBM in a research project in the late 1970s. It rapidly became the standard database language due to its combination of elegance, power, and connectivity. It is commonly used with database servers on mainframes, minicomputers, and PCs. An ANSI standard for the language exists.

suborganization

This is an organization that is a member of and derived from a higher-level (or parent) organization (for example, a department within a division). See [organization](#).

suspended

See [standard approval process](#).

system administrator

This user has both read and write access to all forms and records within Oracle Identity Manager.

Task Assignment Adapter

This adapter enables Oracle Identity Manager to automate the allocation of a process task to a user or group. A task assignment adapter can be written to dynamically assign a task based on parameters in the task request. The new Task Assignment Adapter is associated with a task assignment rule.

The Task Assignment Adapter enhances the mechanism of assigning a task through the Assignment tab of the Editing Task form (nested in the Process Definition form), where a rule is attached to a task, and users or groups are assigned to the current task.

table-view

A presentation mechanism for a collection of data records in which the items are arranged according to common predefined elements. In SQL database tables, the information is organized within columns and rows. A column represents one field or piece of information, such as a name. A row contains information related to one record. A record is a set of columns. Therefore, SQL tables are thought of as having multiple rows of columns. In Oracle Identity Manager, tables are presented in Table views in order to display multiple records on a single screen simultaneously. By contrast, a Form view can display only one record at a time. When queries are performed, only the records that satisfy the search criteria will be displayed in the Table view. See [form](#). See [form tab](#).

target resource

The external resource or application to which you wish to provision a user or organization with access by using Oracle Identity Manager.

Within the context of Oracle Identity Manager's reconciliation functions, this term has a more specific meaning. It is then used to refer to a resource with which Oracle Identity Manager has been set to conduct reconciliation. Target resources differ from trusted sources in that Oracle Identity Manager only accepts changes to the primary user record from a trusted source. All other external applications with which Oracle Identity Manager is conducting reconciliation are referred to as target resources.

target resource reconciliation

This refers to reconciliation that result in creation/update/revocation of resources provisioned to a user in Oracle Identity Manager. Account Discovery, Orphan Account Discovery, Rogue Account Discovery, and Direct Management Discovery are all specific use cases within this type of reconciliation.

task

See [process task](#). See [adapter task](#).

task status

This is the status of a process task. The status of a process' tasks determines the process' overall status.

three-tier architecture

Oracle Identity Manager consists of three distinct tiers. The three tiers of Oracle Identity Manager are the Oracle Identity Manager Client, Oracle Identity Manager Server, and the database. See [client](#). See [server](#). See [database](#).

toolbar

The set of icons along the top edge of the Oracle Identity Manager Design Console window that provides access to frequently used functions. When you click an icon, the function of that icon is triggered. If you take the mouse pointer over a icon, a tool tip describing that icon is displayed.

trusted certificate

A digital ID, which verifies that the user's password for an external application is being transmitted to Oracle Identity Manager from the correct location.

trusted source

This is the Resource object in which a unique key for reconciliation with data in Oracle Identity Manager has been defined. The trusted source is the resource object from which Oracle Identity Manager accepts changes to the user record definition. There can be more than one trusted source and more than one key for each trusted source.

trusted source reconciliation

See [authoritative identity reconciliation](#).

undo task

This is a process task that will be started when a predefined associated process task is canceled.

user

An individual who possesses an account and login credentials within Oracle Identity Manager. There are two distinct types of users in Oracle Identity Manager:

- **End-User Administrators:** This type of user might use either the Administrative and User Console or the Design Console of Oracle Identity Manager. End-user administrators are responsible for configuring Oracle Identity Manager for their company's end-users.
- **End-Users:** This type of user can access only the Oracle Identity Manager Administrative and User Console. End-users are generally only able to perform basic functions within Oracle Identity Manager.

User-Defined Field (UDF)

Supplemental fields that can be created by the user to augment the fields already present on the Organizations, Users, Requests, Resource Objects, User Groups, Form Designer, or Locations forms. By using a user-defined field, an administrator can provide a location for entering and storing data, define default values, format input data, create and apply data validation criteria, and provide a label for the field. The field and its contents are then stored in the database.

user group

This is a collection of one or more users. User group definitions can be used to assign permissions to all members of the group (for example, the users). The user group is an efficient mechanism for managing the privileges and access rights for large numbers of users.

User profile auditor

The user profile auditor inherits from the generic auditor to perform the user profile auditing. The user profile auditor relies on generic auditor to read and parse its XML metadata, process the changes to data objects, and process the offline creation of the snapshot.

user target

This is the user for whom a resource has been requested or direct provisioned.

utility task

This is one of several adapter task types. It is an adapter task that helps an adapter to be populated with any of the methods and APIs that are packaged with Oracle Identity Manager. In addition, this type of task provides you with access to a Java API. See [adapter task](#).

Wide Area Network (WAN)

This is a computer network that connects computers at different locations. A WAN often connects to many LANs.

workspace

The region of the Oracle Identity Manager application window, displayed within the right-hand panel, which contains the forms and tables used to view, edit, and manage information.

XML - Extensible Markup Language

This is an open standard for describing data from the World Wide Web Consortium (W3C). It is used for defining data elements on a Web page and business-to-business documents. It uses a tag structure similar to HTML; however, whereas HTML defines how elements are displayed, XML defines what those elements contain. HTML uses predefined tags, but XML helps tags to be defined by the developer of the page. As a result, virtually any data items, such as product, sales rep and amount due, can be identified, allowing Web pages to function similarly to database records. By providing a common method for identifying data, XML supports business-to-business transactions and is expected to become the dominant format for electronic data interchange. See [Electronic Data Interchange \(EDI\)](#).

Index

A

access policy, 1-4
access privileges, 1-8
account creation, 1-8
account modifications, 1-9
adapter, 2-26
adapters
 entity adapter variable mappings, 2-35
 literals, 2-27
 organization definition, 2-28
 prepopulate adapter variable mappings, 2-36
 process definition, 2-28
 process task adapter variable mappings, 2-31
 references, 2-27
 rule generator adapter variable mappings, 2-35
 task, 2-26
 task assignment adapter variable mappings, 2-33
 task mapping, 2-26
 tasks, 2-27
 user definition, 2-28
 variable, 2-29
 variable mapping, 2-29
 variables, 2-27
Administrative and User Console, 1-1

B

Base Help URL, 2-18
Business Rule Definition folder, 2-4

C

connectors, 3-1

D

data types, 2-14
Deployment Manager, 1-5
Design Console, 2-1
Design Console Administration folder, 2-3
Development Tools folder, 2-4

F

folders
 Business Rule Definition, 2-4

Design Console Administration, 2-3
Development Tools, 2-4
Process Management, 2-3
Resource Management, 2-3
User Management, 2-2

I

Inheritance, 2-18

L

Lookup Query, 2-15

O

Organization Provisioning, 2-5

P

Process Management folder, 2-3
profile editing, 1-9

R

reports, 1-5
 historical reports, 1-6
 operational reports, 1-5
Resource Management folder, 2-3
rule elements, 2-4

S

service account
 management tasks, 2-24
service accounts, 2-24
system properties, 2-18

T

To-Do list, 1-3

U

user group, 1-4
User Management folder, 2-2
user registration operations, 1-7

V

variables, 2-11